

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

Тернопільський національний технічний університет

імені Івана Пулюя

Кафедра комп'ютерних систем та мереж

МЕТОДИЧНІ ВКАЗІВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

з дисципліни “Адміністрування комп'ютерних мережевих систем”

для студентів денної форми навчання

спеціальність 7.05010201 “Комп'ютерні системи та мережі”

Тернопіль – 2011

Методичні вказівки до виконання лабораторних робіт розроблені у відповідності з навчальним планом за спеціальністю 7.05010201 “Комп’ютерні системи та мережі”

Укладачі: д.т.н., проф. Щербак Л.М., асист. Шингера Н.Я.

Відповідальний за випуск: д.т.н., доц. Лупенко С.А.

Затверджено на засіданні кафедри КС

Протокол № 7 від 18.01.2011 р.

Схвалено та рекомендовано до друку методичною комісією факультету комп’ютерно-інформаційних систем і програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя.

Протокол № 6 від 3.02.2011 р.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА №1	Ошибка! Закладка не определена.
ЛАБОРАТОРНА РОБОТА №2	17
ЛАБОРАТОРНА РОБОТА №3	26
ЛАБОРАТОРНА РОБОТА №4	29
ЛАБОРАТОРНА РОБОТА №5	39
ЛАБОРАТОРНА РОБОТА №6	48

ЛАБОРАТОРНА РОБОТА №1

Тема: Моніторинг вузлів мережі, серверів і активного мережевого обладнання засобами SNMP (ОС Windows 2003 Server, ОС Linux)

Мета роботи: одержати уміння та закріпити навички роботи з моніторингу вузлів мережі, серверів і активного мережевого обладнання засобами SNMP.

Теоретичні відомості

Simple Network Management Protocol – розроблений для систем, орієнтованих під операційну систему UNIX, він став фактично загальноприйнятим стандартом мережевих систем управління та підтримується переважною більшістю виробників мережевого устаткування в своїх продуктах. В силу своєї назви – простий протокол мережного управління – основним завданням при його розробці було добитися максимальної простоти його реалізації. У результаті виник протокол, що включає мінімальний набір команд, проте дозволяє виконувати практично весь спектр завдань управління мережевими пристроями - від отримання інформації про місцезнаходження конкретного пристрою, до можливості виробляти його тестування.

Основною концепцією протоколу є те, що вся необхідна для керування пристроєм інформація зберігається на самому пристрої – будь то сервер, модем або маршрутизатор – у так званій Адміністративній Базі Даних (МІВ – Management Information Base). МІВ представляє з себе набір змінних, що характеризують стан об'єкта управління. Ці змінні можуть відображати такі параметри, як кількість пакетів, оброблених пристроєм, стан його інтерфейсів, час функціонування пристрою і т.п. Кожен виробник мережевого устаткування, крім стандартних змінних, включає в МІВ будь-які параметри, специфічні для даного пристрою. Однак, при цьому не порушується принцип подання та доступу до адміністративної інформації - всі вони будуть змінними в МІВ. Тому SNMP як безпосередньо мережевий протокол надає тільки набір команд для роботи зі змінними МІВ.

Протокол SNMP (Simple Network Management Protocol, Простий протокол мережевого управління) – це протокол рівня 7 моделі OSI, використовуваний для віддаленого контролю і настройки мережевих пристроїв. SNMP дозволяє станціям мережевого управління переглядати і змінювати налаштування шлюзів, маршрутизаторів, комутаторів та інших мережевих пристроїв. SNMP може бути використаний для виконання багатьох тих функцій, які виконувалися через безпосередньо підключену консоль, або може бути використаний в рамках інтегрованого програмного забезпечення мережевого управління, такого як DView.

SNMP виконує наступні функції:

- Відправлення та прийом пакетів SNMP через протокол IP.
- Збір інформації про статус і поточної конфігурації мережевих пристроїв.
- Зміна конфігурації мережевих пристроїв.

Протокол SNMP був розроблений з метою перевірки функціонування мережевих маршрутизаторів і мостів. Згодом сфера дії протоколу охопила і інші мережеві пристрої, такі як хаби, шлюзи, термінальні сервери, LAN Manager сервера, машини під управлінням Windows NT і т.д. Крім того, протокол допускає можливість внесення змін у функціонування зазначених пристроїв.

SNMP – протокол контролю та діагностики, в зв'язку з чим, він розрахований на ситуації, коли порушується цілісність маршрутів, крім того в такій ситуації потрібно якомога менш вимогливий з апаратурі транспортний протокол, тому вибір був зроблений у бік UDP.

Але це не означає, що ніякий інший протокол не може переносити пакети SNMP. Таким може бути IPX протокол (наприклад, в мережах NetWare), також у виді транспорту можуть виступати карт Ethernet, осередки АТМ. Відмінною особливістю розглянутого протоколу є те, що передача даних здійснюється без встановлення з'єднання.

Порядок виконання роботи

Наведені в роботі приклади стосуються ОС Linux, але синтаксис команд аналогічний ПЗ для Windows.

1. На першому етапі виконання лабораторної роботи необхідно встановити програмне забезпечення. Програмне забезпечення можна отримати за адресою <http://net-snmp.sourceforge.net>

Установка пакету стандартна:

```
gunzip udc-snmp-3.5.3.tar.gz
tar -xvf udc-snmp-3.5.3.tar
cd udc-snmp-3.5.3
./configure
make
make install
```

Запуск демона (агента)

```
snmpd
```

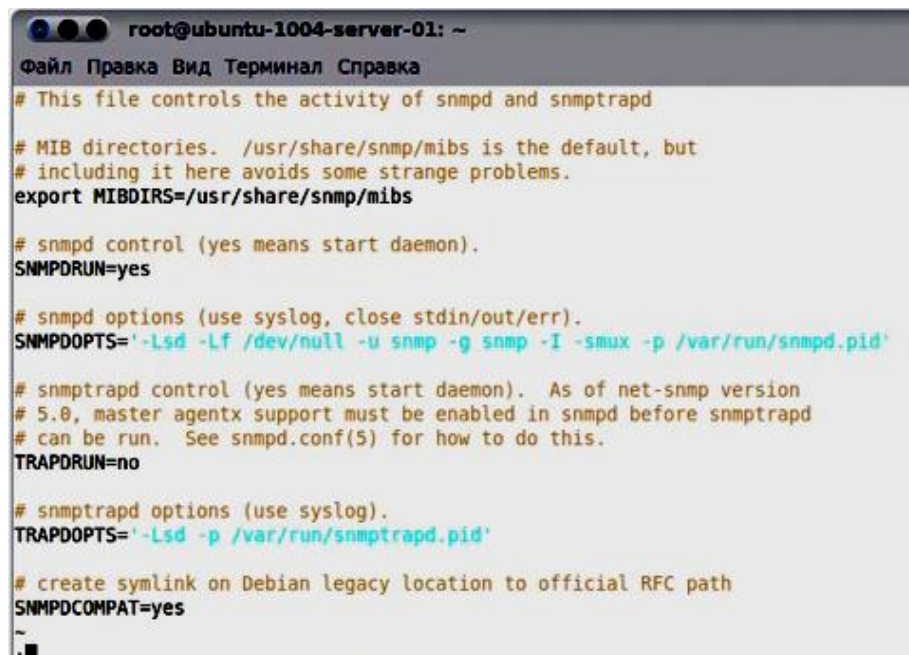
Після успішної інсталяції програмного забезпечення з'явилась доступність до програм:

```
snmpget
snmpset
snmpgetnext
snmpwalk
snmpbulkwalk
snmpcheck
snmpstat
snmpdelta
snmpnetstat
snmpstatus
snmptable
snmptrap
snmptranstat
і демону snmptrapd
```

2. Далі, після редагування файлу snmpd (рис.1), який знаходиться в /etc/default, виконати запуск SNMP агента. Це показано на рис.2.

Дана операція реалізовувалась за допомогою команди:

```
/etc/init.d/snmpd restart
```



```
root@ubuntu-1004-server-01: ~
Файл Правка Вид Терминал Справка
# This file controls the activity of snmpd and snmptrapd

# MIB directories. /usr/share/snmp/mibs is the default, but
# including it here avoids some strange problems.
export MIBDIRS=/usr/share/snmp/mibs

# snmpd control (yes means start daemon).
SNMPDRUN=yes

# snmpd options (use syslog, close stdin/out/err).
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'

# snmptrapd control (yes means start daemon). As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run. See snmpd.conf(5) for how to do this.
TRAPDRUN=no

# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'

# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes
~
:█
```

Рисунок 1 – Редагування файлу snmpd

```
root@ubuntu-1004-server-01: /etc/snmp
Файл Правка Вид Терминал Справка

Настроивается пакет libsensors4 (1:3.1.2-2) ...
Настроивается пакет libsnmp-base (5.4.2.1-dfsg@ubuntu1-0ubuntu2.1) ...
Настроивается пакет libsnmp15 (5.4.2.1-dfsg@ubuntu1-0ubuntu2.1) ...

Настроивается пакет snmp (5.4.2.1-dfsg@ubuntu1-0ubuntu2.1) ...
Настроивается пакет snmpd (5.4.2.1-dfsg@ubuntu1-0ubuntu2.1) ...
update-rc.d: warning: snmpd stop runlevel arguments (1) do not match LSB Default
-Stop values (0 1 6)
 * Starting network management services:
Настроивается пакет fancontrol (1:3.1.2-2) ...

Настроивается пакет lm-sensors (1:3.1.2-2) ...

Обрабатываются триггеры для libc-bin ...
ldconfig deferred processing now taking place
Обрабатываются триггеры для python-central ...
root@ubuntu-1004-server-01:~# vi /etc/default/snmpd
root@ubuntu-1004-server-01:~# cd /etc/snmp/
root@ubuntu-1004-server-01:/etc/snmp# vi snmpd.conf
root@ubuntu-1004-server-01:/etc/snmp# /etc/init.d/snmpd start
 * Starting network management services:
root@ubuntu-1004-server-01:/etc/snmp#
```

Рисунок 2 – Запуск SNMP агента

3. Наступним кроком є виконання команди snmpwalk, яка отримує дерево управління значеннями за допомогою SNMP GetNext запитів (рис.3):

Snmpwalk -v 2c -c publicSec 127.0.0.1 .1

```
root@ubuntu-1004-server-01: /etc/snmp
Файл Правка Вид Терминал Справка

HOST-RESOURCES-MIB::hrSWRunID.38 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.40 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.41 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.42 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.43 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.44 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.45 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.159 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.164 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.177 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.181 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.195 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.196 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.239 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.245 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.467 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.468 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.483 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.485 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.487 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.492 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunID.493 = OID: SNMPv2-SMI::zeroDotZero
^C
root@ubuntu-1004-server-01:/etc/snmp#
```

Рисунок 3 – Виконання команди snmpwalk

4. Зверніть увагу також на поради щодо безпеки мережі. В першу чергу слід приділити увагу налаштуванню фаєрволу. Також змінити встановлені за замовчуванням імена груп. Було б також корисним жорстко зафіксувати адреси машин (менеджерів), із яких дозволяється опитування агентів.

ЛАБОРАТОРНА РОБОТА №2

Тема: Віддалена робота (ОС Windows 2003 Server, ОС Linux)

Мета роботи: одержати уміння по налаштуванню віддаленої роботи ПК.

Теоретичні відомості

За допомогою віддаленого адміністрування можна керувати програмою так само, як ніби вона працює безпосередньо на вашому комп'ютері. Можна інстальювати, налаштовувати програми, переглядати журнали, планувати завдання оновлення, завдання антивірусної перевірки тощо.

Radmin – одна з найкращих програм віддаленого адміністрування для платформи Windows, яка дозволяє повноцінно працювати одразу на кількох віддалених комп'ютерах за допомогою звичайного графічного інтерфейсу.

Загальні завдання віддаленого адміністрування:

- Підключення до іншого комп'ютера за допомогою підключення до віддаленого робочого столу
- Підключення до робочого столу при ввімкнутому брандмауері Windows
- Використання служби «Віддаленої допомоги» Windows для надання допомоги в разі виникнення неполадок з комп'ютером
- Надання службі віддаленої допомоги Windows доступу через брандмауер

Розглянемо, як можна реалізувати кожне із перерахованих завдань.

Підключення до іншого комп'ютера за допомогою підключення до віддаленого робочого столу

За допомогою підключення до віддаленого робочого столу можна увійти до іншого комп'ютера, який підключено до тієї самої мережі або до Інтернету. Таким чином можна зі свого домашнього комп'ютера працювати з усіма програмами, файлами та мережними ресурсами робочого комп'ютера.

Для підключення до віддаленого комп'ютера необхідно:

1. Увімкнути комп'ютер та підключити його до мережі.

2. Увімкнути підключення до віддаленого робочого столу: Пуск – Усі програми або Програми – Стандартні – Підключення до віддаленого робочого столу. Щоб швидко відкрити підключення до віддаленого робочого столу, можна також відкрити меню «Пуск» і ввести **mstsc** у полі пошуку.

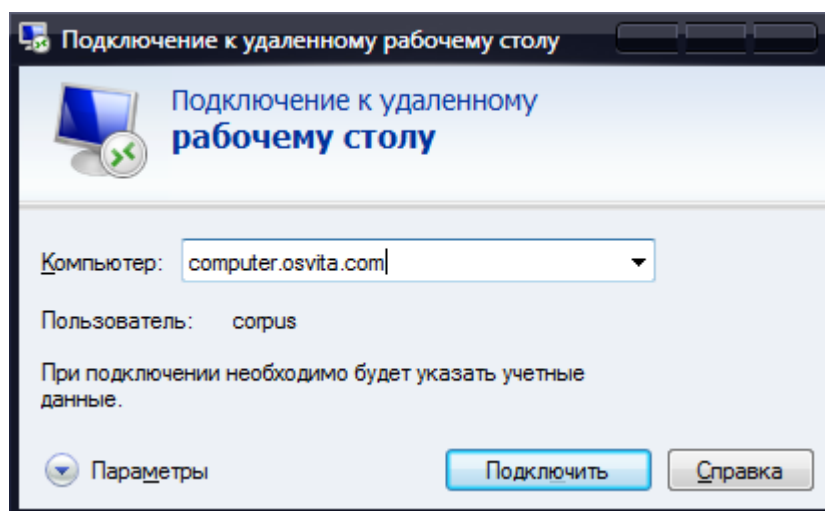


Рисунок 1 – Вікно підключення до віддаленого робочого столу

3. Отримати мережевий доступ до віддаленого комп'ютера (можливий доступ через Інтернет) і дозвіл на підключення. Щоб отримати дозвіл на підключення, ваше ім'я повинно бути у списку користувачів.

4. При натисненні випадаючого меню «Параметри», з'являються додаткові можливості та налаштування нового підключення або ж редагування існуючого. В закладці «Общие» слід ввести ім'я віддаленого комп'ютера та користувача, після чого виконати збереження поточних параметрів підключення (рис.2).

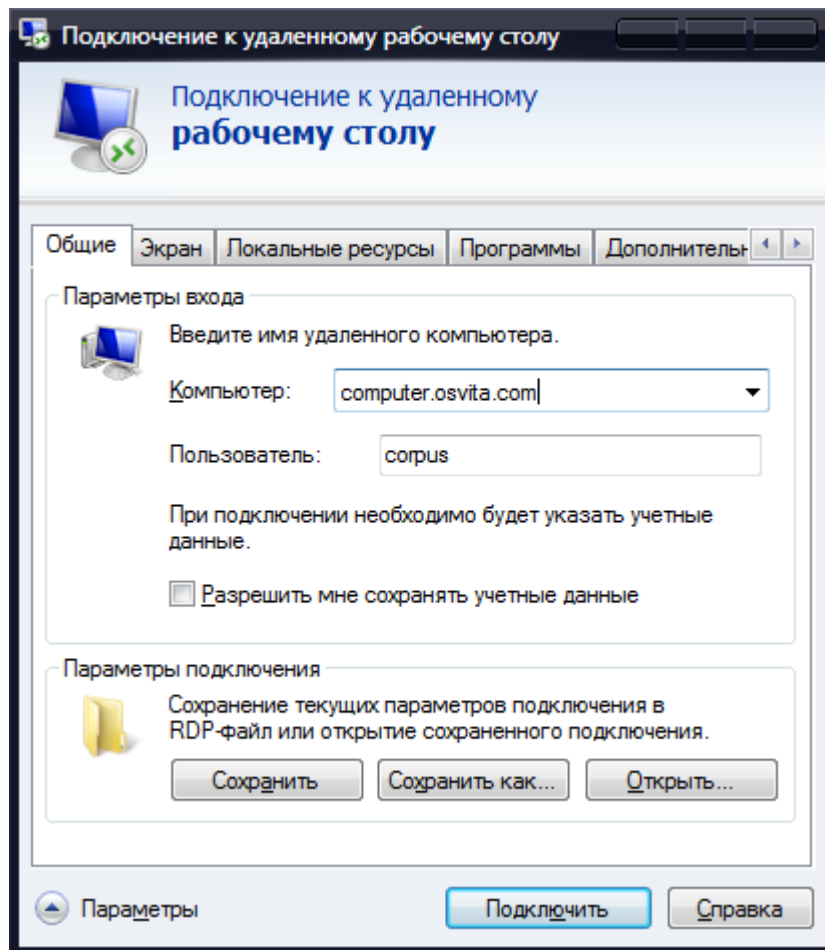


Рисунок 2 – Вікно параметрів підключення до віддаленого робочого столу

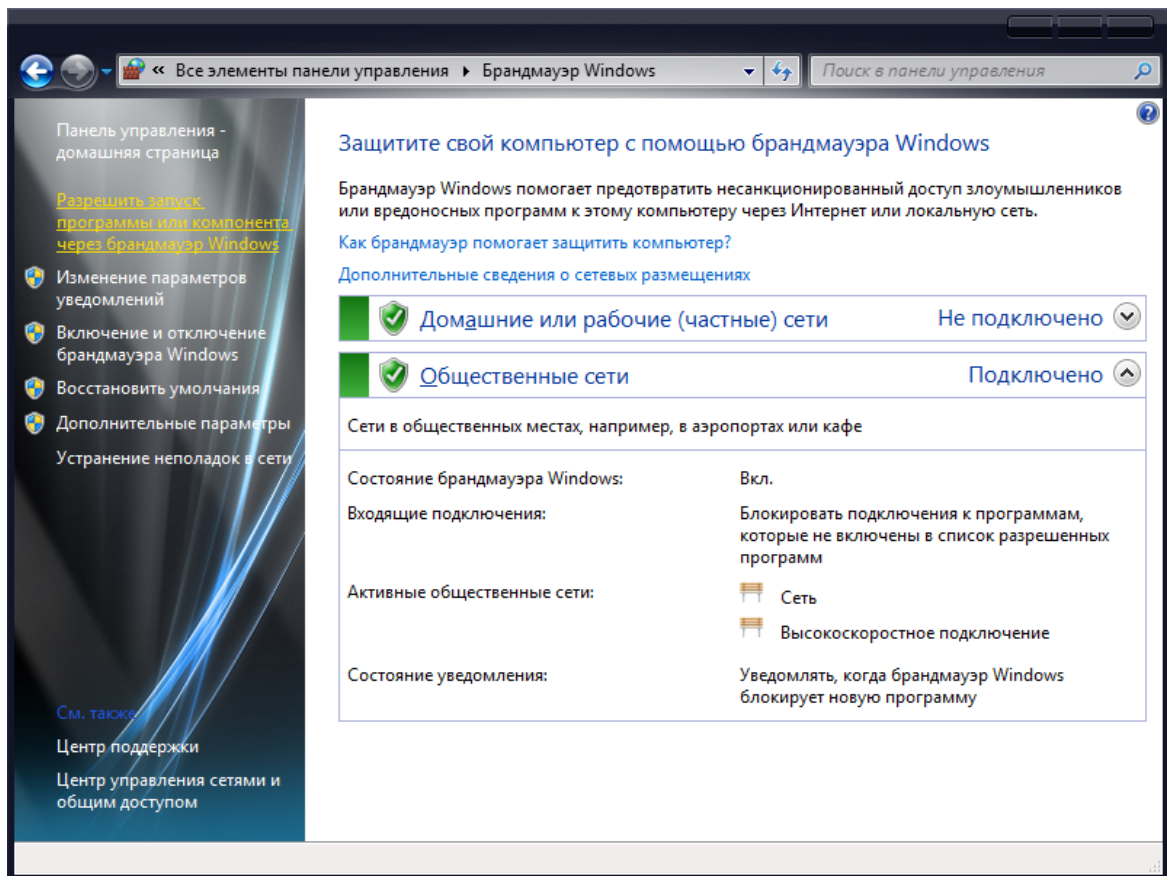
5. Натиснути кнопку «Подключить» та виконати підключення до віддаленого робочого столу. У новому вікні обрати комп'ютер, до якого виконувалось підключення, ввести пароль, натиснути «ОК».

Підключення до робочого столу при ввімкнутому брандмауері Windows

Оскільки брандмауер Windows обмежує зв'язок між комп'ютером та Інтернетом, можливо, потрібно буде змінити його параметри для належної роботи служби «Підключення до віддаленого робочого столу».

1. Відкрийте діалогове вікно «Брандмауер Windows». Для цього виберіть Пуск – Панель керування – Безпека – Брандмауер Windows.

2. Виберіть пункт «Дозволити програмі працювати крізь брандмауер Windows». Якщо потрібно, введіть пароль адміністратора або надайте підтвердження.

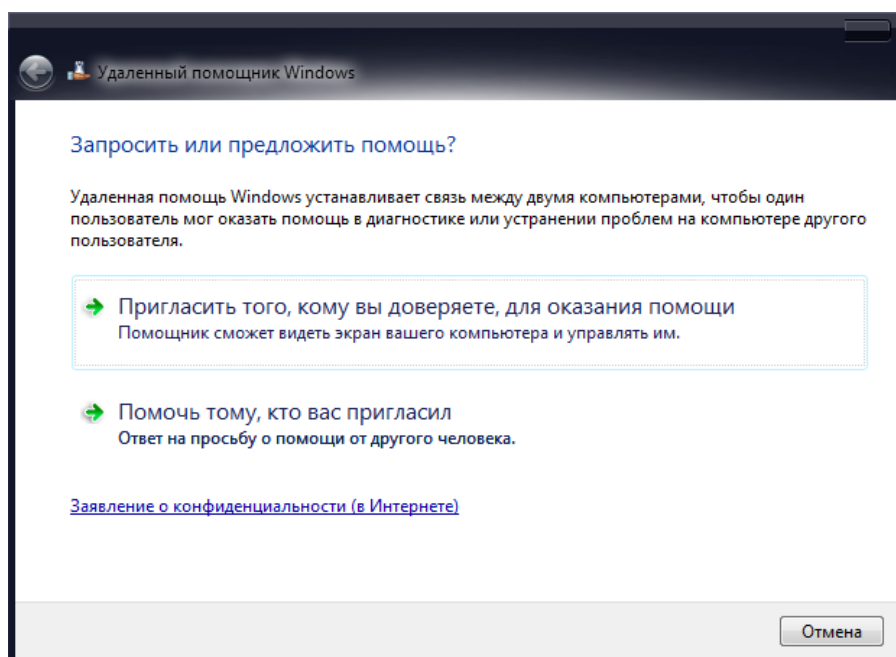


3. У розділі «Програма або порт» встановіть прапорець поруч із пунктом «Віддалений робочий стіл», після чого натисніть ОК.

Використання служби «Віддаленої допомоги» Windows для надання допомоги в разі виникнення неполадок з комп'ютером

Завдяки «Віддаленій допомозі» Windows можна підключитися до комп'ютера іншого користувача і допомогти йому з будь-якої відстані в разі виникнення неполадок із комп'ютером.

1. Відкрийте службу віддаленої допомоги. Для цього: Пуск - Усі програми – Обслуговування – Служба віддаленої допомоги Windows.



2. Дотримуйтесь інструкцій.

Надання служби віддаленої допомоги Windows доступу крізь брандмауер

Оскільки брандмауер може обмежувати зв'язок між комп'ютером та Інтернетом, можливо, для використання служби віддаленої допомоги Windows потрібно буде змінити настройки брандмауера.

1. Відкрийте діалогове вікно «Брандмауер Windows». Для цього: Пуск – Панель керування – Безпека – Брандмауер Windows.
2. Натисніть кнопку «Дозволити програмі працювати крізь брандмауер Windows». Якщо потрібно, введіть пароль адміністратора або надайте підтвердження.
3. У розділі «Винятки» встановіть прапорець «Віддалена допомога» і ОК.

ЛАБОРАТОРНА РОБОТА № 3

Тема: Організація сервера мережевої файлової системи (CIFS, SMB, SMB2, NFS)

Мета роботи: одержати уміння по організації сервера мережевої файлової системи.

Теоретичні відомості

У випадку локальної мережі, ви можете бути зацікавленими в обміні даними з іншими комп'ютерами. TCP/IP сам по собі дозволяє користуватись звичайним FTP або SSH копіюванням файлів, але це не дозволить, скажімо, переглядати файли що знаходяться на Slackware з допомогою Network Neighborhood або My Network Places на Windows-машині. Також, існують зручніші способи копіювати файли між UNIX- машинами.

Мається на увазі *мережева файлова система*, яка дозволяє прозорий доступ до файлів на інших комп'ютерах. Прозорий, означає що відпадає необхідність якихось додаткових дій для того щоб звернутися до файлів на іншій машині, з користувачького боку це виглядає так, ніби ці файли знаходяться на його власному комп'ютері.

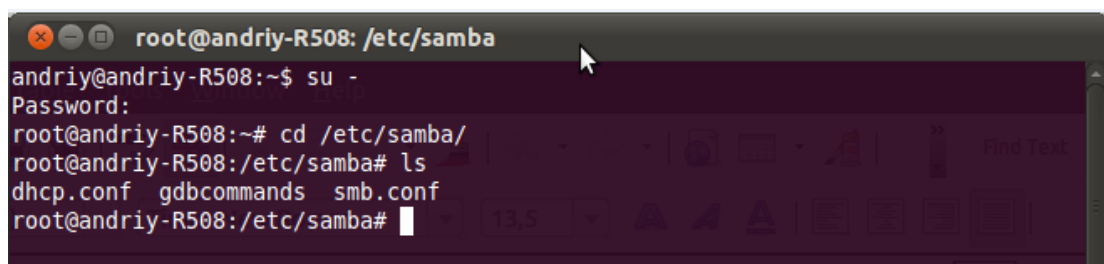
Найживванішими мережевими файловими системами у Linux є SMB (впроваджена Samba сервером) та NFS.

SMB (скорочення від Server Message Block) походить від старшого NetBIOS протоколу, що використовувався раніше IBM для власної LAN Manager програми. Майкрософт завжди був досить зацікавленим у NetBIOS і його спадкоємцях, NetBEUI, SMB та CIFS. Samba проект бере початок у 1991 році, коли вперше втілено зв'язок між IBM ПК і Юнікс сервером завдяки NetBIOS протоколу. На сьогоднішній день SMB протокол використовується, в більшості випадків, для розподілу файлів і друкування через мережу між Юнікс і Віндовс комп'ютерами.

NFS (Network File System) була вперше розроблена Sun для власного втілення Юніксу (Solaris). Хоча дещо легше налагодити ніж SMB, NFS, тим не менш значно менш безпечний. Найголовніша небезпека NFS полягає у тому, що без особливих труднощів можливо підробити користувачькі і групові ID з однієї машини на іншу. NFS не є аутентифікаційним протоколом. Очікується, що майбутні версії NFS, принаймні, посилять безпеку.

Порядок виконання роботи

На першому етапі виконання лабораторної роботи слід провести редагування файлу smb.conf, що є конфігураційним файлом SMB протоколу. Даний файл знаходиться в каталозі /etc/samba/ (рис.1).



```
root@andriy-R508: /etc/samba
andriy@andriy-R508:~$ su -
Password:
root@andriy-R508:~# cd /etc/samba/
root@andriy-R508:/etc/samba# ls
dhcp.conf  gdbcommands  smb.conf
root@andriy-R508:/etc/samba#
```

Рисунок 1 – Вміст каталогу /etc/samba/

Для редагування конфігураційного файлу smb.conf необхідно виконати команду в каталозі /etc/samba/:

```
nano smb.conf
```

Після виконання команди відкриється вікно текстового редактора nano з текстовим вмістом. У файлі smb.conf потрібно додано текст:

```
[global]
# workgroup = NT-Domain-Name or Workgroup-Name, eg: LINUX2
workgroup = MYGROUP
```

За допомогою даного тексту буде додано назву робочої групи, яка повинна відповідати дійсності (рис.2).

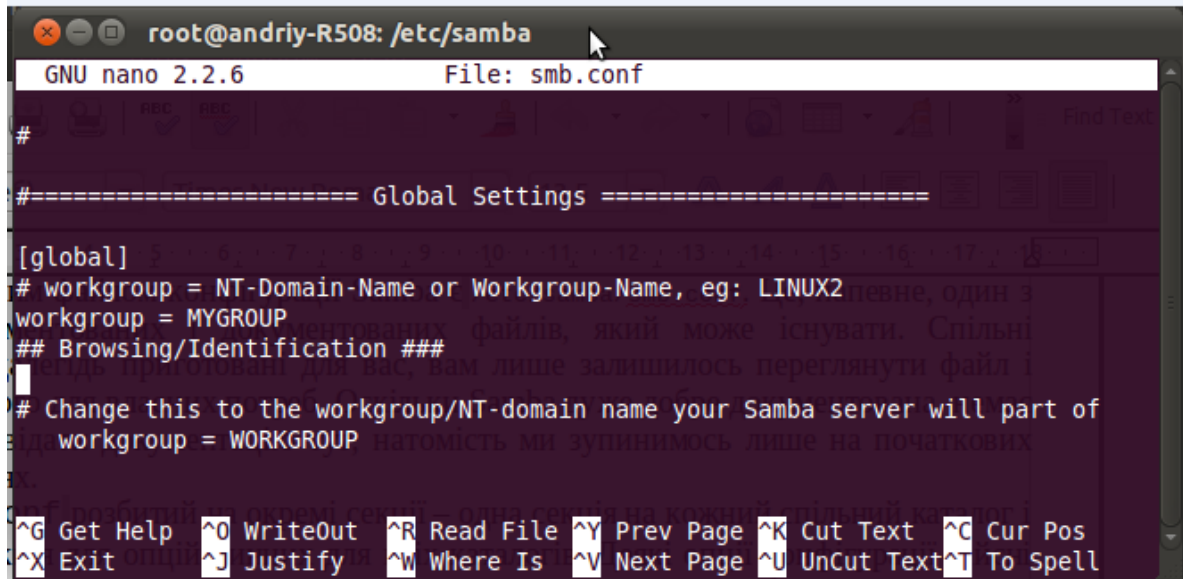
A screenshot of a terminal window showing the nano text editor editing the file /etc/samba/smb.conf. The terminal title is 'root@andriy-R508: /etc/samba'. The editor header shows 'GNU nano 2.2.6' and 'File: smb.conf'. The visible content includes a comment line '# workgroup = NT-Domain-Name or Workgroup-Name, eg: LINUX2' followed by the configuration line 'workgroup = MYGROUP'. The cursor is positioned at the end of the 'workgroup = MYGROUP' line. The bottom status bar shows various keyboard shortcuts like '^G Get Help', '^O WriteOut', etc.

Рисунок 2 – Додання робочої групи

Наступним кроком буде введення назви власної Slackware машини, що відобразатиметься у Network Neighborhood (або My Network Places) теці у Windows (рис.3):

```
# server string is the equivalent of the NT Description field
server string = Samba Server
```

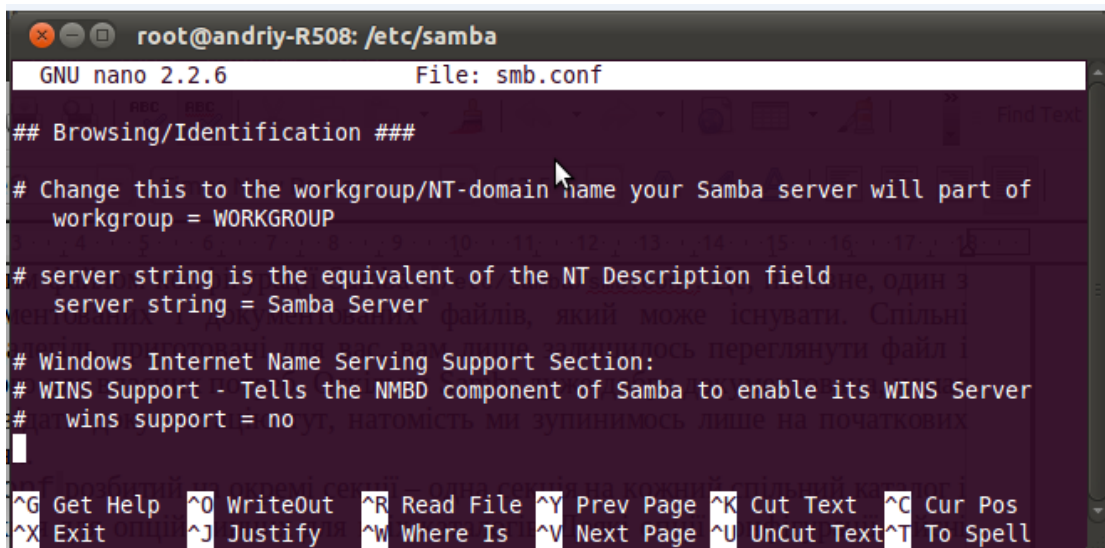
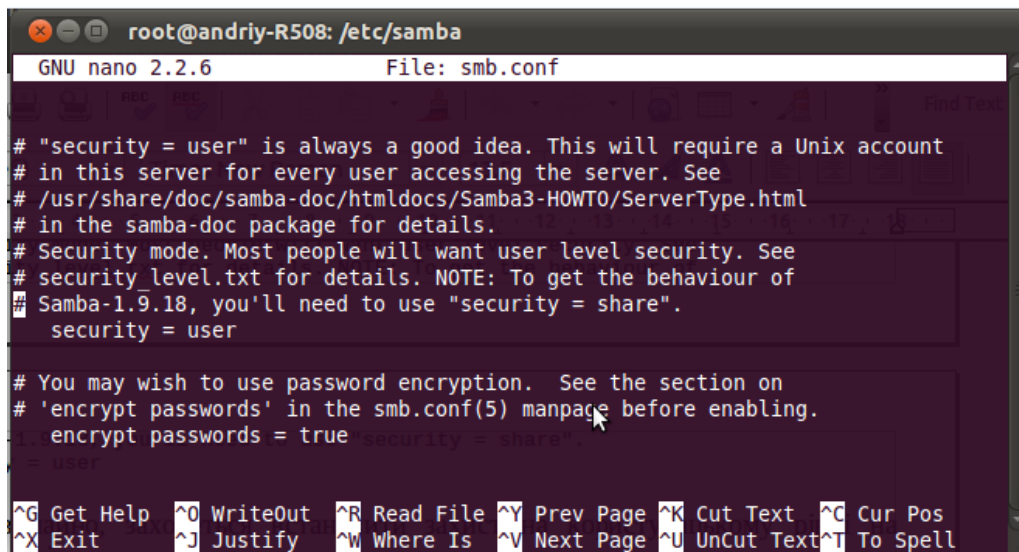
A screenshot of a terminal window showing the nano text editor editing the file /etc/samba/smb.conf. The terminal title is 'root@andriy-R508: /etc/samba'. The editor header shows 'GNU nano 2.2.6' and 'File: smb.conf'. The visible content includes the comment line '# server string is the equivalent of the NT Description field' followed by the configuration line 'server string = Samba Server'. The cursor is positioned at the end of the 'server string = Samba Server' line. The bottom status bar shows various keyboard shortcuts like '^G Get Help', '^O WriteOut', etc.

Рисунок 3 – Додавання назви власної Slackware машини

Останнім налаштуванням файлу конфігурації smb.conf буде налаштування захисту на користувачькому рівні на Slackware системі (рис.4):

```
# You may wish to use password encryption. Please read
# ENCRYPTION.txt, Win95.txt and WinNT.txt in the Samba
# Do not enable this option unless you have read those documents
encrypt passwords = yes
```



```
root@andriy-R508: /etc/samba
GNU nano 2.2.6 File: smb.conf

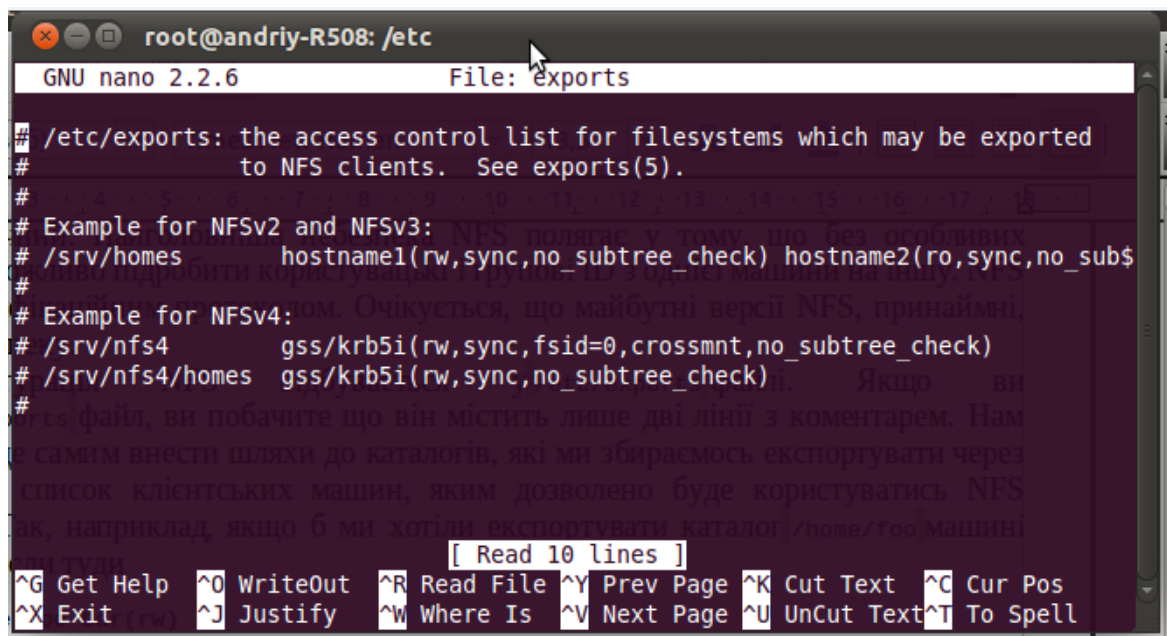
# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/Samba3-HOWTO/ServerType.html
# in the samba-doc package for details.
# Security mode. Most people will want user level security. See
# security level.txt for details. NOTE: To get the behaviour of
# Samba-1.9.18, you'll need to use "security = share".
security = user

# You may wish to use password encryption. See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
encrypt passwords = true

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Рисунок 4 – Налаштування захисту на користувачькому рівні

Конфігурацію NFS слід виконати у /etc/exports файлі. Далі треба відкрити exports файл, який містить лише два рядки з коментарем. Після цього було внести шляхи до каталогів, які потрібно експортувати через NFS, також список клієнтських машин, яким дозволяється користуватись NFS ресурсами. Вміст exports файлу показано на рис.5.



```
root@andriy-R508: /etc
GNU nano 2.2.6 File: exports

# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_sub
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#

[ Read 10 lines ]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Рисунок 5 – Вміст exports файлу

Далі необхідно виконати експорт каталогу безпосередньо з командного рядка на сервері командою:

```
# exportfs -o rw bar:/home/foo
```

Даний рядок виконає експорт /home/foo каталога комп'ютера bar із правами на читання і запис.

ЛАБОРАТОРНА РОБОТА №4

Тема: Встановлення і налаштування веб-сервера (Windows, Linux)

Мета роботи: набутиати вмінь в організації WEB-сервера.

1. Встановлення веб-сервера (Linux Slackware 10.2.)

В описі використано такі версії:

Apache - 2.0.58

MySQL - 5.0.22

PHP - 5.1.4

Новіші версії програмного забезпечення можна знайти на сайтах:

<http://www.apache.org>

<http://www.php.net>

<http://www.mysql.com>

Почнемо з того, що завантажимо усе програмне забезпечення:

```
#wget http://mirrors.ccs.neu.edu/Apache/dist/httpd/httpd-2.0.58.tar.bz2
```

```
#wget http://mysql.dn.ru/Downloads/MySQL-5.0/mysql-5.0.22.tar.gz
```

```
#wget http://ru.php.net/get/php-5.1.4.tar.bz2/from/this/mirror
```

Установка Apache

Розархівовуємо архів:

```
#tar -xjvf httpd-2.0.58.tar.bz2
```

Далі заходимо в директорію, яку ми щойно розпакували:

```
#cd httpd-2.0.58/
```

Починаємо встановлення:

```
#!/configure --prefix=/usr/local/httpd (--prefix=/user/local/httpd – описує шлях встановлення)
```

```
#make
```

```
#make install
```

Потім потрібно перейти в директорію /usr/local/httpd/conf і відредагувати файл httpd.conf:

```
#cd /usr/local/httpd/conf/
```

```
#nano httpd.conf
```

Знаходимо та змінюємо рядки в конфігураційному файлі:

```
ServerAdmin eliziy@example.com
```

```
(замість eliziy@example.com повинна бути ваша електронна адреса)
```

```
ServerName www.example.com:80
```

```
(www.example.com:80 – тут треба вказати адресу сервера і через двокрапку порт)
```

Знаходимо рядки:

```
<Directory />
```

```
Options FollowSymLinks
```

```
AllowOverride None
```

```
</Directory>
```

і змінюємо їх на:

```
<Directory />
  Options None
  AllowOverride None
</Directory>
```

Знаходимо:

```
<Directory "usr/local/httpd/htdocs">
  Options Indexes FollowSymLinks
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
```

змінюємо на:

```
<Directory "/usr/local/httpd/htdocs">
  Options None
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
```

Далі приховуємо інформацію про версію Apache і трохи захищаємо його. Для цього редагуємо в конфігураційному файлі наступні записи:

```
ServerTokens Prod
ServerSignature Off
User nobody
Group nobody
Timeout 45
UserDir disable
```

Виставляємо потрібні права доступу:

```
#cd /usr/local/httpd/
#chown root . bin conf logs
#chgrp root . bin conf logs
#chmod 755 . bin conf logs
#chown root /usr/local/httpd/bin/httpd
#chgrp root /usr/local/httpd/bin/httpd
#chmod 511 /usr/local/httpd/bin/httpd
```

Встановлення MySQL:

Слід додати нову групу і користувача в систему перед початком встановлення:

```
#groupadd mysql
#useradd -g mysql mysql
```

Розпаковуємо архів і переходимо в одержану директорію:

```
#tar -zxvf mysql-5.0.22.tar.gz
#cd mysql-5.0.22/
```

Приступаємо до конфігурування і встановлення:

```
./configure --prefix=/usr/local/mysql (--prefix=/user/local/mysql – описує шлях встановлення)
#make
#make install
```

Копіюємо конфігураційний файл:

```
#cp support-files/my-medium.cnf /etc/my.cnf
```

Переходимо в директорію /usr/local/mysql і виконуємо там установку адміністративних таблиць:

```
#cd /usr/local/mysql  
#bin/mysql_install_db -user=mysql
```

Виставляємо потрібні права доступу:

```
#chown -R root .  
#chown -R mysql var  
#chgrp -R mysql .
```

Тепер потрібно запустити сервер, підключитися до нього і змінити пароль:

```
#!/usr/local/mysql/bin/mysqld_safe &  
#!/usr/local/mysql/bin/mysql -u root  
  
mysql> use mysql;  
mysql> set password for 'root'@'localhost' = password('passwd');  
mysql> flush privileges;  
mysql> \q
```

Замість слова passwd напишіть свій пароль.

Установка MySQL сервера закінчена.

Встановлення PHP:

Розпаковуємо архів:

```
#tar -xjvf php-5.1.4.tar.bz2
```

Переходимо в отриману директорію:

```
#cd php-5.1.4/
```

Конфігурування та встановлення:

```
#!/configure --with-apxs2=/usr/local/httpd/bin/apxs --with-mysql=/usr/local/mysql  
#make  
#make install
```

Копіюємо конфігураційний файл:

```
#cp php.ini-recommended /usr/local/lib/php.ini
```

Відкриваємо і трохи редагуємо конфігураційний файл Apache:

```
#nano /usr/local/httpd/conf/httpd.conf
```

Додаємо на початок файлу рядок:

```
AddType application/x-httpd-php .php  
AddType application/x-httpd-php .phtml  
AddType application/x-httpd-php-source .phps
```

Шукаємо рядок "DirectoryIndex". В кінець цього рядка додаємо значення index.php. Рядок DirectoryIndex має тепер виглядати так:

DirectoryIndex index.html index.html.var index.php

Встановлення всього програмного забезпечення завершено. Залишилось запустити, якщо у вас не заведений Apache, або перезавантажити його для того, щоб вступили в силу внесені нами нові параметри:

```
#!/usr/local/httpd/bin/apachectl start - для запуску сервера
#!/usr/local/httpd/bin/apachectl restart - для перезавантаження сервера
```

Перевіримо, як працює все те, що ми встановили. Для цього потрібно написати скрипт на PHP:

```
#cd /usr/local/httpd/htdocs/
#nano mysql.php

<?
$dblocation="127.0.0.1";

$dbuser="root";

$dbpasswd="passwd";

$dbcnx=mysql_connect($dblocation, $dbuser, $dbpasswd);

if(!$dbcnx)
{
    echo("Не вдалося підключитися до бази даних");

    exit();
}

$dbq=mysql_query("select version()");

echo(mysql_result($dbq,0));
?>
```

У змінній "\$dbpasswd" замініть параметр "passwd" на пароль від вашої бази даних (MySQL).

Тепер відкриваємо будь-який браузер і переходимо за посиланням <http://127.0.0.1/mysql.php>:

```
#lynx http://127.0.0.1/mysql.php
```

Встановлення, налаштування і тестування веб-сервера завершено.

2. Встановлення IIS (Windows)

Нижче наведено основні кроки при встановленні IIS:

- В Control Panel (Панель управління) клацніть на значку Add or Remove Programs (Установка і видалення програм) для відкриття діалогового вікна.
- Клацніть на кнопці Add/Remove Windows Components (Установка/видалення компонентів Windows) для запуску майстра компонентів Windows (Windows Components Wizard).
- Клацніть на компоненті Application Server (Сервер додатків), після чого натисніть на кнопку Details (Подробиці).
- Компоненти IIS розташовуються в області Internet Information Services (IIS).

Якщо відмітити опцію IIS, то будуть встановлені тільки компоненти за замовчуванням. Для установки додаткових компонентів їх слід вказати вручну.

Компоненти IIS

При натисненні на кнопку Details (Подробиці) з'явиться список компонентів IIS (див. рис. 1.1).

Виберіть усі необхідні компоненти, потім три рази натисніть на кнопку ОК, щоб повернутися до головного вікна Windows Components (Компоненти Windows). Після натиснення на кнопку Next (Далі) вставте компакт-диск Windows 2003, якщо він ще не знаходиться в дисководі.

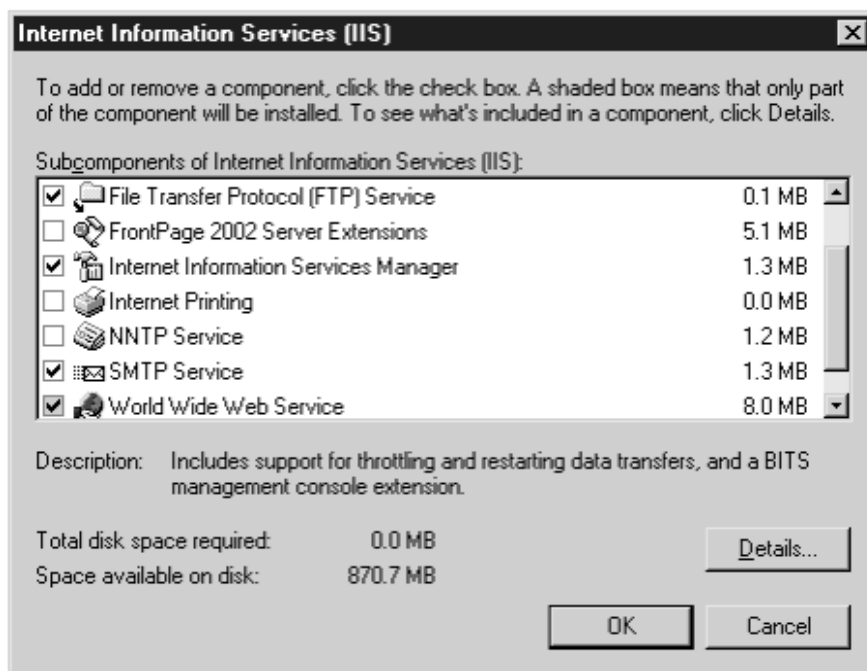


Рисунок 1.1 – Компоненти IIS

Серверні розширення Background Intelligent Transfer Service (BITS)

Компонент **Серверні розширення BITS** складається з двох частин: фільтру ISAPI (Internet Server Application Programming Interface) – інтерфейсу прикладного програмування інтернет-сервера для відвантаження даних через BITS – і оснащення серверних розширень.

Примітка. Фільтр ISAPI, по суті, є динамічно підключеною бібліотекою (DLL), яка перевіряє вхідний код HTTP.

BITS дозволяє передавати файли у фоновому режимі, щоб не переривати роботу користувачів, що знаходяться в системі. Передача файлів контролюється для обмеження використовуваної смуги пропускання каналу зв'язку. У разі порушення з'єднання передача буде відновлена при його повторній установці. Після закінчення передачі файлу додаток, що просив цей файл, отримає повідомлення.

BITS встановлюється разом з Windows 2003 і WindowsXP і існує у вигляді окремої надбудови в Windows 2000.

Загальні файли (Common Files)

Для роботи IIS потрібна установка цього компонента.

Служба протоколу передачі файлів (FTP)

Компонент не встановлюється за замовчуванням. Служба FTP дозволяє створювати FTP-сервер, використовуваний для відвантаження або завантаження файлів.

Серверні розширення FrontPage 2002

Компонент потрібний для відвантаження веб-сайтів користувачів безпосередньо з Microsoft FrontPage або Visual InterDev. Він дозволяє розробникам веб-сторінок здійснювати контроль на веб-сервері, тому установка цього компонента є загрозою безпеки.

Диспетчер IIS (Internet Information Services Manager)

Опції цього компонента дозволяють налаштувати і відкривати для загального доступу принтери через HTTP, аналогічно функціям веб-друку в Windows 2000 Server. Для WS03 ця служба є обов'язковою.

Служба NNTP

Компонент встановлює сервер новин для створення груп новин.

Служба SMTP

Служба SMTP дозволяє відправляти електронну пошту з сервера IIS. Використовується для веб-сайтів, що здійснюють відправку електронної пошти.

Служба WWW

Служба WWW є основною службою, що забезпечує роботу служб HTTP. Містить декілька компонентів.

Active Server Pages (ASP). Встановлює динамічні бібліотеки ASP і інші файли для роботи ASP на веб-сервері. Компонент встановлюється завжди, хоча відключений за замовчуванням.

Internet Data Connector (IDC). Реалізує роботу з базою даних на веб-сайті.

Remote Administration (HTML). Дозволяє виконувати віддалене адміністрування IIS через веб-браузер. Відрізняється від попередніх версій по HTML-адмініструванню IIS, які дозволяли адміністрування тільки одного сервера.

Remote Desktop Web Connection (Підключення до віддаленого робітника столу). Компонент встановлює елементи управління ActiveX для підключення браузеру Internet Explorer до сеансу сервера терміналу з використанням сторінок, що надаються. Цей компонент в Windows 2000 називався Terminal Services Advanced Client.

Server Side Includes (Включення серверної частини). Компонент забезпечує підтримку включень серверної частини і встановлюється завжди.

WebDAV Publishing. Є набором розширень HTTP, що дозволяє користувачам здійснювати доступ і управляти файлами в опублікованих з його допомогою каталогах на веб-сервері. Компонент встановлюється завжди.

World Wide Web Service (Служба WWW). Компонент є ядром додатку служби WWW. Без нього не можлива робота багатьох компонентів IIS.

Служби IIS

Існує декілька служб для підтримки IIS, їх перелік приведено в панелі управління службами в WS03. Набір служб залежить від встановлених компонентів IIS. Якщо компонент не встановлений, то пов'язана з ним служба в панелі управління службами не відображається.

Служба **IIS Admin** є головною службою адміністрування IIS, інші служби залежать від неї. При зупинці служби інші служби IIS будуть також зупинені.

FTP Publishing. Забезпечує роботу FTP-сервера в IIS.

World Wide Web Publishing. Забезпечує роботу веб-сервера в IIS.

Simple Mail Transfer Protocol (SMTP). Забезпечує роботу сервера SMTP в IIS.

Network News Transfer Protocol (NNTP). Забезпечує роботу NNTP-сервера у IIS.

HTTP SSL. Потрібна для виконання службою WWW Publishing функції сертифікації SSL.

Порада. Служби пов'язані між собою таким чином, що службу, для функціонування якої потрібна робота іншої служби, не можна включити без другої служби. Ці залежності показані на вкладці Dependencies вікна Properties (Властивості) служби.

Структура каталогів IIS

Основні компоненти IIS розміщені в каталозі %systemroot%\System32\inetsrv. Структура каталогів inetsrv показана в наступній таблиці.

Каталог	Описание
ASP Compiled Templates	Содержит используемый шаблон ASP.
History	Содержит историю изменений метабазы, позволяющую выполнять откат изменений в метабазе.
iisamdpwd	Содержит ASP-страницы, относящиеся к аутентификации IIS Admin.
MetaBack	Каталог по умолчанию для резервных файлов метабазы.

Веб-сайт адміністрування

У IIS 6 веб-сайт адміністрування дозволяє управляти усім сервером Windows з локального або віддаленого веб-браузеру. Веб-сайт адміністрування розміщений в каталозі %systemroot%\System32\ServerAppliance. Він функціонує через SSL, використовуючи порт 8098 за замовчуванням. Для доступу до веб-сайту адміністрування введіть в рядку адреси браузеру https://ім'я_комп'ютера:8098 (де ім'я_комп'ютера є ім'ям комп'ютера, який необхідно адмініструвати).

Файли довідки IIS

Усі файли довідки IIS 6 переміщені в централізоване місце розташування разом з іншими файлами довідки Windows. Це папка %systemroot%\help\iishelp. Найпростішим способом виклику довідки IIS є вибір команди Help/Help Topics (Довідка/Виклик довідки) в консолі MMC.

Каталог Inetpub

Каталог Inetpub є основним каталогом файлів IIS. У ньому розташовані каталоги з вмістом кожної встановленої служби. Шлях за замовчуванням для каталогу Inetpub – C:\Inetpub. Каталог Inetpub містить наступні підкаталоги.

Каталог	Описание
AdminScripts	Содержит сценарии Visual Basic, используемые для администрирования сервера IIS.
ftproot	Каталог верхнего уровня службы FTP.
mailroot	Каталог верхнего уровня службы SMTP.
nntpfile	Каталог верхнего уровня службы NNTP.
wwwroot	Каталог верхнего уровня веб-сайта по умолчанию.

Облікові записи в IIS

Оскільки функціонування усіх компонентів WS03 розглядається з точки зору безпеки, і для доступу потрібний обліковий запис, IIS встановлює дві облікові записи і одну групу у базу цих облікових записів для використання їх в роботі. Ці елементи дозволяють IIS виконувати програми і робочі процеси, а користувачам – здійснювати доступ до сайту. Нижче приведена детальніша інформація.

IUSR_COMPUTERNAME

Обліковий запис забезпечує анонімний доступ до веб-сайту при підключенні користувача до веб-сторінки без представлення вхідних даних. Такий користувач за замовчуванням є членом групи Guest (Гість).

IWAM_COMPUTERNAME

Обліковий запис використовується для запуску робочих процесів і є членом групи IIS_WPG.

IIS_WPG

Члени цієї групи можуть запускати робочі процеси. Будь-який обліковий запис, що виконує робочі процеси, має бути членом цієї групи. Це обліковий запис з низьким рівнем безпеки, що має права мережевої служби. Процеси, що використовують рівень прав Network Service (Мережева служба), здійснюють доступ до сервера так, як ніби вони знаходилися поза сервером, і тому не мають прямого доступу до операційної системи.

Ці процеси можна проглянути в консолі MMC Computer Management (Управління комп'ютером) панелі Administrative Tools (Адміністрування). Для відкриття списку Users and Groups (Користувачі і групи) виконайте наступні дії.

1. У меню Start (Пуск) виберіть Administrative Tools\Computer Management (Адміністрування\Управління комп'ютером).
2. Список користувачів і груп міститься у вікні Local Users and Groups (Локальні користувачі і групи) консолі Computer Management (Управління комп'ютером).
3. Якщо комп'ютер є контролером домена, список користувачів і груп розташовується у вікні Active Directory Users And Computers (Комп'ютери і користувачі Active Directory) панелі Administrative Tools (Адміністрування).

ЛАБОРАТОРНА РОБОТА №5

Тема: Встановлення і налаштування FTP-сервера (ОС Windows Server, ОС Linux)

Мета: вивчення можливостей ОС Linux та Windows Server для побудови FTP-сервера в локальній мережі.

Теоретичні відомості

Файлова служба мережі на основі протоколу FTP (File Transfer Protocol) являє собою одну з найбільш ранніх служб, яку використовували для доступу до файлів, які знаходяться на відстані. До появи служби WWW це була найпопулярніша служба доступу до даних в Інтернеті й корпоративних IP - мережах. Перші специфікації FTP відносяться до 1971 року (RFC114 (File Transfer Protocol A.K. Bhushan Apr-10-1971), RFC959 (File Transfer Protocol J. Postel, J.K. Reynolds Oct-01-1985)). Сервери й клієнти FTP є практично в кожній ОС сімейства UNIX, WINDOWS, а також у багатьох інших мережних ОС. Клієнти FTP вбудовані сьогодні в програми перегляду (браузери) Інтернету, тому що файлові архіви на основі протоколу FTP як і раніше популярні й для доступу до таких архівів браузером використовується протокол FTP

Головне призначення FTP - це пересилати (копіювати, передавати) файли. FTP можна використовувати самостійно, а також через інші системи. File Transfer Protocol протокол високого рівня а саме, рівня додатків.

FTP служба побудована по добре відомій схемі клієнт-сервер.

Клієнт (браузер, Windows Commander, NetVampir ...) посилає запити серверу і приймає файли. Сервер HTTP (Apache, IIS ...) обробляє запити клієнта на отримання файлу.

Протокол FTP підтримує два режими роботи: активний і пасивний.

В обох режимах FTP використовує контрольне з'єднання, яке встановлюється клієнтом по 21 порту (за замовчуванням). По контрольному з'єднанню ніякі данні, файли чи заголовки каталогів не передаються. Для передачі будь-якого файлу чи заголовку створюється окреме з'єднання.

Протокол FTP використовує при взаємодії клієнта із сервером кілька команд (не треба їх плутати з командами користувацького інтерфейсу клієнта, які використовує людина).

Ці команди діляться на три групи:

- команди керування доступом до системи;
- команди керування потоком даних;

- команди служби FTP.

Для налаштування FTP-сервера в ОС Linux спеціально виділяють файли конфігурації, де встановлюються параметри і права доступу FTP-сервера. Він розташований в каталозі /etc і має ім'я proftpd.conf. Робочі файли можуть знаходитися в каталозі /home. Файли логів повинні зберігатися в папці /log.

Для створення облікових записів користувачів і робочих груп необхідно користуватися командою useradd. Установка і зміни прав на файл або каталог здійснюються з допомогою команди chmod. Числове позначення прав доступу визначене таким чином:

0 – прав немає

1 – виконання

2 – запис

4 – читання.

Також можуть знадобитися команди:

- виклик редактора – mcedit

- робота з FTP-сервером – ftp

- визначення IP-адреси – ifconfig

- тестування каналу – ping

- запуск файлового провідника – mc

- допомога – man [команда]

Алгоритм налаштування FTP-сервера (ОС Linux)

1) Встановити пакет proftpd за допомогою команди `sudo aptitude install proftpd`. Якщо FTP-сервер не використовуватиметься постійно відповісти на питання, що з'явилося, про спосіб запуску: "самостійно".

2) Відкрити файл /etc/shells командою `sudo nano/etc/shells`

3) Додати в нього рядок /bin/false

4) Створити в /HOME каталозі папку FTP-shared командою `sudo mkdir /home/FTP-shared`

5) Створити користувача з ім'ям userftp команда `sudo useradd userftp -p`

`parol - d /home/FTP - shared - s /bin/false` замість "parol" - ввести слово чи фразу в якості пароля

6) В папці FTP-shared створити дві вкладені папки: `sudo mkdir /home/FTP-shared/public sudo mkdir /home/FTP-shared/upload`

7) Присвоїти потрібні права створеним текам командами `sudo chmod 755 /home/FTP-shared;`
`sudo chmod 755 /home/FTP-shared/public;` `sudo chmod 777 /home/FTP-shared/upload`

8) Переіменувати наявний конфігураційний файл proftpd.conf і створити новий: `sudo mv /etc/proftpd/proftpd.conf`

`/etc/proftpd/proftpd.conf.old;` `sudo nano/etc/proftpd/proftpd.conf`

9) Додати в нього рядка згідно вашого завдання

10) Після виконаних дій ftp-сервер матиме наступні параметри доступу: user (користувач) : donet; password(пароль): parol (той, що присвоєний для userftp)

11) Якщо треба зробити анонімний доступ, слід закоментувати обидві секції для donet і розкоментувати секцію для аноніма

12) Сервер вже запущений, але з параметрами за замовчуванням перезапустити: `sudo /etc/init.d/proftpd restart`

13) Для перевірки синтаксису створеного конфіг-файлу можна виконати: `sudo proftpd - td5`

14) Щоб знати, хто підключений до ftp-серверу в даний момент використовується команда `ftptop` (клавіша t міняє відображення, q – вихід) можна також використати команду `ftprwho`

15) ftp-сервер з двома папками, одна з них (public) доступна тільки для читання, інша (upload) – для запису

Якщо треба підключити яку-небудь папку до FTP-серверу (наприклад, перевірити роботу тільки що створеного FTP-сервера) без

/тут/шлях/папки/яку/я/хочу/розшарити/ /home/FTP-shared/public або з доступом на запис: `sudo mount -o bind`

/тут/шлях/папки/яку/я/хочу/розшарити/ /home/FTP -shared/upload.

Таким чином, можна в терміновому порядку тимчасово підключити папку чи диск і потім відмонтувати командою: `sudo umount/home/FTPshared/ public` або `sudo umount /home/FTP-shared/upload`.

Для постійного доступу до потрібних папок підключити їх за допомогою `fstab`. Бекап файлу `fstab`: `sudo cp /etc/fstab /etc/fstab.old`. Відкрити файл `/etc/fstab` комадою `sudo nano /etc/fstab` і додати потрібні шляхи: `/тут/шлях/папки/яку/я/хочу/розшарити /home/FTP-shared/public none bind 0 0`.

Тепер навіть при рестарті серверу (комп'ютера) інформація буде доступна, якщо сервер за роутером то тільки в локальній мережі. Щоб побачити фтп-сервер з інтернету потрібно надати йому зовнішню IP-адресу. Для цього слід відкрити потрібний порт (в даному випадку 21) для локальної адреси (192.168.xxx.xxx) на якій висить сервер, для доступу ззовні.

Наступним кроком треба дати зовнішній динамічній IP-адресі осмислену і постійну адресу. Зробити це можна за допомогою сервісу `DynDNS.com`, створивши за допомогою його зручну адресу (виду `moj-server.homeip.net`). Внести реєстраційні дані з сервісу `DynDNS` в налаштування роутера і поміняти `ServerName "server"` у файлі `proftpd.conf` на `ServerName "moj-server.homeip.net"`. Рестарт FTP-сервера: `sudo /etc/init.d/proftpd restart`

Алгоритм налаштування FTP-сервера (ОС Windows)

Встановлюватимемо FTP-сервер Gene6.

1. Запустити інсталяційний файл. Вибрати мову та шлях встановлення сервера. Вибрати компоненти, які потрібно встановити (рис.1). Ввести порт для адміністрування (8021) та встановити пароль для управління сервером (рис.2). Виконати інсталяцію FTP-сервера.

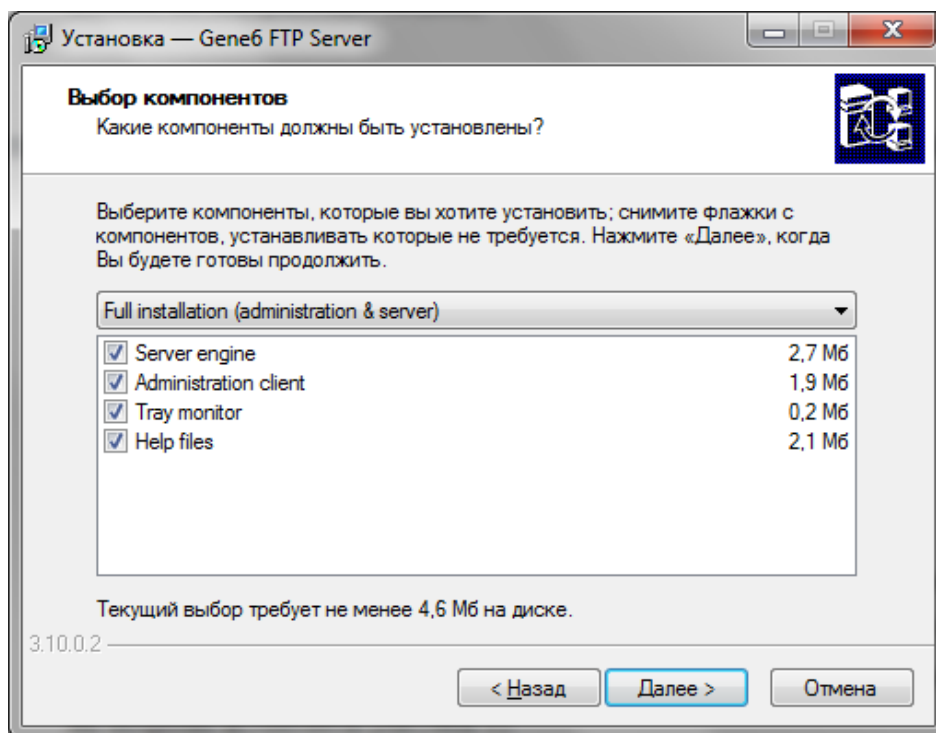


Рисунок 1 – Вікно вибору компонентів

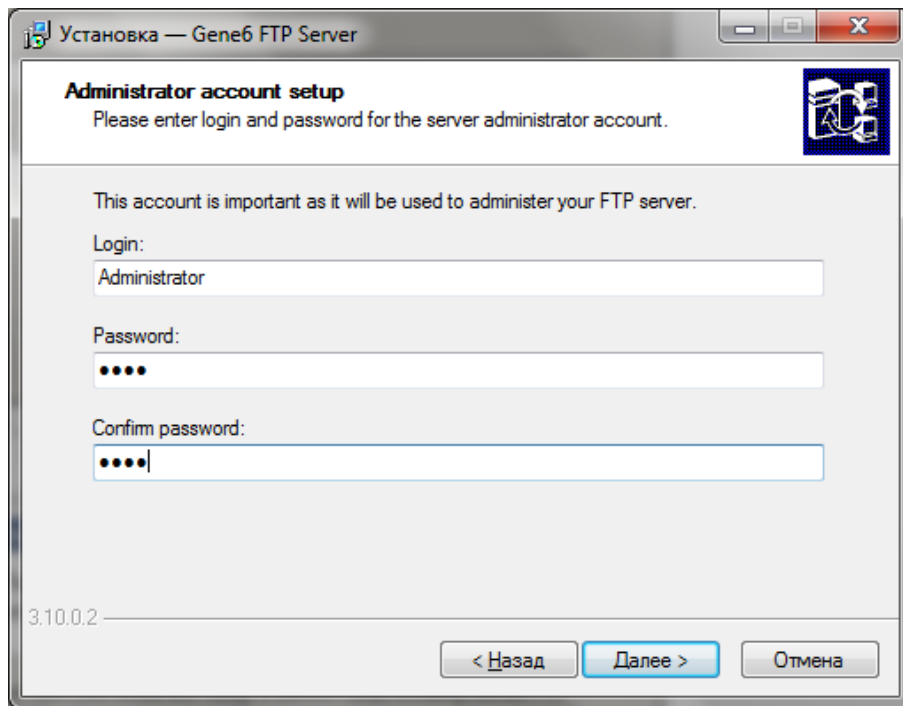


Рисунок 2 – Вікно встановлення паролю та логіну для управління сервером

2. Після встановлення сервера запуснути програму, ввести пароль, який було задано при встановленні, відмітити галочкою «Remember password» і натиснути «ОК» (рис.3).

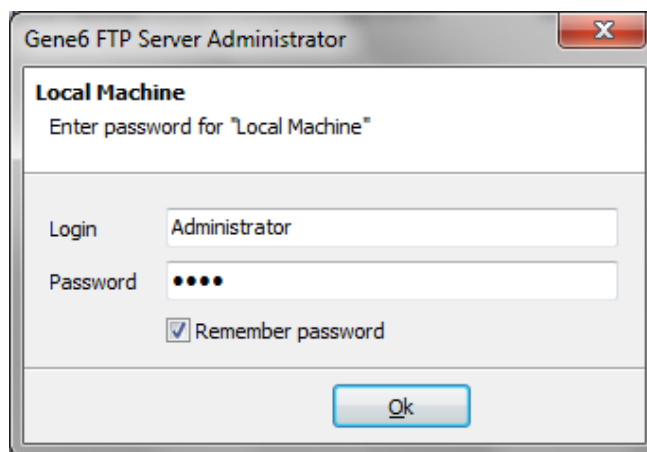


Рисунок 3 – Вікно введення паролю для управління сервером

3. У головному вікні вибрати підрозділ «Domains», а потім операцію створення домену «Double click here to add a domain». Ввести назву домену і обрати кількість одночасно підключених клієнтів і кількість одночасно підключених до однієї IP-адреси (наприклад, 10) (рис.4). Зі списку вибрати власну IP-адресу в мережі (рис.5).

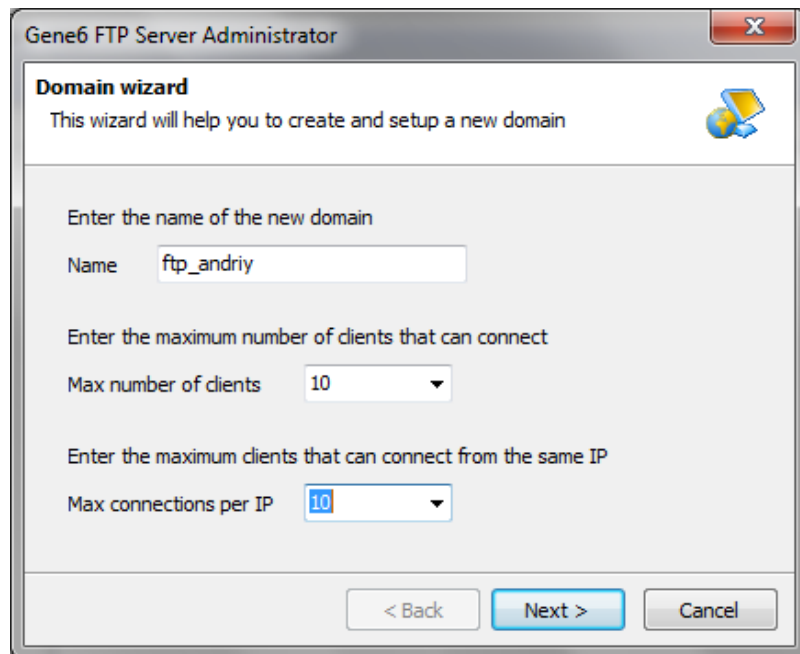


Рисунок 4 – Вікно створення домену

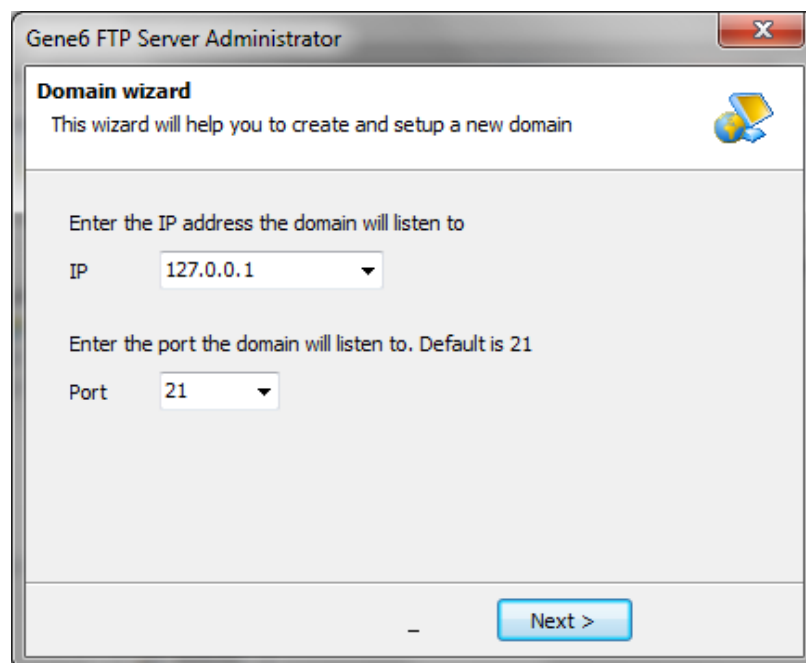


Рисунок 5 – Вікно вибору IP адреси домену

4. Встановити галочку «Create anonymous FTP account» і в значенні Home прописати empty:// (рис.6).

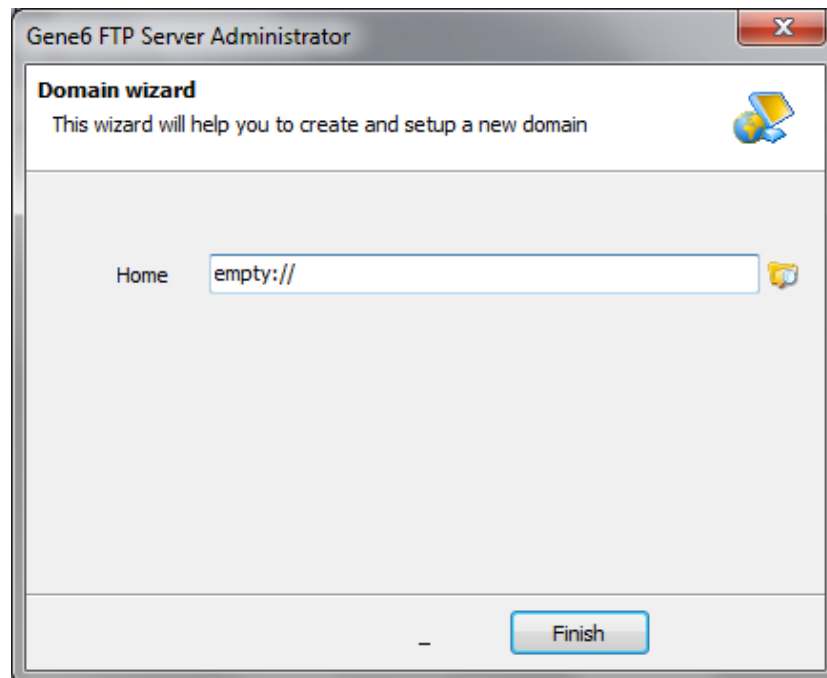


Рисунок 6 – Вікно додаткових налаштувань

5. Після налаштування домену створити анонімного користувача в розділі «Users». В розділі «Access rights» за допомогою кнопки «+» додати папки для загального доступу, де вказати віртуальний шлях (який буде видимий користувачам по FTP) і реальний шлях в себе на диску (рис.7).

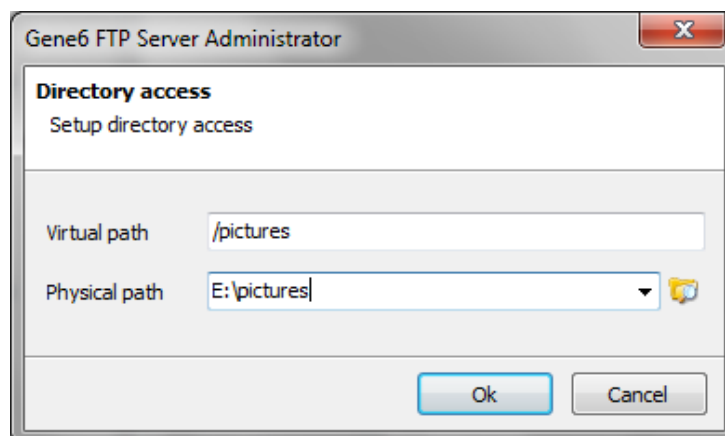


Рисунок 7 – Вікно налаштувань папки загального доступу

6. Визначити права для користувача Anonymous (рис.8) та виконати створення нових користувачів.

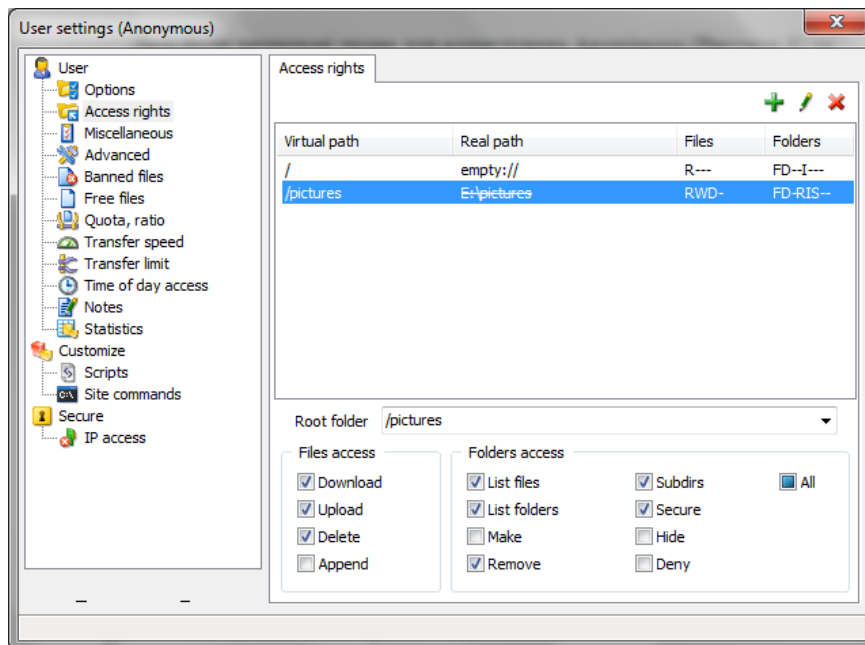


Рисунок 8 – Вікно визначення прав користувача

7. Виконати тестування FTP-сервера через cmd.exe та WEB-браузер (рис.9, 10).

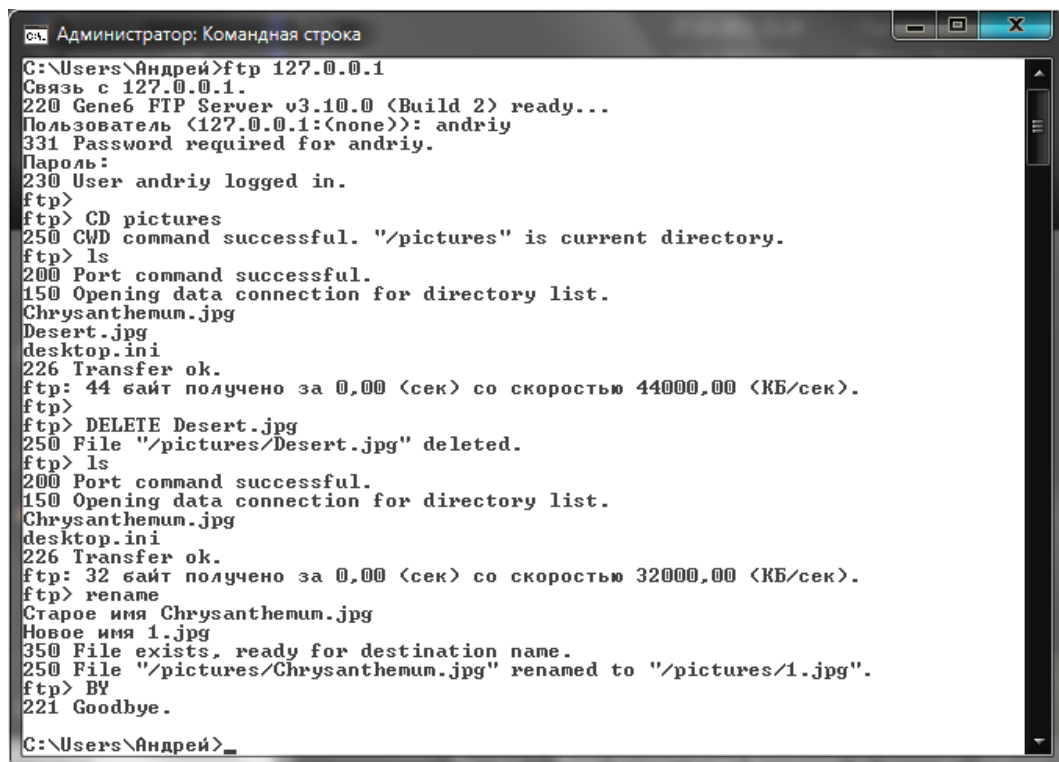


Рисунок 9 – Работа з FTP-сервером через cmd.exe

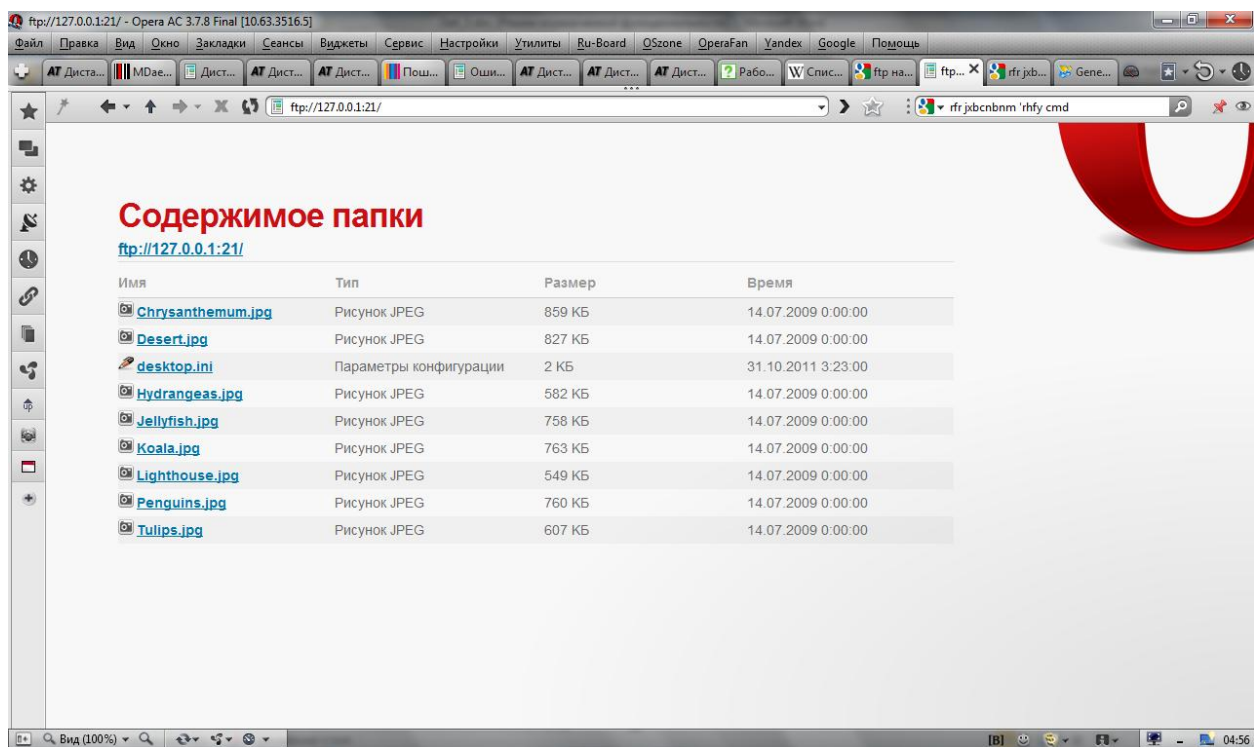


Рисунок 10 – Робота з FTP-сервером через cmd.exe

Початкові дані для проведення лабораторної роботи

Початковими даними для виконання лабораторної роботи є обліковий запис, IP-адреса FTP-клієнта.

Порядок проведення лабораторної роботи

1. Налаштувати FTP-сервер з наступними параметрами:
 - Максимальною кількістю користувачів – 2
 - Обліковий запис – student і пароль – ftppass
 - Робоча група – ftpgroup
 - Без можливості доступу анонімних користувачів
 - Ім'я сервера – Прізвище студента
2. Створити простий файл і переслати на комп'ютер сусіда і продемонструвати роботу налагодженого сервера викладачеві.

ЛАБОРАТОРНА РОБОТА №6

Тема: Захист мережевого сервісу (засобами ОС Windows 2003 Server, ОС Linux)

Мета: навчитися встановлювати і налаштовувати мережеву систему аутентифікації користувачів Kerberos на прикладі Linux Ubuntu.

Теоретичні відомості

Розглянемо принцип роботи системи. Протокол описаний у RFC 1510 (tools.ietf.org/html/rfc1510) і RFC 4120 (tools.ietf.org/html/rfc4120). Нині клієнтські компоненти для роботи з Kerberos є у більшості сучасних операційних систем. Для підтвердження достовірності використовується довірена третя сторона, яка володіє секретними ключами усіх суб'єктів і що бере участь в попарній перевірці достовірності.

Коли клієнт намагається отримати доступ до ресурсу, він посилає запит, що містить відомості про себе і про запрошену послугу. Увесь процес відбувається в три етапи, у відповідь контролер Kerberos (Key Distribution Center, KDC) видає квиток, що засвідчує користувача TGT (ticketgranting ticket). Кожен квиток має обмежений термін життя, що знижує інтерес до його

перехоплення. Тому однією з вимог до системи Kerberos є синхронізація часу між усіма учасниками. При подальшому зверненні до інших сервісів вводити пароль вже не треба.

Кожен учасник системи Kerberos як служба, так і користувач іменуються принципіал (principal). Кожен принципіал має ім'я і пароль. Типове ім'я принципіалу виглядає так root/admin@GRINDER.COM, що означає ім'я (primary name) root, характеристику (instance), який належить сектору GRINDER.COM. Такий підхід дозволяє розрізнити декілька служб, що працюють на одному комп'ютері, і серед однотипних служб вибирати потрібну. Уся схема роботи від користувача прихована. При зверненні до ресурсу він, як і раніше, вводить тільки свій логін і пароль.

Для зручності комп'ютери можуть бути об'єднані в сектори (realms), до речі в деякій літературі realms перекладають як домен. Усі принципіали зберігаються у базі даних сервера Kerberos. У мережі може бути використано декілька KDC, один з яких є основним (master). На master KDC встановлюється адміністративний сервер kadmind керівник політиками. Усе, звичайно, не так просто, і на порядок або два складніше, але цього вистачає для розуміння, того що ми нааштовуватимемо далі.

Хід роботи

1. Встановлюємо NTP

Перш ніж встановити Kerberos, необхідно налаштувати службу синхронізації часу (NTP – Network Time Protocol), без якої не можлива нормальна робота Kerberos.

```
$ sudo apt-get install ntp
```

Всі налаштування виконуються в одному файлі.

```
$ sudo mcedit /etc/ntp.conf
```

```
driftfile /var/lib/ntp/ntp.drift
statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
```

```
# сервери, з якими будемо синхронізувати час
server ntp.ubuntulinux.org
server pool.ntp.org
server time.nist.gov
```

```
# використовуємо локальний час у випадку невдачі
server 127.127.1.0
fudge 127.127.1.0 stratum 13
```

```
restrict default kod notrap nomodify nopeer noquery
```

```
# локальні користувачі можуть здійснювати запит часу
restrict 127.0.0.1 nomodify
```

```
# вмикаємо broadcast
broadcast 192.168.1.255
```

```
# прослуховування часу в мережі
disable auth
broadcastclien
```

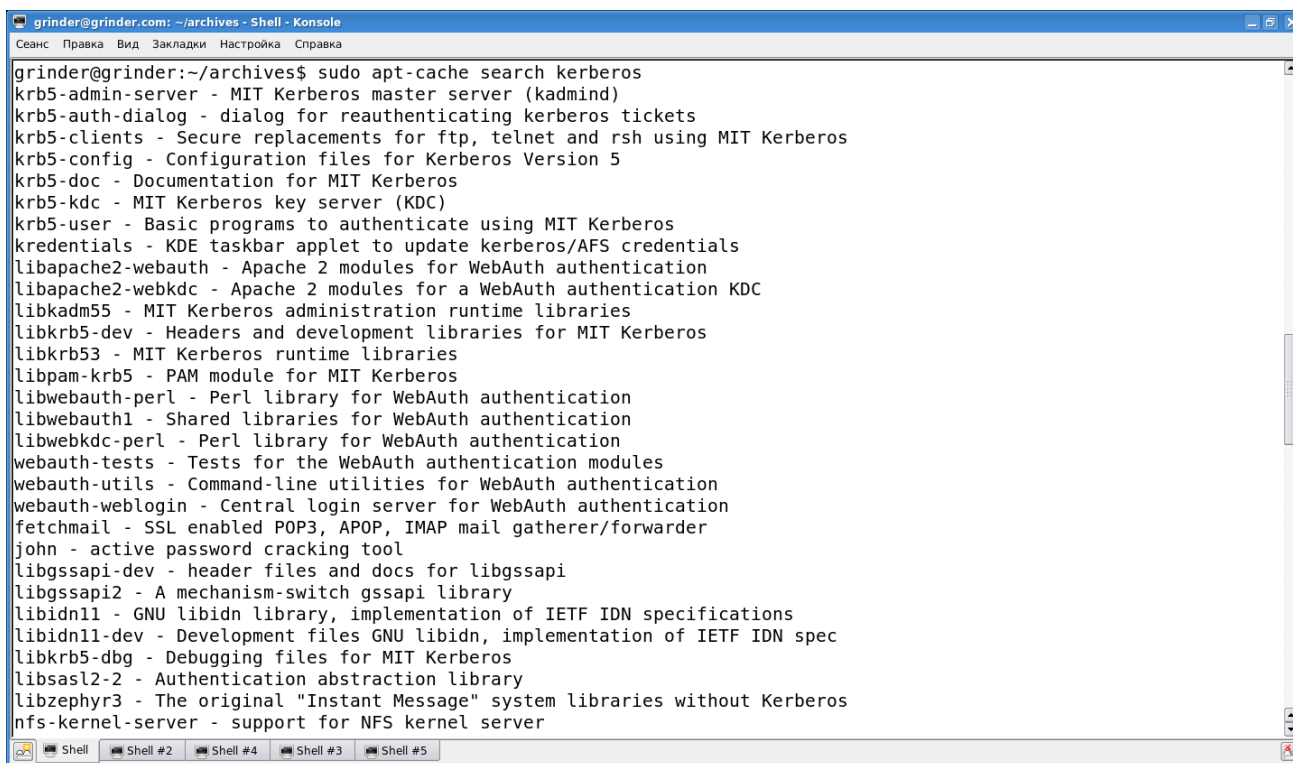
```
Перезапускаємо сервер.  
$ sudo /etc/init.d/ntp restart  
* Stopping NTP server ntpd [ OK ]  
* Starting NTP server ntpd [ OK ]
```

```
Тепер синхронізуємо час.  
$ ntpq -p -c as && echo && ntptrace
```

2. Установка Kerberos

У репозитаріях пакетів дистрибутивів Linux вже є все необхідне. Хоча за бажанням можна встановити систему з початкових текстів. Дистрибутив Heimdal знайдете на FTP сервері Стокгольмського університету <ftp://ftp.pdc.kth.se/pub/heimdal/src>. Там же можна знайти готові пакети для деяких дистрибутивів. Версія від MIT знаходиться за адресою <http://web.mit.edu/kerberos/>.

Команда "sudo apt-cache search kerberos" в Ubuntu видасть великий список пакетів, в якому можна знайти вирішення від MIT і Heimdal. (<http://www.tux.in.ua/wp-content/uploads/2008/01/319.png>)

A screenshot of a terminal window titled "grinder@grinder.com: ~/archives - Shell - Konsole". The terminal shows the command "sudo apt-cache search kerberos" and its output, which lists various packages related to Kerberos and WebAuth authentication, such as "krb5-admin-server", "krb5-kdc", "krb5-config", "krb5-user", "krb5-clients", "libkrb5-dev", "libkrb53", "libpam-krb5", "libwebauth-perl", "libwebauth1", "libwebkdc-perl", "webauth-tests", "webauth-utils", "webauth-weblogin", "fetchmail", "john", "libgssapi-dev", "libgssapi2", "libidn11", "libidn11-dev", "libkrb5-dbg", "libsasl2-2", "libzephyr3", and "nfs-kernel-server". The terminal window has a standard Ubuntu-style interface with a title bar and window controls.

Основні їх налаштування практично ідентичні. Також ці системи розуміють квитки, видані одне одним, хоча є і проблеми сумісності (про них тут не згадуватимемо). Для прикладу виберемо версію від MIT.

```
$ sudo apt-get install krb5-admin-server krb5-kdc krb5-config krb5-user krb5-clients
```

Основні налаштування Kerberos проводяться у файлі /etc/krb5.conf. Набивати його повністю не треба, можна використати готовий шаблон.

```
$ sudo cp /usr/share/kerberos-configs/krb5.conf.template /etc/krb5.conf
```

Тепер відкриваємо файл і починаємо підганяти під свої умови.

```
$ sudo mcedit /etc/krb5.conf
```

```
[libdefaults]  
default_realm = GRINDER.COM
```

```
# kdc і admin сервер для GRINDER.COM  
[realms]
```



```
GRINDER.COM = {  
kdc = server.grinder.com  
admin_server = server.grinder.com  
}
```

```
# повідомляємо kdc, які вузли входять в область GRINDER.COM  
# якщо область і домен співпадають, цю секцію можна опустити  
[domain_realm]  
grinder.com = GRINDER.COM  
.grinder.com = GRINDER.COM  
  
# відключаємо сумісність із 4 версією Kerberos  
[login]  
krb4_convert = false  
krb4_get_tickets = false
```

Цей файл використовується як сервером, так і додатками, тому його можна практично без змін поширити а решту систем, що входять в один realms (якщо їх багато, можна використовувати службу DNS). Усі налаштування KDC здійснюються в /etc/krb5kdc/kdc.conf. Більшу частину параметрів можна залишити без змін, виправивши лише realms:

```
$ sudo mcedit /etc/krb5kdc/kdc.conf
```

```
[kdcdefaults]  
kdc_ports = 750,88
```

```
[realms]  
GRINDER.COM = {  
database_name = /var/lib/krb5kdc/principal  
admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab  
acl_file = /etc/krb5kdc/kadm5.acl  
key_stash_file = /etc/krb5kdc/stash  
kdc_ports = 750,88  
max_life = 10h 0m 0s  
max_renewable_life = 7d 0h 0m 0s  
master_key_type = des3-hmac-sha1  
supported_encetypes = des3-hmac-sha1:normal des-cbc-crc:normal des:normal des:v4 des:norealm  
des:onlyrealm des:afs3  
default_principal_flags = +preauth  
}
```

Перезапускаємо KDC і сервер адміністрування.

```
$ sudo /etc/init.d/krb5-kdc restart  
$ sudo /etc/init.d/krb5-admin-server restart
```

Створюємо принци піали і ключі

Спочатку слідж створити нову базу даних і наповнити її принципіалами. Тут можливі кілька варіантів, один з яких виклик kadmin з ключем -l. Можна використовувати спеціальні утиліти.

```
$ sudo kdb5_util create -s  
Loading random data  
Initializing database '/var/lib/krb5kdc/principal' for realm 'GRINDER.COM',  
master key name 'K/M@GRINDER.COM'  
You will be prompted for the database Master Password.  
It is important that you NOT FORGET this password.  
Enter KDC database master key:
```

Re-enter KDC database master key to verify:

Нову базу створено. Утиліта просить ввести пароль. Не забудьте його. Створимо принципіал, який буде потрібен для адміністративних цілей:

```
$ sudo kadmin.local -q «addprinc admin/admin»
Authenticating as principal root/admin@GRINDER.COM with password.
Enter password for principal «admin/admin@GRINDER.COM»:
Re-enter password for principal «admin/admin@GRINDER.COM»:
Principal «admin/admin@GRINDER.COM» created.
Authenticating as principal root/admin@GRINDER.COM with password.
Enter password for principal «admin/admin@GRINDER.COM»:
Re-enter password for principal «admin/admin@GRINDER.COM»:
Principal «admin/admin@GRINDER.COM» created.
```

Для додавання принципіалів для KDC, admin сервера, свого комп'ютера, користувачів скористаємось інтерактивним режимом роботи:

```
$ sudo kadmin.local -p admin/admin
Authenticating as principal admin/admin with password.
# зареєструвались, використавши принципіал адміністратора
# створюємо принципіал комп'ютера. Оскільки комп'ютер не буде вводити пароль,
використовуємо випадковий пароль
kadmin.local: addprinc -randkey host/grinder.com
Principal «host/grinder.com@GRINDER.COM» created.
# тепер користувач
kadmin.local: addprinc grinder
Enter password for principal «grinder@GRINDER.COM»:
Re-enter password for principal «grinder@GRINDER.COM»:
Principal «grinder@GRINDER.COM» created.

# додамо принципіал комп'ютера в файл keytab, у якому зберігаються власні принципіали
kadmin.local: ktadd host/grinder.com
Entry for principal host/grinder.com with kvno 3, encryption type Triple DES cbc mode with
HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/grinder.com with kvno 3, encryption type DES cbc mode with CRC-32
added to keytab WRFILE:/etc/krb5.keytab.
```

І так далі. Щоб мати можливість заходити віддалено на сервер з використанням Kerberos необхідно створити файл .k5login (з крапкою), у який вписати ім'я принципіал.

```
$ echo grinder@GRINDER.COM > ~/k5login
```

3. Налаштовуємо робочу станцію

До складу обох варіантів Kerberos входять утиліти, призначені для заміни стандартних системних утиліт на зразок /bin/login. Налаштування керберизації в різних дистрибутивах будуть відрізнятися. Хоча б тому, що у більшості систем використовується /sbin/init і достатньо в /etc/inittab замінити /bin/login на керберизований /usr/bin/login, після чого при реєстрації користувача спочатку буде іти звернення до Kerberos, а у випадку невдачі – до локальної бази /etc/passwd. В Ubuntu з 6.10 замість /sbin/init використовується нова система завантаження upstart, тому тут все дещо по-іншому.

Для налаштування нам знадобляться пакети krb5-clients, krb5-user і libpam-krb5. Файл /etc/krb5.conf беремо з KDC. Потім приступаємо до налаштування PAM. У каталозі /etc/pam.d необхідно створити файл common-krb5 такого змісту:

```
auth sufficient /lib/security/pam_krb5.so use_first_pass
```

В самому кінці файлу /etc/pam.d/login є рядки, що описують методи аутентифікації.

```
# Standard Un*x account and session
```

```
@include common-account
```

```
@include common-session
```

```
@include common-password
```

Перед цими рядками додаємо іще один:

```
@include common-krb5
```

Якщо реєстрація в системі здійснюється у графічному менеджері (GDM в Ubuntu, KDM в KUbuntu, в файлах gdm і/або kdm), діємо аналогічно. До речі, в репозитарії є пакет kredentials, після встановлення якого в панелі задач з'явиться аплет, за допомогою якого можна керувати особистими квитками. Встановити його можна командою

```
$ sudo apt-get install kredentials
```

Після чого ярлик для запуску перейде в меню К.

Нам вдалося створити систему, яка буде надійно аутентифікувати користувачів. Реєстрація користувачів та сервісів управляється з одного місця. Користувач, який успішно зареєструвався в системі, може без проблем потрапити на будь-який дозволений мережевий ресурс.

ЛАБОРАТОРНА РОБОТА №7

Тема: Організація VPN-мереж

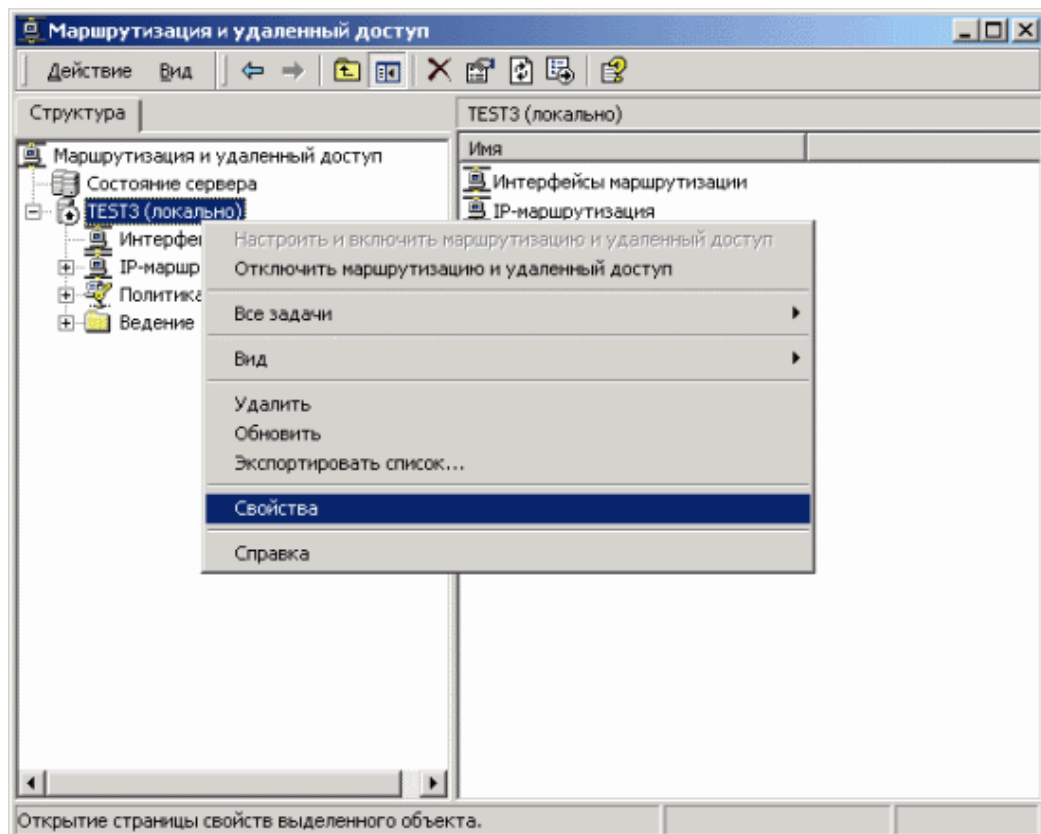
Мета: освоїти навички налаштування VPN-сервера у Windows 2003 Server.

VPN PPTP-сервер для захищеного підключення клієнтів може бути налаштований лише на серверних версіях Windows 2000/2003. Він налаштовується як сервер віддаленого доступу (RAS-сервер) в службі RRAS (Маршрутизація і віддалений доступ).

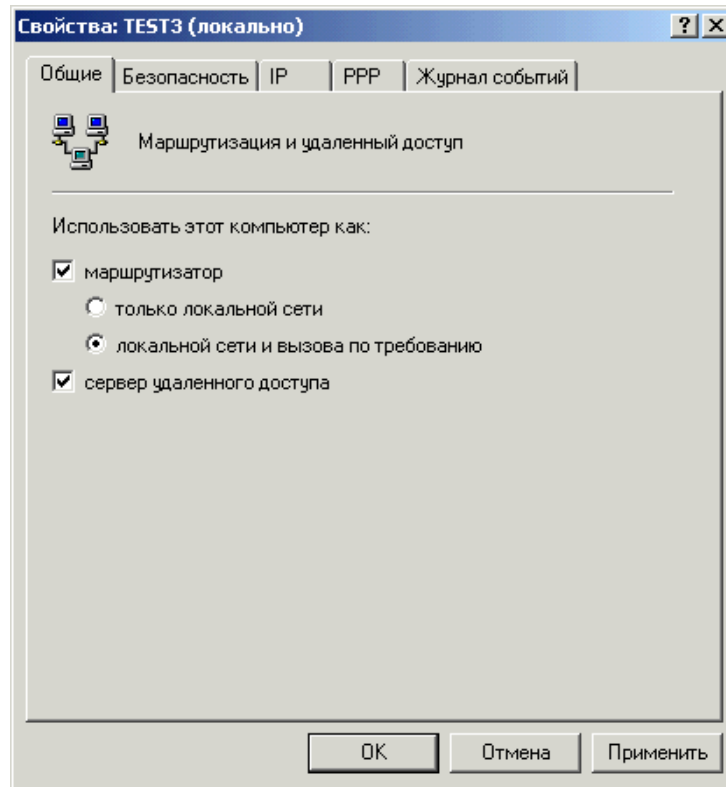
Хід роботи

Створення VPN-сервера

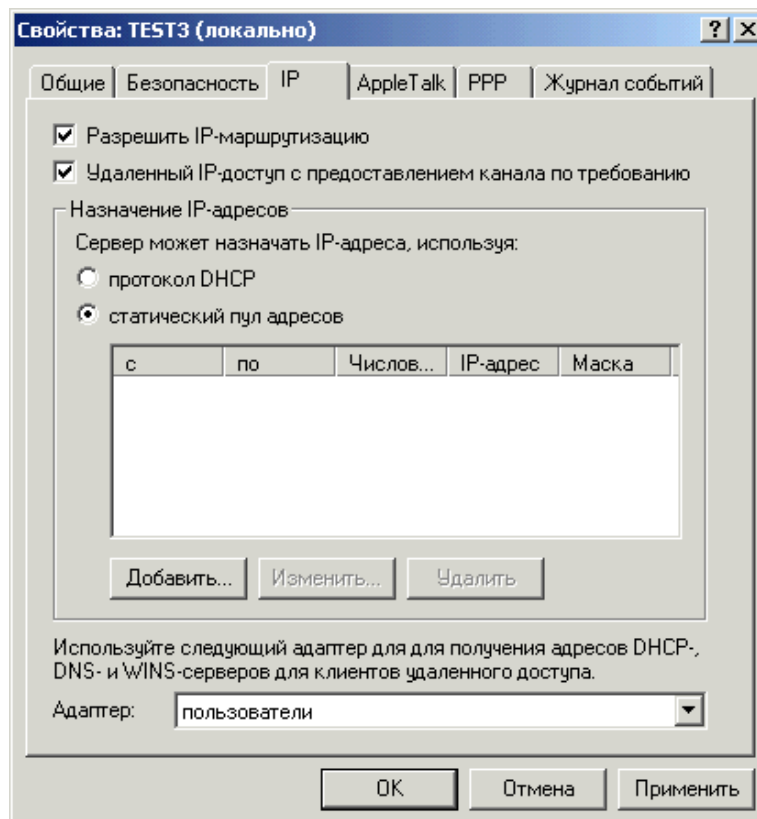
1. Відкрийте службу "Маршрутизація і віддалений доступ" і зайдіть у властивості сервера.

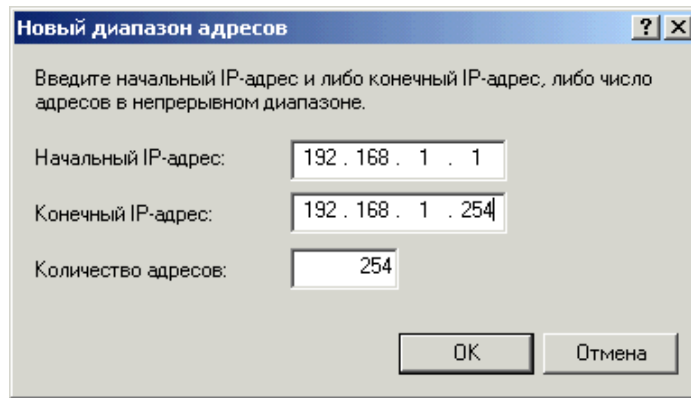


2. Виставте параметр "локальной сети и вызова по требованию", а також "сервер удаленного доступа"

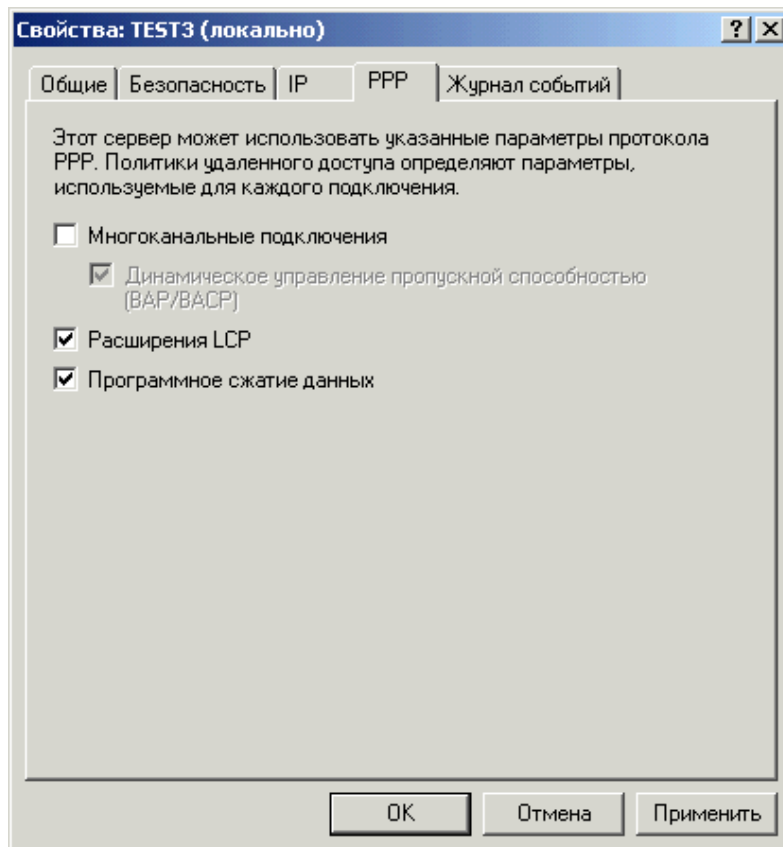


3. Зайдите на вкладку "IP", выберите название внутреннего адаптера и создайте статичный пул адрес, отличный от внутреннего, який буде присвоюватися VPN-клієнтам.

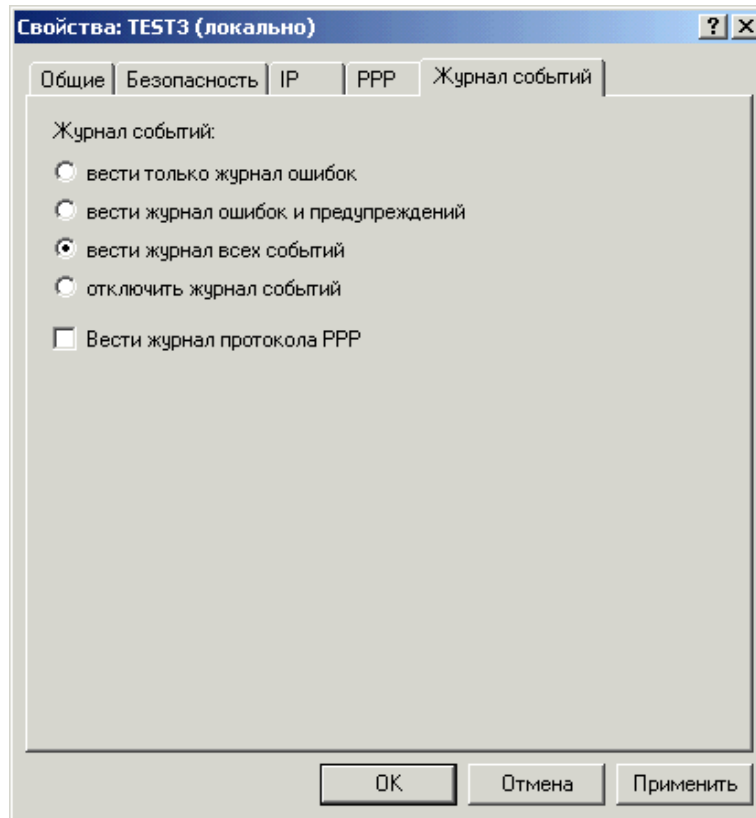




4. Далі у вкладці "PPP" зніміть галочку з "Многоканальные подключения" – це прискорить роботу Інтернету.

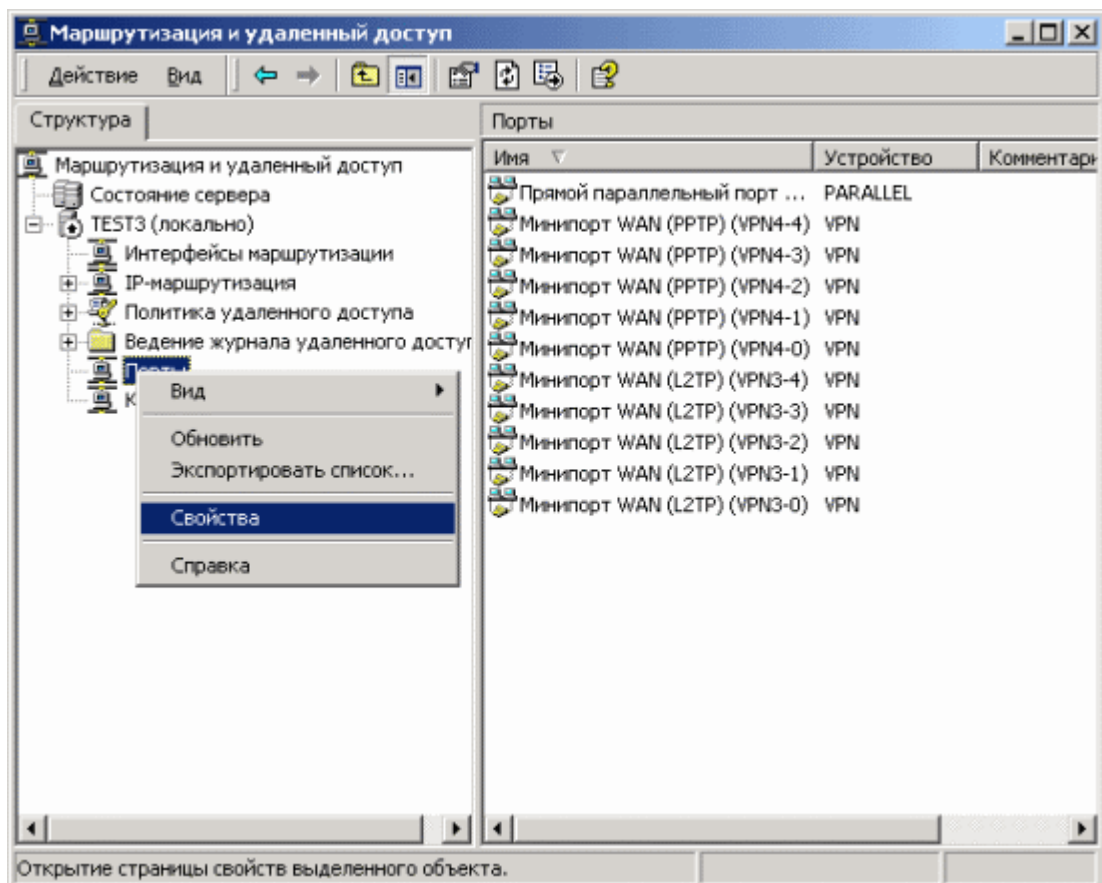


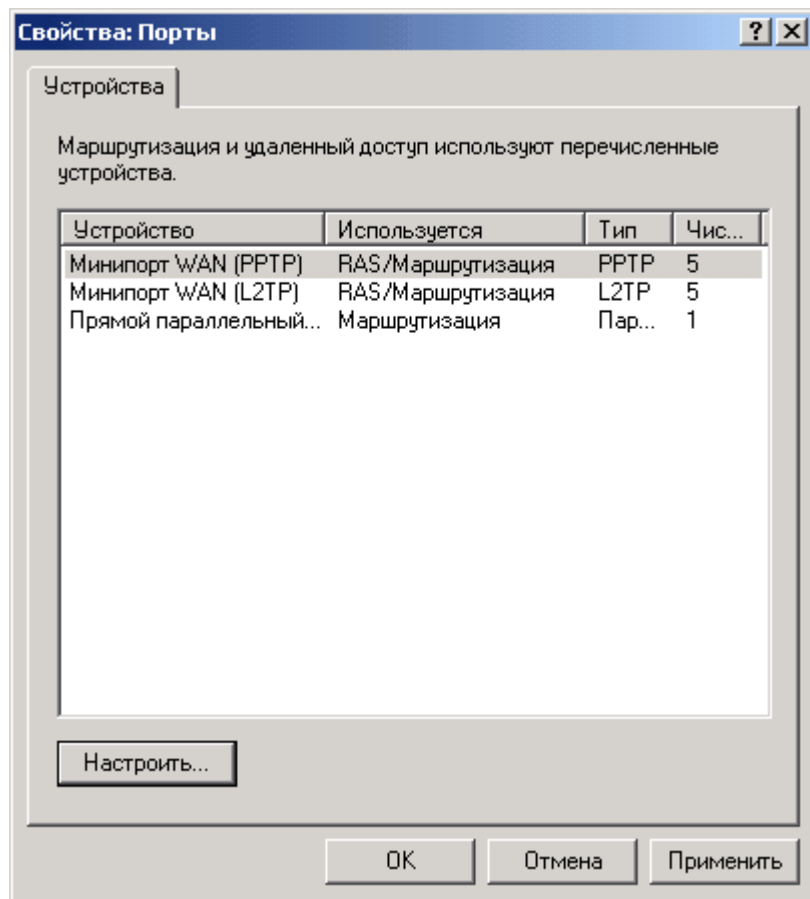
5. У вкладці "Журнал событий" виставить параметр "вести журнал всех событий"



Конфігурація портів

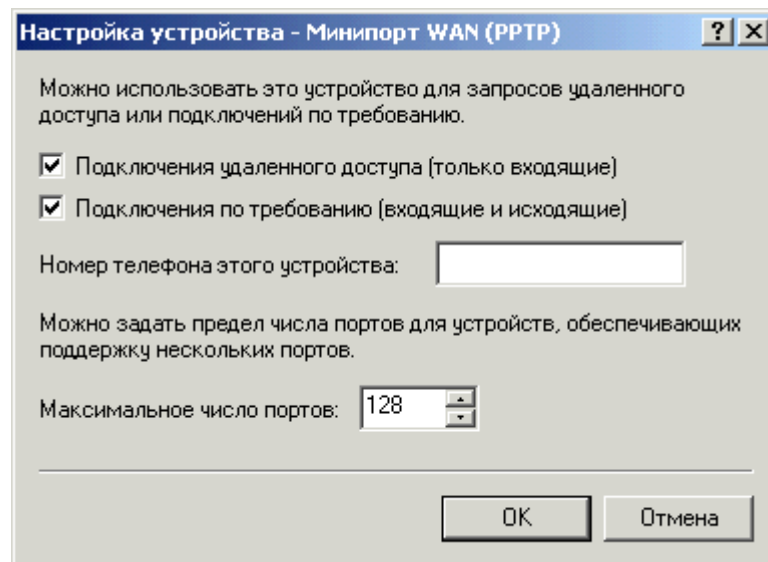
1. Зайдіть у властивості "Порты". За замовчуванням RRAS створить 5"PPTP", 5"L2TP" і 1 "Прямой параллельный". Для стабільної роботи сервера рекомендується видалити непотрібні порти (прямий параллельний, L2TP, і.т.д.) і створити необхідну кількість портів. Їх має бути більше, ніж одночасних підключень.



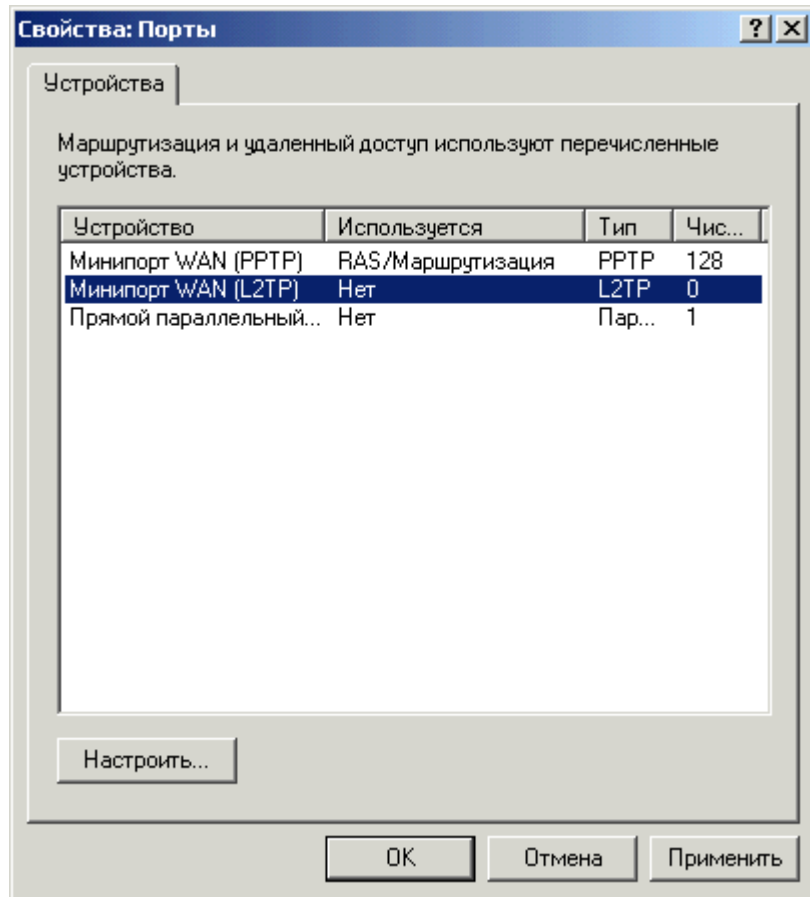


2. Видаляємо порти WAN(L2TP)

3. Виставте необхідну кількість PPTP портів (кількість портів має бути більша, ніж планованих одночасних підключень)

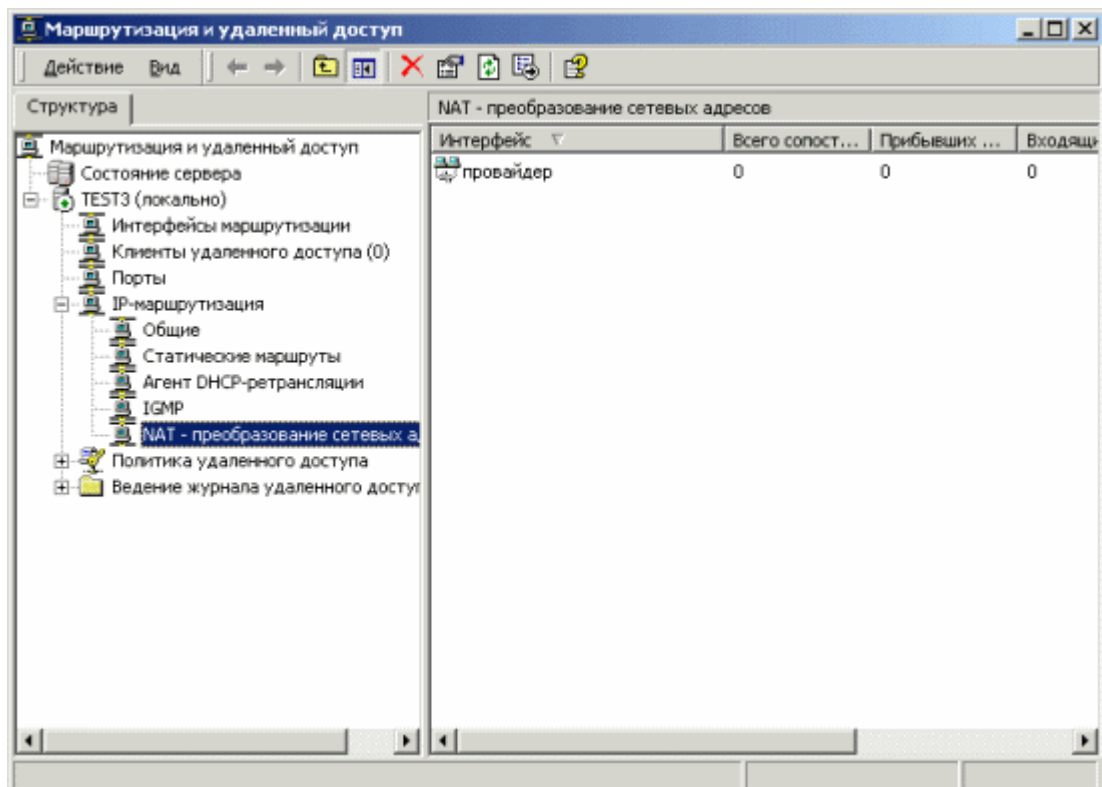


4. В результаті у вас з'явиться таке вікно:



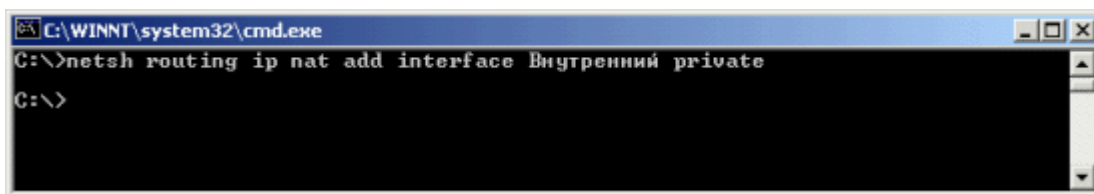
Конфігуруємо NAT

1. Зайдіть у "IP-маршрутизация" / "NAT-преобразование сетевых адресов". Якщо ви збираєтесь надавати доступ тільки по VPN з'єднанню, тоді видаліть внутрішній інтерфейс, якщо ні – тоді залиште. Якщо ви використовуєте Windows 2003 вам необхідно відключити basic firewall. Її використання при наявності Traffic Inspector може призвести до конфліктів. Для цього зайдіть у властивості зовнішнього підключення і відключіть.

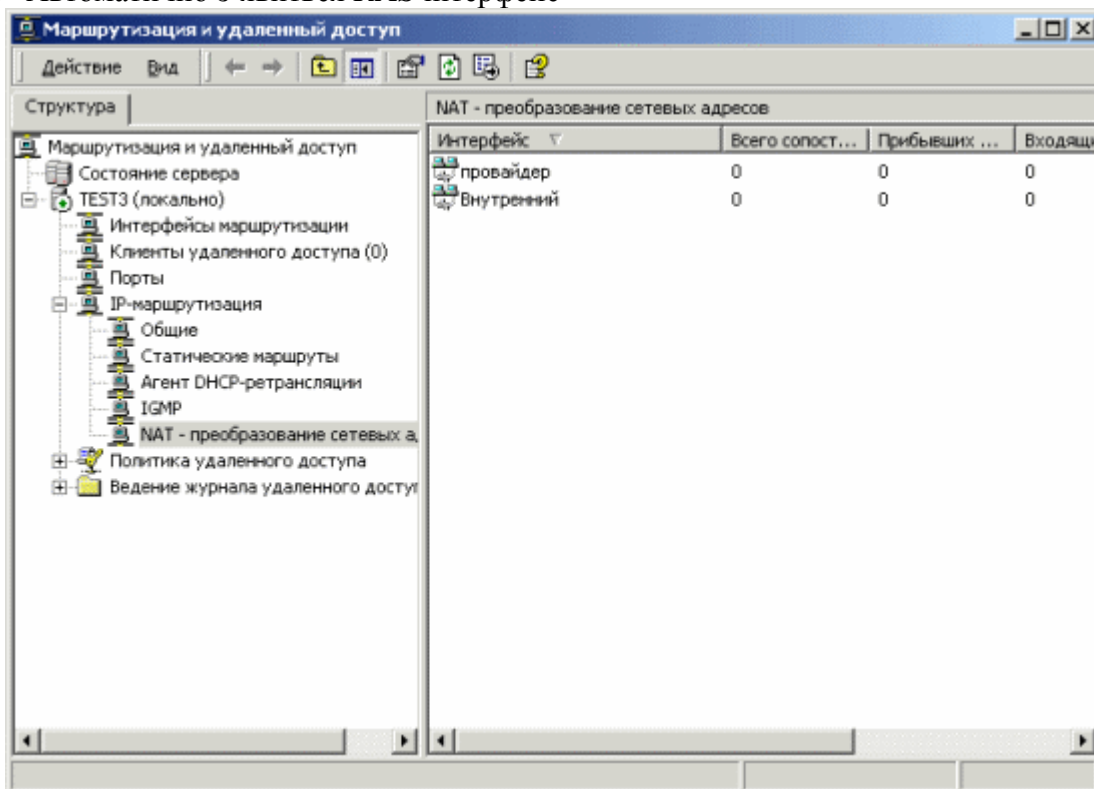


Далі вам потрібно додати RAS інтерфейс. Для цього в командному рядку наберіть "netsh routing ip nat add interface Внутрішній (у англійській версії windows "internal") private" див. рис. Крім того дуже корисно озаборонити прив'язку NetBios до інтерфейсу Внутрішній (internal), якщо він активний (див. вище). Це важливо, якщо використовується RAS-сервер для підключення діалогних клієнтів (модеми або VPN) і допоможе звільнитися від деяких проблем при роботі сервера в мережі Windows.

Якщо NetBios дозволений на цьому інтерфейсі, то сервер реєструватиме свої NetBios-імена з IP-адресами усіх інтерфейсів, на які є прив'язка цієї служби. Поява IP-адреси інтерфейсу Внутрішній (internal) в цих реєстраціях може призвести до проблем. Для цього редактором реєстру в розділі HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesRemoteAccessParametersIp додаємо параметр DisableNetbiosOverTcpip типу DWORD і значенням 1. Службу потрібно перезапустити.



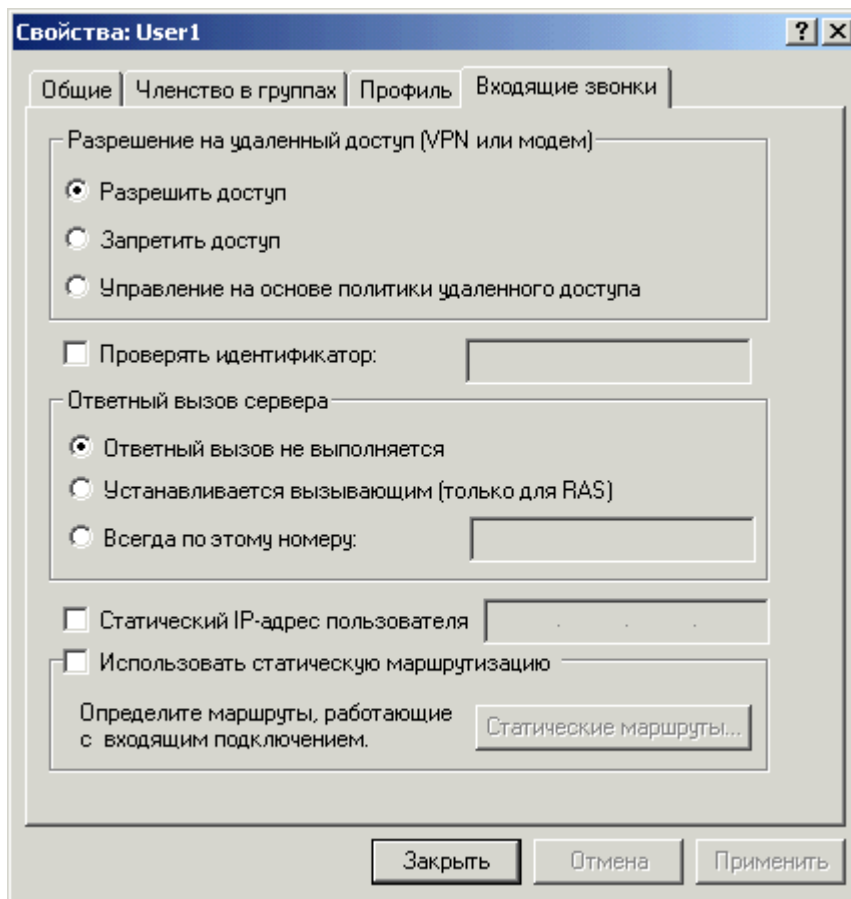
2. Автоматично з'явиться RAS інтерфейс



Створення клієнтів

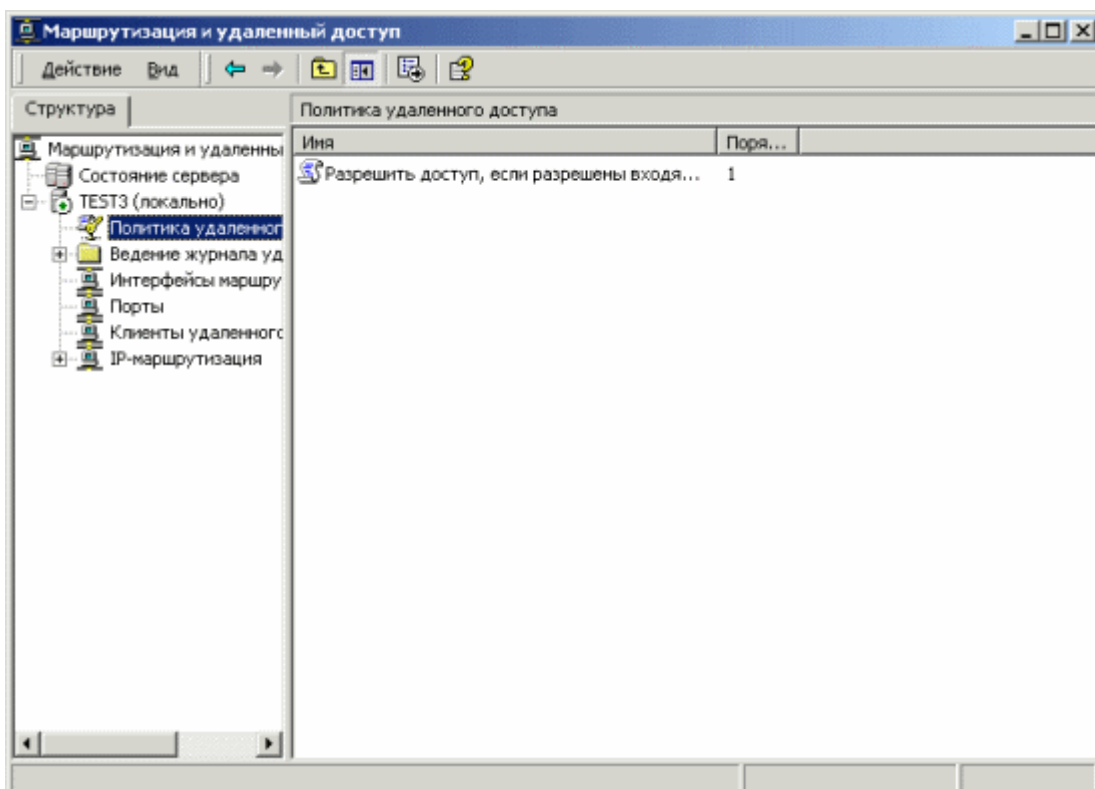
1. Зайдіть у "Управление компьютером", далі в "Локальные пользователи и группы", "Пользователи"

2. Створіть користувача, імена користувачів повинні співпадати з іменами клієнтів. Далі зайдіть на вкладку "Входящие звонки".

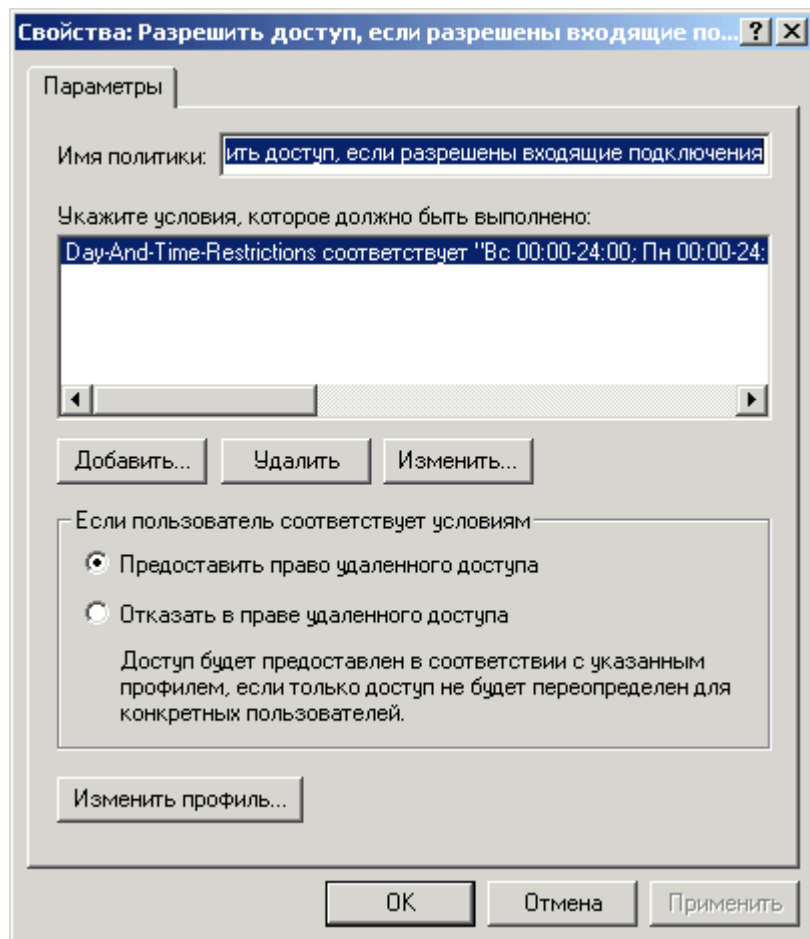


Налаштування VPN з'єднання

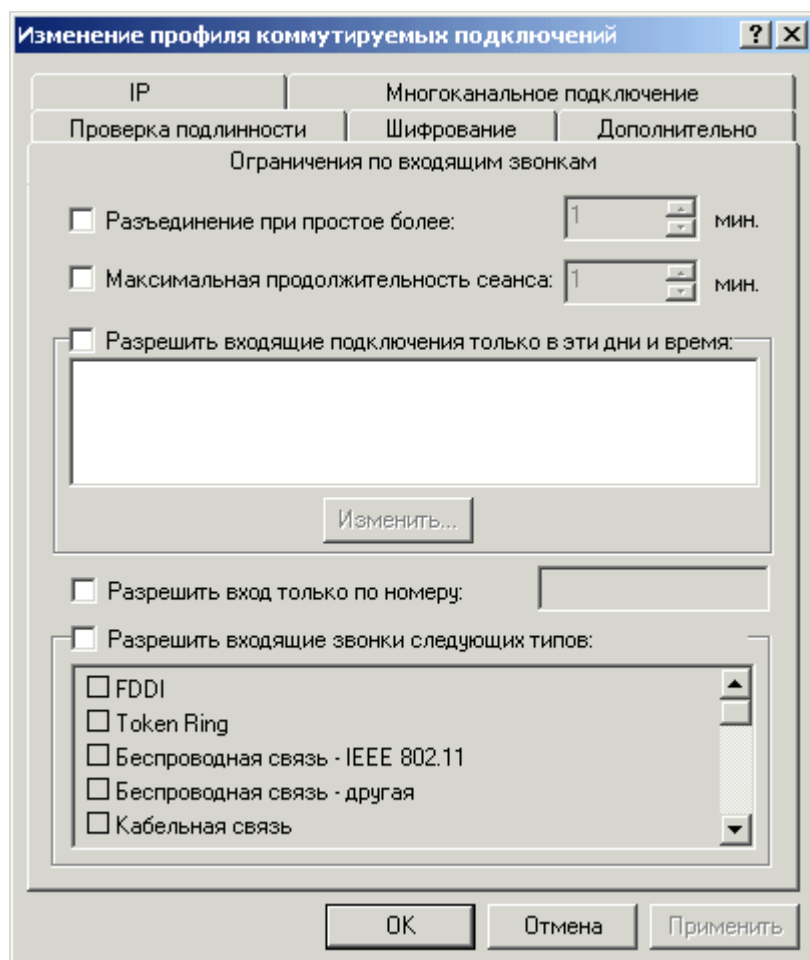
1. В групі "Политика удаленного доступа" зайдіть у властивості "Разрешить доступ, если разрешены входящие подключения"



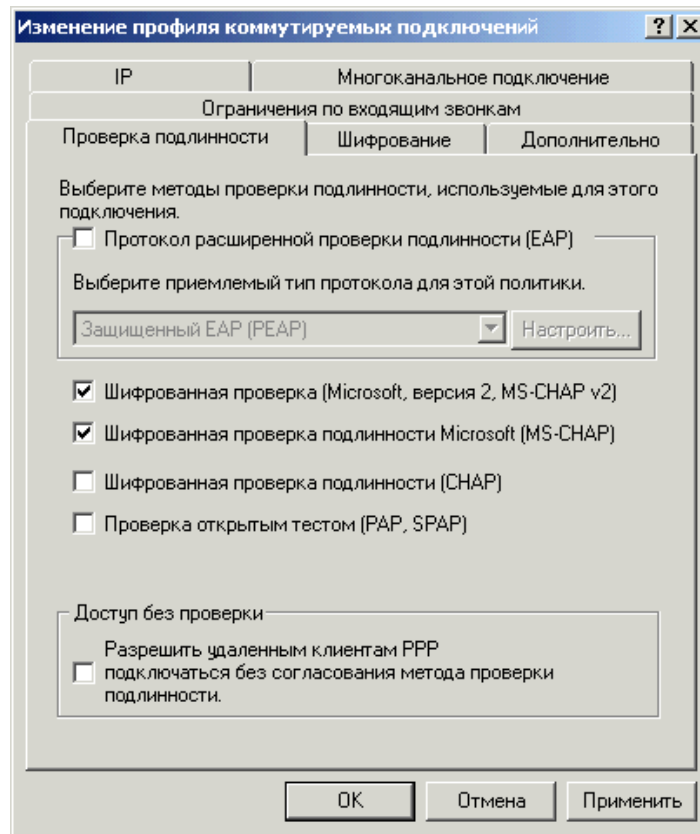
2. Натисніть кнопку "Изменить профиль..."



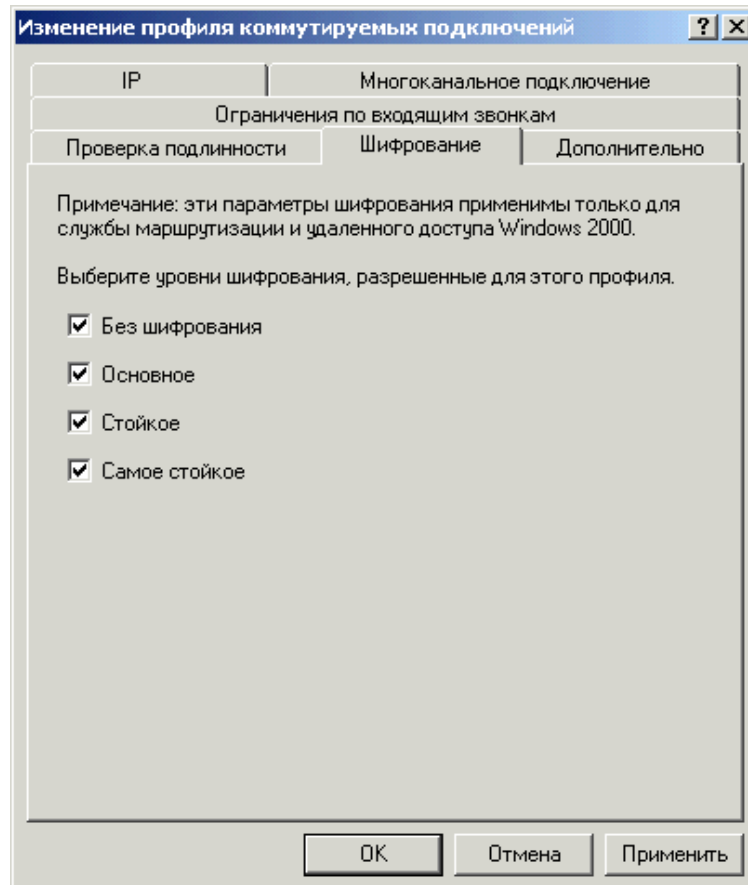
3. Зайдіть на вкладку "Проверка подлинности"



4. Залиште два параметри перевірки справжності MS-CHAP для ОС Windows і CHAP для інших ОС.



5. Далі зайдіть на вкладку "Шифрование", виберіть параметри шифрування. Усі виконані налаштування повинні бути ідентичними при налаштуванні VPN з'єднання у клієнтів.



Перезапустіть сервер.

ЛАБОРАТОРНА РОБОТА №8

Тема: Організація систем для хостингу та налаштування web-програми

Мета: організація системи для веб-хостингу шляхом встановлення та налаштування веб-сервера Apache, СУБД MySQL, додатку phpMyAdmin або комплексу Денвер; налаштування програми PhpMyAdmin.

Порядок виконання роботи

Встановлення Apache, php, MySQL під Windows

Етапи інсталяції:

1. Отримання дистрибутивів

Дистрибутиви Apache, php і MySQL можна скачати із сайтів www.apache.org, www.php.net, www.mysql.com.

2. Встановлення Apache

Запускаємо дистрибутив. Треба буде вказати, що ви згодні з умовами ліцензії, і ввести синтаксично коректні домен, url та email – вони будуть повертатись користувачу при помилці.
Критерій успішного встановлення: При виклику браузером адреси <http://localhost/> ви побачите напис «It works!»

Якщо Ви не бачите напис «It works!»:

1. Перевірте, чи не заблоковано Apache вашим брандмауером.
2. Перевірте, чи встановилась служба **Apache2.2**. З'ясувати це можна, якщо зайти в Панель Управління Windows — в розділ Адміністрування/Служби (Administrative Tools/Services). Якщо служби **Apache2.2** там немає, спробуйте інсталювати її з командного рядка. Встановіть активною директорію `Apache2.2\bin` і виконайте дві команди: **httpd -k install**
httpd -k start
3. Якщо запущено MS IIS — він захопить порт 80. Апачу доведеться йти на порт, наприклад, 8080. Тоді доведеться правити директиву Listen файлу `httpd.conf`, і після перезавантаження Апача звертатись до посилання <http://localhost:8080/>
4. У Windows Vista часто Apache запускається й зупиняється тільки через консоль **Служби**.
5. Якщо при спробі запустити Apache видається повідомлення:

```
httpd.exe: Could not reliably determine the server's fully qualified domain name, using
127.0.0.1 for ServerName
(OS 10048)+свўэю ЁрчЁх°рхСё юфэю шёяюыЎчютрэшх рфЁхёр ёюьхСр
(яЁюСюьюю/ёхСхтющрфЁхё/яюЁС). :
make_sock: could not bind to address 0.0.0.0:80 no listening sockets available, shutting down
Unable to open logs
Note the errors or messages above, and press the <ESC>> key to exit. 30...
```

спробуйте поставити директиву `Win32DisableAcceptEx` в файл `httpd.conf`

3. Розпакування архіва php в `c:\php`

Саме на це розташування орієнтовані рядки в конфігураційних файлах php. Якщо ви вперше встановлюєте Apache/php/MySQL, краще обрати саме це розташування, оскільки в іншому випадку доведеться міняти частину параметрів в конфігураційних файлах.

4. Внесення виправлень в файл `httpd.conf`

Їх суть: ми повідомляємо Апачу, що в нього є модуль, який повинен спрацювати на розширення php. В розпакованому архіві `c:\php` є файл `install.txt`. В ньому написано англійською мовою, які зміни потрібно внести в файл `httpd.conf`. А саме: в рядку 808 файла `install.txt` є рядок: **LoadModule php5_module "c:/php/php5apache2.dll"**. Його потрібно відредагувати, виправивши версію Апача: **LoadModule php5_module "c:/php/php5apache2_2.dll"** і вставити в закінчення блока інструкцій `LoadModule` файла `httpd.conf` (127-й рядок файла `httpd.conf`).

Таким чином, ми вказали, що при завантаженні apache запускає інтерпретатор php як свій модуль. Тепер вкажемо Апачу, де шукати файл php.ini (параметри php). В рядку 812 файлу **install.txt** є рядок **PHPIniDir "C:/php"**. Його треба поставити в файл **httpd.conf** (в рядок 128). Тепер потрібно вказати, що цей модуль повинен обробляти файли з розширенням php. В рядку 809 файлу **install.txt** є рядок: **AddType application/x-httpd-php .php**. Його вставляємо в закінчення блока AddType файла **httpd.conf** (приблизно 383 рядок файла **httpd.conf**)

5. Створюємо та описуємо в httpd.conf папку для зберігання WEB-папок

Один WEB-сервер може управляти роботою кількох сайтів (чи веб-додатків). Розрізняти їх Apache буде за доменним ім'ям, і кожному з цих імен призначити відповідну WEB-папку (в якій будуть зберігатись файли сайта). Створимо папку, в якій будуть зберігатись WEB-папки. Назвемо її, наприклад, **c:\www** (звичайно, можна назвати і по-іншому). Тепер у файл **httpd.conf** додаємо опис цієї папки: ми дозволимо доступ до цієї папки по протоколу http (за замовчуванням цього доступу немає). Після опису загальних замовчань (починаючи десь із рядка 194) додамо наступний блок:

```
<Directory "C:/www">
    AllowOverride All
    Order deny,allow
    Allow from all
</Directory>
```

Зверніть увагу: слеш **прямий**: **c:/www**

6. Вмикаємо механізм віртуальних хостів

Як уже було сказано, можна задати декілька WEB-папок для різних доменних імен на одному комп'ютері за допомогою так званих віртуальних хостів. В першу чергу потрібно налаштувати Windows на «впізнавання» цих доменних імен. Тобто задати відповідності ім'я ? IP-адреса. Для цього звернемося до файлу **%System32%\drivers\etc\hosts** (**%System32%** - це звичайно **C:\Windows\System32** або **C:\Winnt\System32**). В ньому після пояснення ми знайдемо список відповідностей імен та IP-адрес. Додамо поки що одне нове ім'я – **tm**. Відредагований файл буде мати вигляд:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host

127.0.0.1        localhost
127.0.0.1        tm
```

Тепер звернімося до папки **extra**, яка знаходиться в тій самій папці, що й файл **httpd.conf**. У ній ми знайдемо файл **httpd-vhosts.conf**. Відкриємо його й внесемо наш новий віртуальний хост:

```
# Virtual Hosts
#
# If you want to maintain multiple domains/hostnames on your
# machine you can setup Virtual Host containers for them.
#... (для скорочення пропускаємо подальші коментарі)
```

```
# Use name-based virtual hosting.
#
NameVirtualHost *:80

# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#

<VirtualHost *:80>
    DocumentRoot "c:/www/tm"
    ServerName tm
</VirtualHost>
```

Зверніть увагу: слеш **прямий**: c:/www/tm.

Тепер шукаємо в httpd.conf рядок **#Include conf/extra/httpd-vhosts.conf** (номер цього рядка приблизно 467-й) і забираємо знак коментаря (#) з початку рядка. Наступний крок: створення папки c:\www\tm.

7. Правимо директиву DirectoryIndex (приблизно 245-й рядок файла **httpd.conf**), щоб включити в список пошуку файлу за замовчуванням в WEB-папці файли **index.php DirectoryIndex index.html index.htm index.php**

8. Створення конфігураційного файла

Перейменовуємо c:\php\php.ini-production у **php.ini**

9. Перезапускаємо apache

У випадку вдалої установки Апача в правій нижній частині екрана є піктограма виклику монітора Apache.



Подвійним кліком запускаємо його й натискаємо **Restart**. Після чого закриваємо вікно монітора Апача.

В деяких останніх версіях Windows так перезапустити Apache не вдасться. До того ж можна навіть не помітити, що Apache не перезапустився: зовні все буде виглядати як при успішному запуску. В цьому випадку доведеться перезапустити **службу** Apache через панель управління Windows.

10. Перевірка

Створюємо файл **C:\www\tm\index.php** наступного змісту: `<?php phpinfo(); ?>` і запускаємо в браузері адресу `http://localhost/`. У випадку успіху ви побачите таблицю параметрів php.

11. Налаштування php

Редагування файла php.ini. Мета: підключити потрібні нам бібліотеки функцій. У рядку 813 треба поправити директиву `extension_dir`: вона повинна мати вигляд `extension_dir = "c:/php/ext"` (без крапки з комою на початку!). Розділ розширень (**Dynamic Extensions**) починається приблизно на 655-му рядку. В ньому ми побачимо список розширень. Знак `;` на початку – це коментар. Тобто, якщо ми стираємо `;` на початку рядка, ми тим самим включаємо відповідне розширення. А якщо ставимо `;` на початку рядка, – відключаємо відповідне розширення. Список розширень з коментарями можна знайти за адресою: <http://www.php.net/manual/en/install.windows.extensions.php>

Включимо три розширення, які будуть потрібні нам у роботі:

- **php_gd2.dll** – функції для роботи з графікою (953-й рядок файла php.ini);
- **php_mysql.dll** – функції для роботи с MySQL (963-й рядок файла php.ini);

- **php_mysqli.dll** – функції для роботи с MySQL (964-й рядок файла php.ini).

Зверніть увагу: є дві бібліотеки функцій для роботи с MySQL – стара й нова. Документація php рекомендує використовувати нову – **php_mysqli.dll**. Проте більшість сайтів і додатків «за звичкою» використовують стару. Тому ввімкнемо обидві, тим більше, що вони не конфліктують.

12. Перезапускаємо apache.

13. Встановлення й налаштування MySQL

Встановлення MySQL дуже просте. Труднощі можуть виникнути хіба що з налаштування кирилиці.

Встановлення Apache і PHP на Linux

Хоча в більшість дистрибутивів розробники включають вже скомпільовані пакети, ми все-таки розглянемо збирання Apache і PHP з вихідних кодів. **Почнемо з Apache.** Останню версію качаємо тут: <http://httpd.apache.org>.

Архів повинен мати приблизно таку назву: `httpd-2.x.xx.tar.bz2`. Скачуємо його та зберігаємо в каталозі `/usr/local/src` чи в іншому зручному для вас місці. Тепер переходимо в каталог з архівом і розпаковуємо:

```
# cd /usr/local/src
# bunzip2 httpd-2.x.xx.tar.bz2
```

Після цього зникне розширення `.bz2`. Далі виконуємо:

```
# tar xvf httpd-2.x.xx.tar
```

Переходимо в папку `httpd-2.x.xx` (сюди розпакувався архів) і починаємо компіляцію. Для цього спершу виконуємо команду `configure`. До неї можна додати необхідні параметри. Наприклад, для того, щоб завантажити модуль PHP, треба встановити підтримку DSO. Це можна зробити, додавши до команди `configure` параметр `-enable-module=so`. Опція `-prefix` дає змогу змінити каталог для інсталяції – для цього після неї просто вводьте назву потрібної папки. Якщо хочете отримати довідку по цій команді, введіть в консолі `configure --help`.

```
# cd httpd-2.x.xx
# ./configure --enable-module=so
```

Після цього в терміналі будуть з'являтися різні букви J – команда `configure` шукатиме найкращі варіанти налаштування для компіляції. По завершенні цього процесу знову стане доступним командний рядок і можна буде продовжити встановлення. Команда `make` запускає процес компіляції: **# make**

Знову з'явиться довга низка рядків. Швидкість компіляції залежатиме від потужності комп'ютера. В кінці повинно вивестись повідомлення такого типу:

```
make [1]: Leaving directory '/usr/local/src/httpd-2.x.xx'
```

Це означає, що процес компіляції пройшов без помилок. Тепер можна встановити зібрану програму: **# make install**

От і все. Apache готовий до роботи. Запускаємо за допомогою команди `apachectl start`, вводимо в будь-якому браузері `localhost` або `127.0.0.1`. Якщо не з'явилося повідомлення про помилку завантаження сторінки, то ви все зробили правильно.

Встановлення PHP. Свіжу версію можна скачати звідси: www.php.net/downloads.php. У компіляції продукт мало чим відрізняється від Apache. Скачаний архів також зберігаємо в `/usr/local/src`, і розпаковуємо:

```
# cd /usr/local/src
# bunzip2 php-5.x.x.tar.bz2
# tar xvf php-5.x.x.tar
# cd php-5.x.x
```

Детальніше зупинимось на команді `configure`. Для того щоб додати підтримки MySQL, використовується опція `-with mysql`. Після неї вказуємо шлях до програми `mysql_config`. Також необхідно включити опції `-with-apxs` для Apache або `-with-apxs2` для Apache 2.0 і вказати місце знаходження програми `apxs`. Приклад налаштування для стандартної інсталяції Apache 2:

```
# ./configure --with-apxs2=/usr/local/apache2/bin/apxs
```

Після конфігурування вводимо: **# make**. Після вдалого завершення має з'явитись наступний напис: **Build complete. (It is safe to ignore warnings about tempnam and tmpnam)**. Останній крок – встановити щойно зібраний модуль PHP. Вводимо: **# make install**. Потім налаштовуємо файли з розширенням .php так, щоб вони оброблялись модулем PHP. В файл httpd.conf додаємо рядок:

```
AddType application/x-httpd-php .php
```

При необхідності можна вказати альтернативні розширення. Перезапускаємо Apache:

```
# apache2ctl restart
```

Напишемо простий скрипт, який назвемо info.php, за допомогою якого перевіримо роботу PHP: **phpinfo (); ?>**

Зберігаємо його в /usr/local/apache2/htdocs/index.php або в іншому каталозі, який призначений для тестування скриптів на локальній машині, запускаємо браузер, вводимо в рядку адреси http://localhost. Повинна з'явитись сторінка з детальним описом конфігурації PHP.

Встановлення готових пакетів

Спочатку необхідно дізнатись, які пакети є в репозитарії:

```
# aptitude update
```

```
# aptitude search apache
```

```
# aptitude search php5
```

```
# aptitude search mysql
```

Буде видано великий список пакетів. Для установки виберемо наступні:

```
# aptitude install apache2 apache2-mpm-prefork apache2-utils\
```

```
> libapache2-mod-php5 php5 \
```

```
> php5-cli php5-common php5-curl \
```

```
> php5-gd php5-imagick php5-mysql \
```

```
> php5-xmllrpc php5-xsl \
```

```
> mysql-client-5.0 mysql-server-5.0
```

При цьому менеджер пакетів АРТ автоматично перевірить залежності і доставить решту пакетів. Разом вони займуть близько 40 Мб. Потрібно закоментувати в файлі /etc/apache2/apache2.conf рядок 189. Зберігаємо зміни в файлі, запускаємо сервер командою apache2 (для цього необхідні права адміністратора) і вводимо http://localhost.

Тепер вкладаємо наш PHP-скрипт в папку /var/www/apache2-default і набираємо http://localhost/index.php. Якщо відкрилась сторінка з інформацією про модуль PHP5, то все зроблено правильно, і сервер коректно налаштований. Для керування використовується команда apache2ctl (для першої версії просто apachectl), після команди через пробіл вводиться дія (stop, start, restart). Ця команда доступна тільки користувачу root, оскільки вона знаходиться в папці /usr/sbin. Якщо треба, щоб кожен міг запускати сервер, можна пересунути файл з /usr/sbin/apache2ctl в /usr/bin/apache2ctl, або дати доступ на виконання звичайному користувачу.

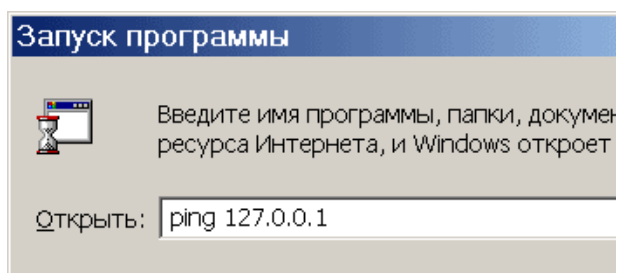
Також звичайному користувачеві заборонено записувати в папку /var/www/apache2-default, тому даємо йому такі права: **# chmod a+rw /var/www/apache2-default -R**

При необхідності даємо право на виконання PHP-скриптів: **# chmod a+x /var/www/*.php**

Установка комплексу Денвер

1. Підготовка до робот из мережею

Установка драйверів і мережевих протоколів, які дозволять Apache запуснитися і працювати на локальній машині: **Пуск — Выполнить:**



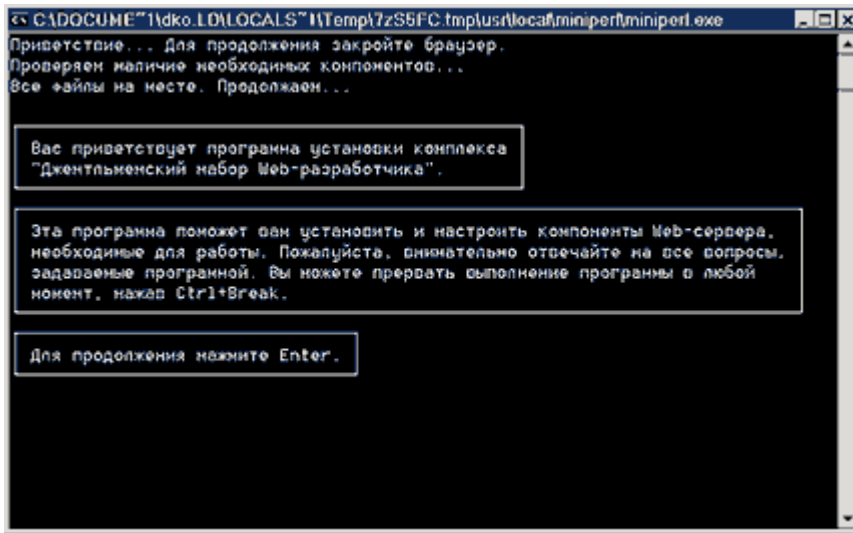
Після натиснення Enter бачимо наступне:

```
Обмен пакетами с 127.0.0.1 по 32 байт:
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

Процес повинен тривати кілька секунд. В цьому випадку можна приступати до інсталяції дистрибутиву. У випадку ж, якщо вікно відкриється і одразу закриється, потрібно продовжити роботу із встановлення мережевих протоколів.

2. Установка дистрибутиву

Після запуску інсталятора Денвера з'являється вікно:



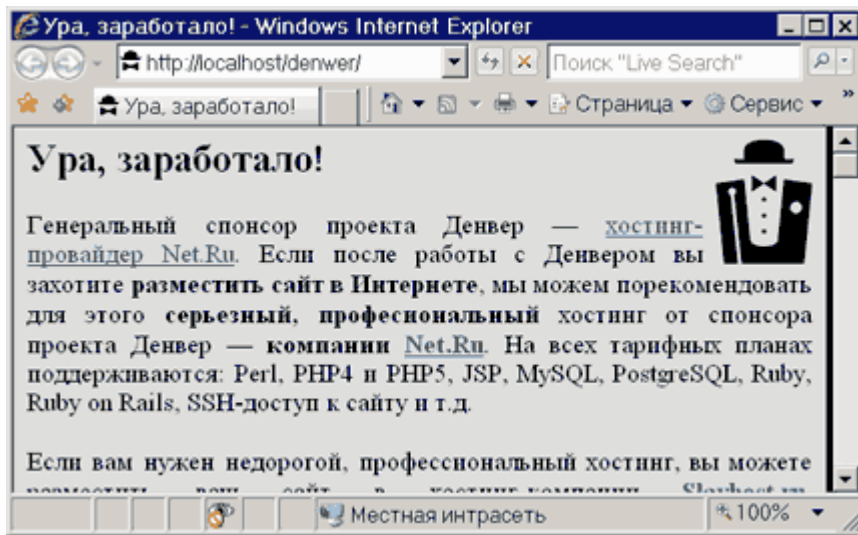
За замовчуванням комплекс встановлюється в каталозі C:\WebServers (натисненням Enter підтверджуємо свою згоду з цим). У вказаному каталозі будуть розміщені абсолютно всі компоненти системи, і поза ним жодні файли в подальшому не створюються. Далі пропонується ввести ім'я віртуального диску, який буде пов'язаний із щойно вказаною директорією. Рекомендується погодитися із значенням за замовчуванням (z:).

Після цього почнеться копіювання файлів дистрибутива, а під кінець вам буде поставлено питання, як саме ви збираєтесь запускати і зупиняти комплекс. У вас є дві альтернативи:

- Створювати віртуальний диск при завантаженні машини (інсталятор потурбується, щоб це відбувалося автоматично), а при зупинці серверів його (диск) не відключати. Це найзручніший режим.
- Створювати віртуальний диск тільки по явній команді старту комплексу (при клацанні по ярлику запуску на Робочому столі). І, відповідно, відключати диск від системи при зупинці серверів.

3. Перший запуск Денвера

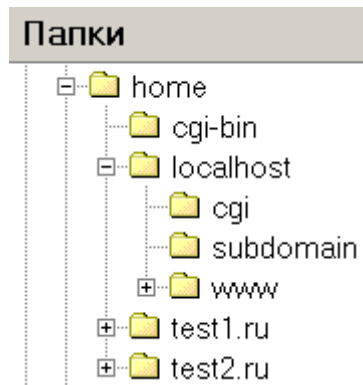
Клацайте по створеному інсталятором ярлику Start Denwer на Робочому столі, а потім, дочекавшись, коли усі консольні вікна зникнуть, відкривайте браузер і набирайте в ньому адресу: <http://localhost/denwer/>. Виходити з Інтернету при цьому не обов'язково.



4. Работа з віртуальними хостами

Перш ніж продовжити, переконайтеся, що у вас запущена служба "DNS-клієнт". Це можна зробити, відкривши Панель управління – Адміністрування – Служби. Інакше віртуальні хости працювати не будуть. При розробці Web-сайтів рhexуї обслуговувати одним сервером одразу кілька хостів. Іншими словами, ввівши у браузері шлях `http://localhost`, ви потрапите на один сайт, а, надрукуювши `http://test1.ru`, - зовсім на іншій (але теж на локальній машині).

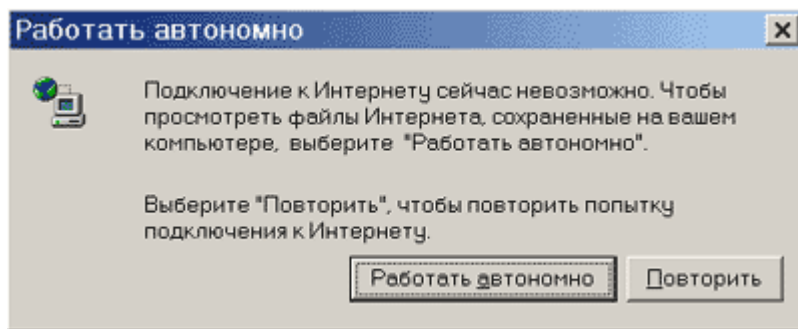
Додати новий віртуальний хост в Денвері надзвичайно просто. Нехай це буде `test1.ru`. Треба виконати наступне:



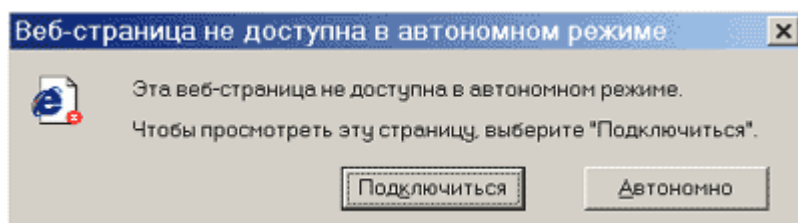
- Створити в папці `/home` директорію з ім'ям, що співпадає з іменем віртуального хоста (у нашому випадку `test1.ru`). Ця директорія зберігатиме директорії документів доменів третього рівня для `test1.ru`. На малюнку показано, як може виглядати директорія `/home`. Не забудьте створити папку `www` в директорії віртуального хоста, адже саме в ній зберігатимуться його сторінки і скрипти!
- Перезапустити сервер, скориставшись, наприклад, ярликом `Restart Denwer` на Робочому столі.

5. Контролер віддаленого доступу

Може статися, що при першому відкритті хоста контролер віддаленого доступу пропонуватиме вам альтернативу на кшталт наступної:



або таке:



В цьому випадку завжди вибирайте Підключитися або Повторити.

6. Проксі-сервер

Багато версій Windows поставляються з включеним за замовчуванням проксі-сервером. Це може викликати деякі проблеми при роботі з Денвером.

- Якщо після запуску Денвера сторінка <http://localhost> не працює, найімовірніше, вам треба відключити проксі-сервер в налаштуваннях браузеру. Для "простих" хостів (localhost, test, dklab і т. д.) досить прапорця "Не використовувати проксі-сервер для локальних адрес" на вкладці Властивості оглядача – Підключення – Налаштування мережі – Додатково.
- Якщо localhost працює, а test1.ru (і взагалі хости, ім'я яких складається з декількох частин) – ні, ймовірно, браузер не може розпізнати останній хост як локальний. В цьому випадку необхідно або повністю відключити проксі-сервер, або ж перерахувати хости в списку Підключення – Налаштування мережі – Додатково – Виключення.

ЛАБОРАТОРНА РОБОТА №9

Тема: Організація DNS-сервера (ОС Windows 2003 Server, ОС Linux)

Мета: оволодіти основними навиками встановлення та налаштування DNS-сервера в операційних системах Windows Server 2008 та Linux.

Теоретичні відомості

Доменна система імен (Domain Name System, DNS) – це розподілена база даних, яка містить інформацію про комп'ютери (хости), підключені до мережі Інтернет. Найчастіше інформація включає ім'я машини, IP-адресу та дані для маршрутизації пошти.

Для звернення до хостів в мережі Інтернет використовуються 32-розрядні IP-адреси, що однозначно ідентифікують будь-який комп'ютер в цій мережі. Однак для користувачів застосування IP-адрес при звертанні до хостів є незручним. Тому було створено систему перетворення імен, яка дозволяла б комп'ютеру у випадку відсутності у нього інформації про відповідність імен та IP-адрес отримати необхідні відомості від DNS-сервера, IP-адреса якого зберігається в налаштуваннях підключення до Інтернет.

Таким чином, основне завдання DNS – перетворення імен комп'ютерів в IP-адреси і навпаки.

Для реалізації системи DNS було створено спеціальний мережений протокол DNS. В мережі також є спеціальні виділені інформаційно-пошукові сервери – DNS-сервери.

DNS-сервери (сервери імен DNS) – це комп'ютери, на яких зберігаються ті частини бази даних простору імен DNS, за які дані сервери відповідають, і, на яких функціонує програмне забезпечення, що обробляє запити DNS-клієнтів і видає на них відповіді.

DNS-клієнт – це будь-який мережений вузол, який звернувся до DNS-сервера для перетворення імені вузла в IP-адресу чи, навпаки, IP-адреси в ім'я вузла.

Основою DNS є уявлення про ієрархічну структуру доменного імені. Кожен сервер, відповідальний за ім'я, може передавати відповідальність за наступну частину домена іншому серверу (з адміністративної точки зору – іншій організації чи людині). Це дозволяє скласти відповідальність за актуальність інформації на сервери різних організацій (людей), що відповідають тільки за «свою» частину доменного імені.

Характеристики DNS:

- **Розподіленість адміністрування** (відповідальність за різні частини ієрархічної структури несуть різні люди чи організації)
- **Розподіленість зберігання інформації** (кожен вузол мережі в обов'язковому порядку повинен зберігати тільки ті дані, як і входять в зону його відповідальності і (можливо) адреси кореневих DNS-серверів)
- **Кешування інформації** (вузол може зберігати деяку кількість даних не із своєї зони відповідальності для зменшення навантаження на мережу)
- **Ієрархічна структура** (усі вузли об'єднані в дерево, і кожен вузол може або самостійно визначати роботу розміщених нижче вузлів, або передавати їх іншим вузлам)
- **Резервування** (за зберігання і обслуговування своїх вузлів (зон) відповідають (зазвичай) кілька серверів, розмежованих як фізично, так і логічно, що забезпечує збереженість даних та продовження роботи навіть у випадку збою одного з вузлів).

Як працює DNS. Для перетворення імен машин в IP-адреси програми прикладного рівня, такі як Netscape Navigator і т. п., викликають підпрограму gethostbyname. Якщо конфігурація машини передбачає використання DNS, gethostbyname запитує адресу в сервера імен, IP-адреса якого вказана в налаштуваннях підключення до Інтернет.

Сервери імен бувають рекурсивними та нерекурсивними. Нерекурсивний сервер діє наступним чином: якщо у нього є адреса, кешована з попереднього запиту, або якщо вона авторитетна для домена, до якого відноситься ім'я, то він дає відповідну відповідь. В протилежному випадку замість правильної відповіді він відсилає до авторитетних серверів іншого домена, які повинні знати відповідь.

Рекурсивний сервер повертає тільки реальні відповіді та повідомлення про помилки. Базова процедура обробки запиту по суті така ж; єдина відмінність полягає в тому що цей сервер імен сам займається обробкою відсилок (відсилань), не передаючи їх клієнту.

Проте у відслідковуванні сервером відсилань є один побічний ефект: у його кеш надходить інформація про проміжні домени. Серверу домена високого рівня (такого як com чи ua) не рекомендується зберігати інформацію, що запитується машиною, розміщеною на кілька рівнів нижче. Його кеш швидко наповниться, і через додаткові затрати часу на обробку рекурсивних запитів пропускна здатність сервера знизиться.

У зв'язку з цим сервери імен нижчих рівнів зазвичай є рекурсивними, а сервери вищих рівнів (верхнього чи частково другого) – нерекурсивними.

Динамічний DNS – технологія, що дозволяє інформації на DNS-сервері оновлюватися в реальному часі, і (за бажанням) в автоматичному режимі. Вона застосовується для присвоєння постійного доменного імені пристрою (комп'ютеру, мереженому накопичувачу) з динамічною IP-адресою. Це може бути IP-адреса, отримана по DHCP чи по PCP в PPP-з'єднаннях (наприклад, при віддаленому доступі через модем). Інші машини в Інтернеті можуть встановлювати з'єднання з цією машиною по доменному імені і навіть не знати, що IP-адреса змінилася.

Динамічна DNS також часто застосовується в локальних мережах, де клієнти отримують IP-адресу по DHCP, а потім реєструють свої імена в локальному DNS-сервері.

Реалізація служби DNS в системах сімейства Windows Server

Головна особливість служби DNS в системах сімейства Windows Server полягає в тому, що служба DNS розроблялася для підтримки служби каталогів Active Directory. Для виконання цієї функції необхідно забезпечити дві умови:

- підтримка службою DNS динамічної реєстрації (dynamic updates);
- підтримка службою DNS записів типу SRV (**Записи DNS**, или **Ресурсные записи** — единицы хранения и передачи информации в DNS. SRV – один із різновидів записів в DNS. Вказує розміщення серверів для різних сервісів. SRV запис складається з таких частин: service proto priority weight port hostname).

Служба DNS систем Windows Server задовольняє обидві умови.

Приклади управління службою DNS:

- установка служби DNS;
- створення основної та додаткової зони прямого перегляду;
- створення зони оберненого перегляду;
- виконання динамічної реєстрації вузлів в зоні.

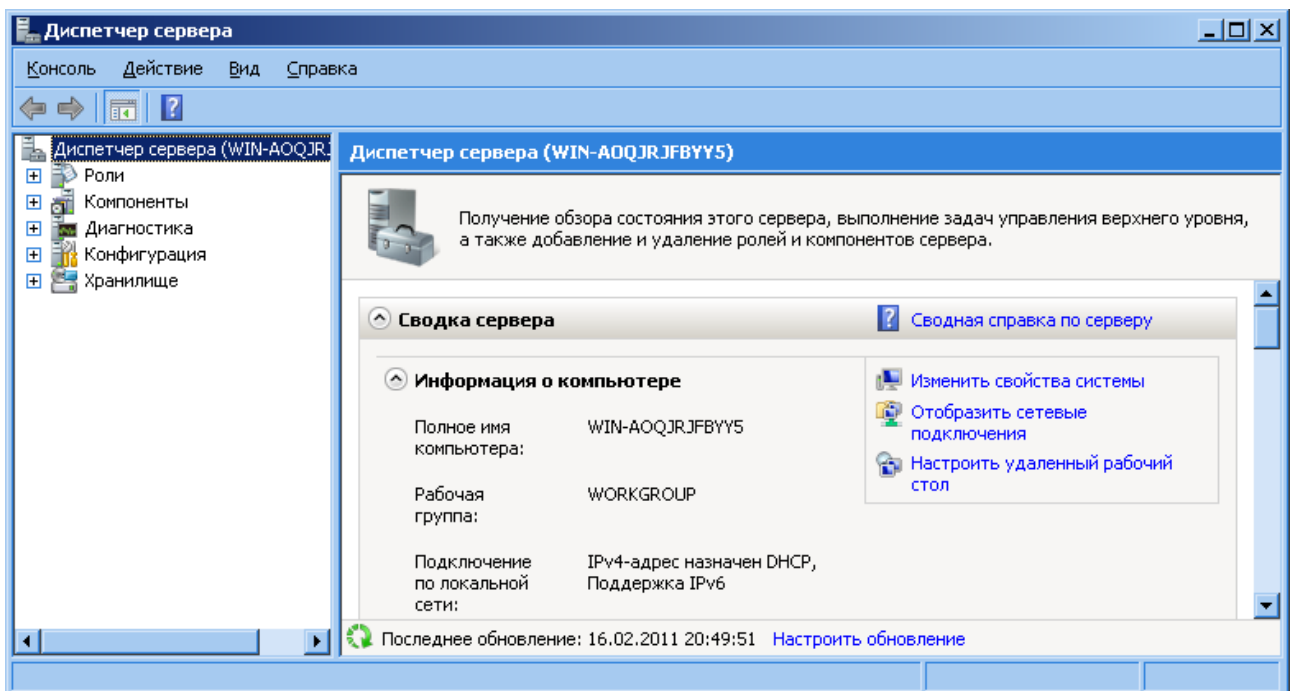
Зона прямого перегляду (*forward lookup zone*) – зони, які служать для перетворення імен вузлів в IP-адреси. Найчастіше для цього використовуються записи типу **A**, **CNAME**, **SRV**.

Зона оберненого перегляду (*reverse lookup zone*) – зони, які служать для визначення імені вузла за його IP-адресою. Основний тип запису PTR.

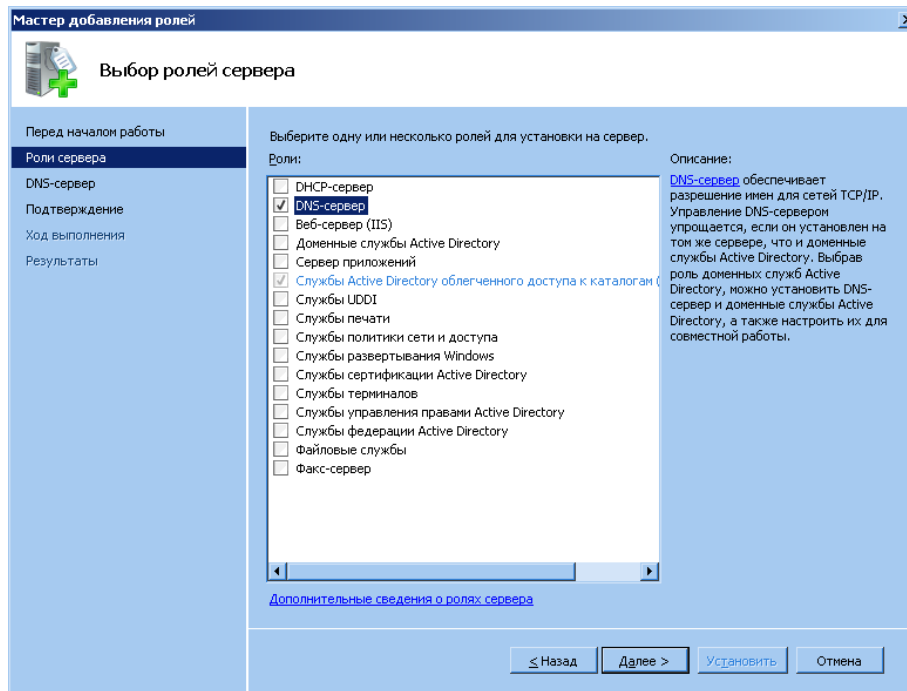
Порядок виконання роботи (ОС Windows Server)

Для установки DNS-сервера з Панелі управління (Control Panel):

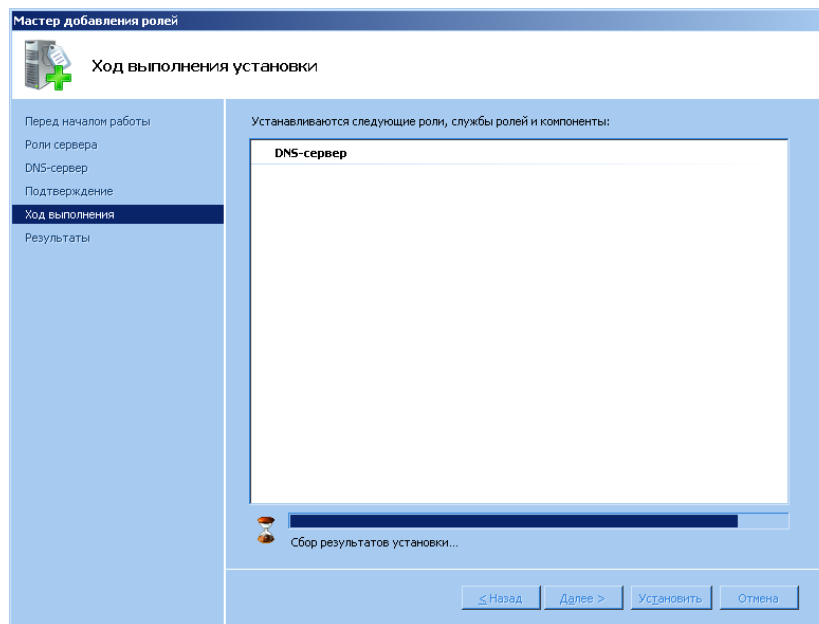
1. У меню Пуск (Start) вибрати Панель управління (Control Panel) і Адміністрування (Administrative Tools), потім Управління сервером (Server Manager).
2. Відкрити вкладку і вибрати об'єкт Ролі (Roles).



3. Натиснути Додати ролі (Add Roles) і дотримуюсь вказівок майстра, вибравши як ролі сервера DNS-сервер (DNS-server), натиснути Встановити (Install).



По завершенню установки, консоль управління DNS-сервером знаходиться в меню Пуск (Start) – Програми (All Programs) – Адміністрування (Administrative Tools) – DNS. У Windows 2008 вбудований майстер налаштування DNS-сервера.



Для конфігурації DNS-сервера потрібно дізнатися значення наступних термінів:

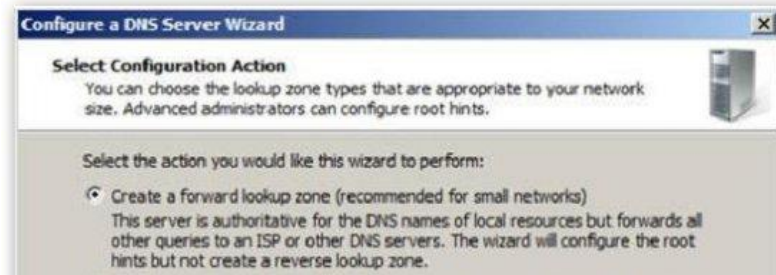
- Зона прямого перегляду (Forward lookup zone) – відповідає за перетворення імен хостів в IP-адреси.
- Зона зворотного перегляду (Reverse lookup zone) – відповідає за розпізнавання DNS-сервером DNS-імені хоста. Наявність зони зворотного перегляду не обов'язкова, але вона легко налаштовується і забезпечує повну функціональність DNS в Windows Server 2008 Server.
- Типи зон (Zone types) – надаються наступні варіанти: Active Directory (AD) Integrated (Інтегрована в AD), Standard Primary (Основна), і Standard Secondary (Додаткова). Зона «AD Integrated» зберігає інформацію про розподіленій базі даних в AD і дозволяє здійснювати безпечно оновлення бази даних.

Щоб відкрити майстра налаштування DNS-сервера:

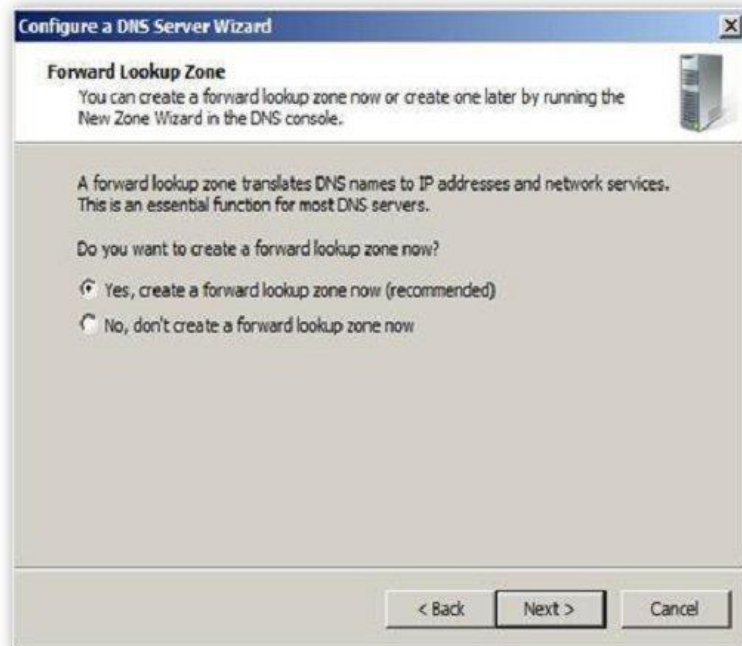
1. Вибрати об'єкт DNS з папки Адміністрування (Administrative Tools), щоб відкрити консоль управління DNS-сервером.

2. Видалити ім'я даного комп'ютера і натиснути Дія (Action) - Конфігурація DNS-сервера (Configure a DNS Server), щоб запустити Майстер налаштування DNS-сервера.

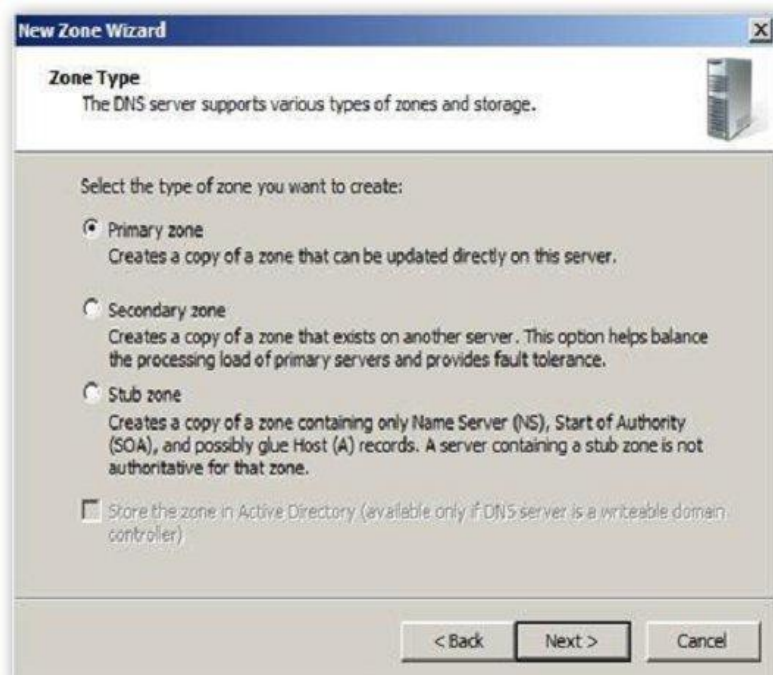
3. Натиснути Далі (Next) і вибрати об'єкт налаштування: зона прямого перегляду (forward lookup zone), зони прямого і зворотного перегляду (forward and reverse lookup zone), тільки кореневі посилання (root hints only)



4. Натиснути Далі (Next) і потім Так (Yes) для того, щоб створити зону прямого перегляду.

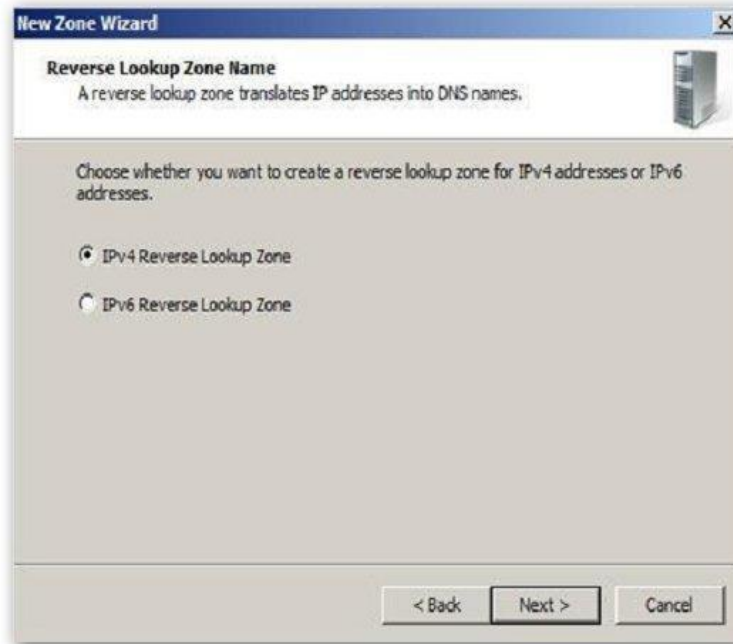


5. Вибрати відповідний тип зони.

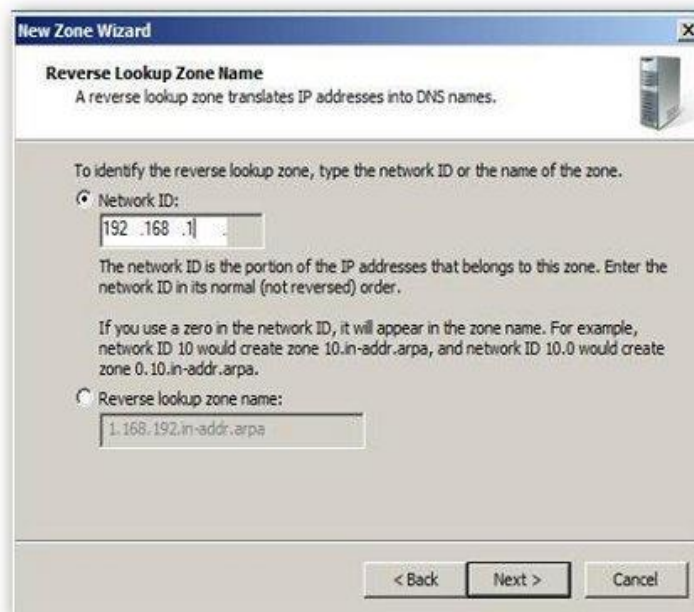


6. Натиснути Далі (Next) і ввести ім'я створюваної зони. Натиснути Далі (Next) і потім Так (Yes) для того, щоб створити зону зворотного перегляду.

7. Вибрати протокол зони зворотного перегляду: IPv4 або IPv6.



8. Натиснути Далі (Next) і ввести ідентифікатор зони зворотного перегляду.



Можна створити новий або використовувати копію вже існуючого файлу DNS



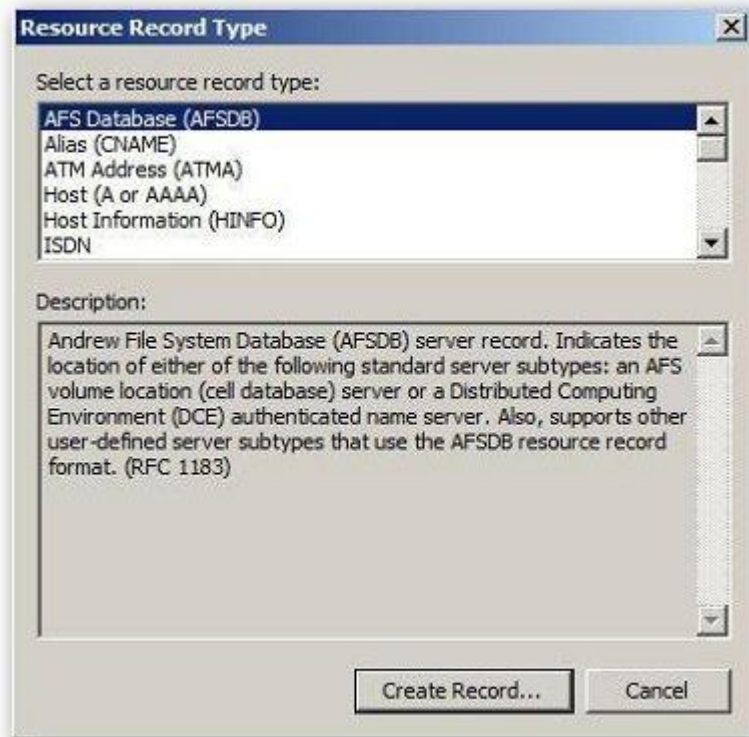
10. У вікні Динамічне оновлення (Dynamic Update) вибрати спосіб оновлення DNS: безпечний (secure), небезпечний (nonsecure), не отримувати динамічні оновлення (no dynamic updates). При бажанні можна включити перенаправляючий DNS-сервер у вікні Перенаправлення (Forwarders).



Після установки і налаштування DNS-сервера можна додавати записи в створену зону. Існує кілька типів записів DNS, багато з яких інколи не використовуються. Нижче перераховані основні записи:

- **Запис SOA (Start of Authority) – початковий запис зони.** Запис SOA є первинним в будь-якій стандартній зоні. На вкладці запис зони (Start of Authority) при необхідності можна провести будь-які налаштування, наприклад, змінити первинний сервер, на якому зберігається запис SOA або вибрати особу, відповідальну за управління SOA.
- **Запис NS (Name Server) – Сервер імен.** Записи Серверів імен (Name Servers) визначають імена серверів для конкретного домену. З їх допомогою встановлюються всі імена первинних і вторинних серверів.
- **Запис A (Host) – Запис вузла.** Запис A пов'язує ім'я хоста з IP-адресою. З їх допомогою сервери розпізнаються в зоні прямого перегляду, а виконання запитів в середовищі з зонами відбувається значно краще.
- **Запис PTR (Pointer) – Показчик.** Для виконання зворотних запитів показчики (PTR) створюють відповідні вхідні повідомлення в зоні оберненого перегляду. Як видно на зображенні H, при створенні хоста можна також створити та запис PTR. Якщо ви не скористалися цією опцією в той момент, створити показчик можна буде в будь-який час.
- **Запис CNAME (Canonical Name) або Alias – Канонічна запис імені.** Канонічне ім'я (CNAME) або псевдонім дозволяє DNS-сервера призначати безліч імен одного вузла. Наприклад, псевдонім може містити декілька записів, що вказують на один сервер в середовищі. Це часто застосовується в тому випадку, якщо веб-сервер і поштовий сервер знаходяться на одній машині.
- **Запис MX (Mail Exchange) – Поштовий обмінник.** Даний запис указує поштові сервери обміни поштою в базі даних DNS всередині зони. З її допомогою можна призначити пріоритети і відстежувати розміщення всіх поштових серверів.

Можна створювати й інші види записів. Для докладного опису у вікні консолі DNS виконується з меню Дія (Action) команда Інші записи (Other New Records), вибирається будь-який запис з його описом.



Порядок виконання роботи (ОС Linux)

1. Перш за все необхідно вибрати відповідний сервіс Dynamic DNS. Нехай це буде сервіс DynDNS (<http://www.dyndns.com>). На ньому можна отримати безкоштовно два домени третього рівня.

2. Реєстрація аккаунта. Реєстрація на сервісі DynDNS дуже проста. Потрібно заповнити декілька полів (username, email, password) і погодитися з правилами (policy). Після реєстрації на електронну адресу, вказану при реєстрації, буде вислано лист з підтвердженням реєстрації. Пряме посилання на сторінку реєстрації: <https://www.dyndns.com/account/create.html>.

3. Створення домена. Домен створюється так само просто, як проходить реєстрація. Перейти на сторінку реєстрації домена (<https://www.dyndns.com/account/services/hosts/add.html>) і заповнити необхідні поля.

- Hostname – вказуємо бажане ім'я і вибираємо на власний розсуд доменне ім'я другого рівня.
- Wildcard – ставимо галочку, якщо хочемо щоб працювали імена на зразок ftp.host.domain.org або www.host.domain.org
- Service type – залишаємо значення за замовчуванням (Host with IP address).
- IP address – залишаємо без змін (тут буде вказаний поточна IP -адреса).

Після заповнення необхідних полів натиснути на кнопку Create Host. Домен створено. Ще можна створити один безкоштовний домен.

4. Установка і налаштування клієнта. Будемо працювати з клієнтом inadyn, він дуже простий і легко налаштовується. Установка клієнта буде автоматичною, оскільки він є в репозиторії (принаймні він є в репозиторії Ubuntu). Встановлюємо клієнта ось так: `sudo apt - get install inadyn`.

Тепер необхідно створити файл конфігурації /etc/inadyn.conf (за замовчуванням він не створюється). Є можливість створити файл конфігурації автоматично, для цього скористаємося механізмом створення файлу конфігурації (<https://www.dyndns.com/support/tools/clientconfig.html>), який нам надає сервіс DynDNS. На сторінці створення файлу конфігурації вибираємо необхідний домен, клієнта і тиснемо кнопку Generate.

Тепер залишилося скопіювати отриману конфігурацію і вставити її у файл. Нам ще треба додати у файл свій логін і пароль (логін і пароль які ми використали при реєстрації на сервісі). Тепер можна зробити перший запуск клієнта (`sudo /usr/sbin/inadyn`).

5. Потрібно так само проконтролювати роботу програми. Це можна зробити подивившись лог файл (/var/log/syslog). Найпростіший спосіб це зробити командою tail (tail - n5 /var/log/syslog). У лог файлі повинні з'являтися рядки на зразок наступних:

INADYN: Started 'INADYN version 1,96' - dynamic DNS updater.

INADYN: IP address for alias 'mea.homelinux.com' needs update to 'xxx.xxx.188.75'

INADYN: Alias 'mea.homelinux.com' to IP 'xxx.xxx.188.75' updated successful.

6. Тепер нам необхідно настроїти запуск клієнта автоматично і найпростіший спосіб це запуск клієнта через cron. Викликаємо на редагування кронтаб (sudo crontab - e). Додаємо рядок запуску (@reboot /usr/sbin/inadyn). Зберігаємо кронтаб і виходимо. Перевіряємо чи зберігся в кронтабе наш рядок (sudo crontab - l). Дивимось чи запущений клієнт (ps - A | grep inadyn). На цьому усі роботи можна вважати завершеними і тепер ваші динамічні IP-адреси прив'язуватимуться до ваших доменів.

ЛАБОРАТОРНА РОБОТА №10

Тема: Знайомство з службами каталогів (ОС Windows 2003 Server, ОС Linux)

Мета: ознайомитися із службою каталогів Active Directory

Теоретичні відомості

Служба каталогів (Directory Service) – програмний комплекс, який дає змогу адміністратору працювати з упорядкованим масивом інформації про мережеві ресурси (загальні папки, сервера друку, принтери, користувачі).

Цей масив зберігається в одному місці, що дозволяє централізовано керувати як самими ресурсами, так і інформацією про них, а також дає змогу контролювати їх використання третіми особами.

Служби каталогів мають цілий ряд:

- комерційних реалізацій (Active Directory, Novell eDirectory, iPlanet Directory);
- вільних програмних реалізацій (OpenLDAP, Apache Directory Server, Fedora Directory Server).

Active Directory — LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів за допомогою Microsoft Systems Management Server 2003, а також встановлювати оновлення операційних систем, прикладного та серверного ПЗ на всіх комп'ютерах в мережі.

Active Directory зберігає дані і налаштування середовища в централізованій базі даних.

LDAP (Lightweight Directory Access Protocol – це мережевий протокол для доступу до служби каталогів X.500, розроблений IETF як полегшений варіант розробленого ІТУ-Т протоколу DAP. LDAP – відносно простий протокол, що використовує TCP/IP і дозволяє проводити операції авторизації (bind), пошуку (search) та порівняння (compare), а також операції додавання, зміни або видалення записів.

Порядок виконання роботи

1. Налаштування сервера Сервер LDAP

Сервер LDAP складається з двох серверних процесів: slapd і slurpd.

Процес slapd займається прийомом і обробкою запитів від клієнтів; це основний процес, який безпосередньо працює з базою даних.

Сервіс slurpd використовується в тих випадках, коли дані потрібно реплікувати на інші сервери – він контролює зміни в базі і, при необхідності, пересилає їх на підпорядковані сервери.

Конфігураційні файли сервера LDAP:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/nis.schema
```

У перших етапах потрібно підключити необхідні схеми, які входять в OpenLDAP. Підключаються ті, які потрібно використовувати.

Схеми є частиною конфігураційного файлу, але винесені в окремі фрагменти:

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /etc/openldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/openldap/ssl/slapd.pem
```

LDAP можна використовувати для централізованої авторизації користувачів мережі замість NIS. У таких випадках з каталога може запитуватися конфіденційна інформація – наприклад, пароль. Для запобігання перехоплення таких даних бажано використовувати протокол LDAPS (LDAP via SSL / TLS):

```
database ldbm
```

Як спосіб зберігання використовується власний формат LDBM. Якщо передбачається звичайна конфігурація сервера, то цей формат кращий.

```
suffix "dc=example,dc=com"
```

Коренем інформаційної структури буде об'єкт `dc = example, dc = com`. У принципі, суфікс для каталогу можна взяти будь-який, в даному випадку `o = Example Inc`.

```
rootdn "cn=admin,dc=altlinux,dc=ru"
rootpw secret
```

DN описує адміністратора та його пароль. У даному випадку пароль записаний у відкритому вигляді, тому файл конфігурації сервера повинен мати відповідні права доступу, що обмежують його читання звичайними користувачами.

Пароль можна записати і у вигляді хешу DES чи MD5 – тоді рядок матиме наступний вигляд:

```
rootpw {MD5}IFJFxyGN3Nap7xsJFBmeTA==
```

Ці опції потрібні тільки на час первинної настройки бази. Після того як структура створена і можна регулювати права доступу за допомогою ACL, ці опції рекомендується відключити.

```
index objectClass eq
```

Формат `ldbm` підтримує найпростіші індекси з метою прискорення операцій пошуку. Такі індекси бажано створювати по атрибутах, що передбачає найбільшу кількість запитів. Останній параметр даної опції вказує за яким критерієм створюється індекс. Це можуть бути `pres`, `eq`, `approx`, `sub`, `none`. (`present`, `equality`, `approximate`, `substring`, `no index`).

```
access to attr=userPassword
  by dn=".*,ou=Admins,dc=example,dc=com" write
  by self write
  by anonymous auth
  by * none

access to * by * read
```

Після налаштування можна відразу запустити процес slapd - наприклад, такою командою:
slapd -u ldap -h ldap://127.0.0.1 / ldaps://ldap.altlinux.ru /

Перший об'єкт, який потрібно створити в базі - кореневий елемент (root entry), який вказаний в конфігураційному файлі як suffix.

2. Налаштування реплікації

Однією з важливих особливостей LDAP є вбудовані засоби реплікації даних. Цей механізм реалізований у вигляді окремого серверного процесу, контролюючого зміни в базі даних і ретранслює ці зміни на інші сервери.

Перш ніж включити таку реплікацію, необхідно переконатися в тому, що відповідні дані на обох серверах ідентичні. Це пов'язано з тим, що slurpd пересилає саме зміни на поточному сервері - він не перевіряє і не аналізує стан даних на віддаленому сервері.

Налаштування slurpd знаходяться в тому ж файлі, що і налаштування файла slapd.

```
replica /var/log/slapd.replog
```

Спочатку треба вказати файл, в який slapd буде записувати всі свої дії і з якого slurpd буде їх читати.

```
replica uri=ldap://ldap2.example.com  
bindmethod=simple  
binddn="cn=slurpd,ou=Apps,dc=example,dc=com"  
credentials=secret
```

Репліка такого виду описується для кожного підлеглого сервера.

На підпорядкованому сервері потрібно створити відповідний об'єкт і вказати, що він має права на зміну інформації. Це робиться за допомогою відповідного списку доступу і параметрів updatedn і updateref.

3. Налаштування клієнта

Існує величезна кількість клієнтів, що працюють з LDAP. Це можуть бути поштові програми, які звертаються до каталогу у пошуках адреси електронної пошти співробітника або за інформацією про маршрутизації пошти, FTP-сервер, який бере інформацію для авторизації свого клієнта і багато інших програм, але всі вони мають схожі налаштування.

Фрагмент настроювання поштового сервера Postfix:

```
virtual_maps = ldap:virtual, hash:/etc/postfix/virtual  
  
virtual_server_host = localhost  
virtual_search_base = ou=People,dc=example,dc=ru  
virtual_query_filter = (&(objectclass=inetLocalMailRecipient)(cn=%s))  
virtual_result_attribute = mailLocalAddress,mailRoutingAddress
```

ЛАБОРАТОРНА РОБОТА №11

Тема: Організація контролера домену засобами служб каталогів (ОС Windows 2003 Server, ОС Linux)

Мета: Оволодіти основними навиками встановлення та налаштування контролера домену засобами служб каталогів в операційній системі Windows Server 2008.

Теоретичні відомості

Одна із найважливіших концепцій роботи в мережах Windows пов'язана з доменом. Домен – це набір облікових записів користувачів та облікових записів комп'ютерів, які об'єднані разом таким чином, що ними можна централізовано управляти. Завдання контролера домену полягає у забезпеченні цього централізованого управління над ресурсами домену.

Будь-яка робоча станція, яка працює під управлінням операційної системи Windows XP, містить багато вбудованих облікових записів користувачів. Операційна система Windows XP навіть дозволяє створювати додаткові облікові записи користувачів на робочій станції. До тих пір, поки робоча станція працює як окрема система або є частиною рівноправної мережі, облікові записи цієї робочої станції (які ще називаються local user accounts або локальні облікові записи користувачів) не використовуються для контролю доступу до мережевих ресурсів. Замість цього локальні облікові записи користувачів використовуються для регулювання доступу до локального комп'ютера. Вони працюють в основному, як механізм, який гарантує, що адміністратори можуть виконувати підтримку робочої станції, при цьому кінцеві користувачі не зможуть втручатися в налаштування робочої станції.

Причина того, що локальні облікові записи не використовуються для контролю доступу до ресурсів за межами робочої станції, полягає в тому, що такий підхід призвів би до різкого збільшення навантаження на адміністраторів. Адже локальний обліковий запис користувача розміщується на кожній конкретній робочій станції. Це означає, що якби локальний обліковий запис користувача був би основним механізмом безпеки в мережі, то адміністратору довелося би фізично переміщуватися до комп'ютера, який містить обліковий запис, в той момент, коли необхідно внести які-небудь зміни в права для цього облікового запису. Це не надто велика проблема для невеликих мереж, але внесення змін в безпеку у великих мережах було б непосильним завданням.

Ще одна причина того, що локальний обліковий запис користувача не використовується для контролю доступу до мережевих ресурсів, полягає в тому, що їм не потрібно переміщуватися з користувачем від одного комп'ютера до іншого. Наприклад, якщо комп'ютер користувача вийшов з ладу, то користувач не може просто увійти в інший комп'ютер і працювати на ньому, поки не буде відремонтовано його власний, тому що обліковий запис користувача в цьому випадку зв'язаний з комп'ютером, який зламався. Щоб користувач зміг продовжити роботу, для нього необхідно створити новий обліковий запис на новому комп'ютері.

Це лише кілька причин того, чому непрактично використовувати локальні облікові записи користувачів для забезпечення безпеки мережевих ресурсів. Навіть якщо застосувати спробу використати такий тип безпеки, операційна система Windows не дозволить цього. Локальні облікові записи користувачів можна використовувати лише для забезпечення безпеки для локальних ресурсів.

Домен вирішує ці та інші проблеми за допомогою централізації облікових записів користувачів. Це полегшує адміністрування і дозволяє користувачам входити в мережу з будь-якого комп'ютера в мережі (якщо тільки не встановлено інших обмежень).

На серверах Windows, які працюють під управлінням операційних систем Windows 2000 Server, Windows Server 2003 чи Longhorn Server, робота контролера домену полягає в тому, щоб запускати службу Active Directory. Active Directory діє як сховище для об'єктів директорій. Серед цих об'єктів знаходяться облікові записи. Таким чином, одна з основних задач контролера домену полягає в наданні служб для аутентифікації.

Дуже важлива концепція, пов'язана з контролерами доменів, полягає в тому, що вони забезпечують саме аутентифікацію, а не авторизацію. Це означає, що коли користувач входить в мережу, контролер домену перевіряє ім'я користувача та пароль і підтверджує, що користувач

саме той, за кого себе видає. Однак при цьому контролер домену не зможе повідомити користувачу, до яких ресурсів у нього є доступ.

Безпека ресурсів в мережах Windows забезпечується за допомогою списків контролю доступу (access control lists или ACL). ACL – це просто список, який повідомляє, у кого на що є права. Якщо користувач намагається отримати доступ до ресурсу, він підтверджує свою автентичність (справжність) серверу, на якому міститься ресурс. Цей сервер перевіряє, що користувач пройшов аутентифікацію, а потім за допомогою посилань перевіряє за списком ACL, на які ресурси у нього є права.

Часто виникає необхідність, щоб користувачі із одного домену мали можливість отримати доступ до ресурсів, які розміщені в іншому домені. Для цього компанія Microsoft створила довірчі відносини як спосіб для забезпечення такого доступу. Довірчі відносини працюють наступним чином. Нехай є адміністратор, на домені якого містяться ресурси, до яких хочуть отримати доступ користувачі з іншого домену. Адміністратори кожного з доменів не можуть контролювати того, хто створює облікові записи користувачів в іншому домені. Якщо адміністратор першого домену довіряє компетентності та професіоналізму адміністратора другого домену, то він може встановити довірчі відносини, щоб таким чином його домен довіряв членам іншого домену.

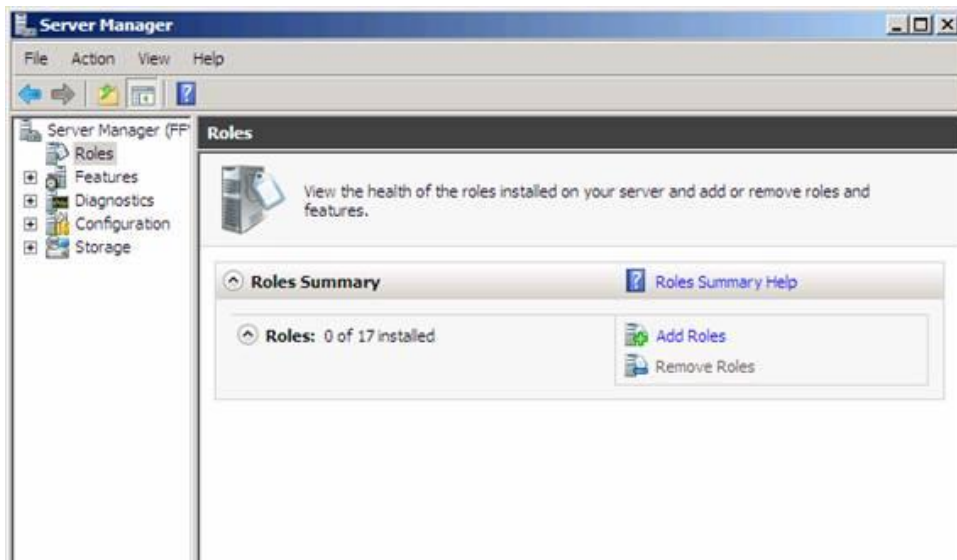
Типи довірчих відносин:

- Односторонні довірчі відносини. Це однонаправлений канал аутентифікації між двома доменами. Такі відносини між доменами А і В означають, що користувачі домену А можуть отримати доступ до ресурсів домену В. Однак користувачі з домену В не можуть отримати доступ до ресурсів домену А. Довірчі відносини можуть бути транзитивними та нетранзитивними:
 - транзитивні довірчі відносини проходять через групу доменів, таку як дерево доменів, і формують зв'язок між деяким доменом та всіма доменами, які йому довіряють (якщо домен А довіряє домену В, а В довіряє домену С, то А довіряє С); транзитивні відносини можуть бути одно- або двосторонніми;
 - нетранзитивні довірчі відносини обмежені двома доменами (хоча домен А довіряє домену В, а домен В довіряє домену С, довірчі відносини між А та С відсутні); нетранзитивні відносини також можуть бути одно- або двосторонніми.
- Двосторонні довірчі відносини. У двосторонніх довірчих відносинах домен А довіряє домену В, а В довіряє А. Це означає, що запити на аутентифікацію можуть передаватися між цими доменами в обох напрямках. Двосторонні довірчі відносини можуть бути як транзитивними, так і не транзитивними.

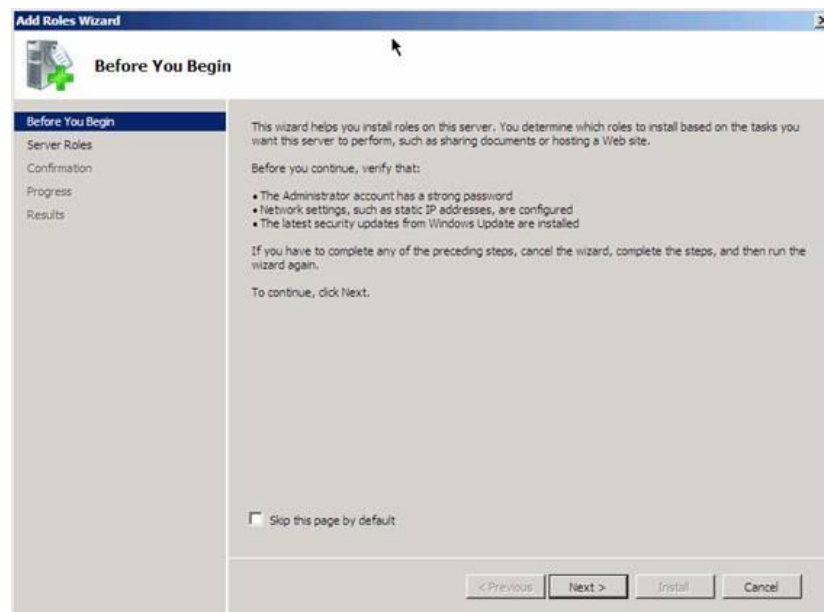
Те, що контролери домену здійснюють аутентифікацію, а не авторизацію, залишається справедливим, навіть якщо справа стосується довірчих взаємовідносин. Просте створення довірчих відносин з іншим доменом не дозволить користувачам із цього домену отримати доступ до всіх ресурсів у вашому домені. Тут знову потрібно буде назначити права, як і для користувачів вашого власного домену.

Порядок виконання роботи

1. Встановити роль Active Directory Domain Controller.
2. Зайти в Диспетчер сервера (Server Manager) і перейти у вузол Ролі (Roles) в лівій панелі консолі. Потім натиснути Додати ролі (Add Roles) у правій панелі.



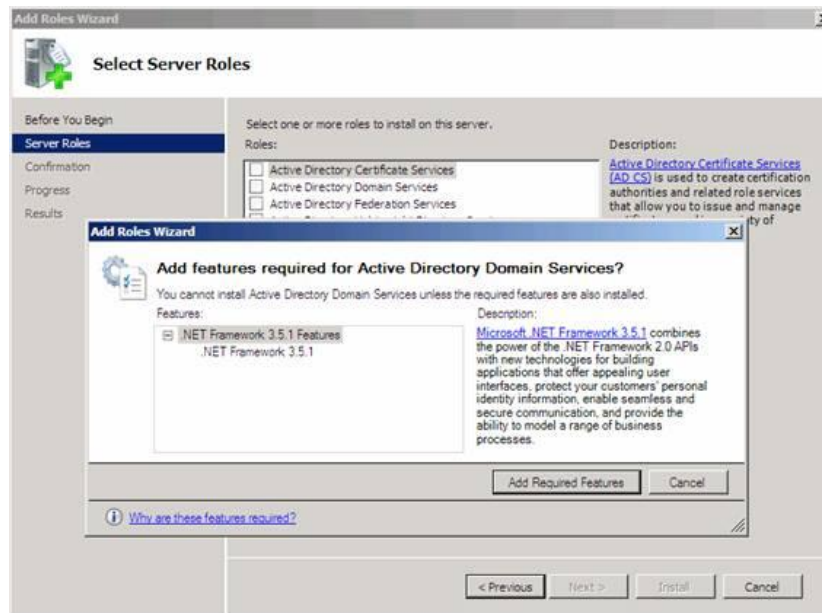
3. Відкриється сторінка Before You Begin, натиснути кнопку Далі.



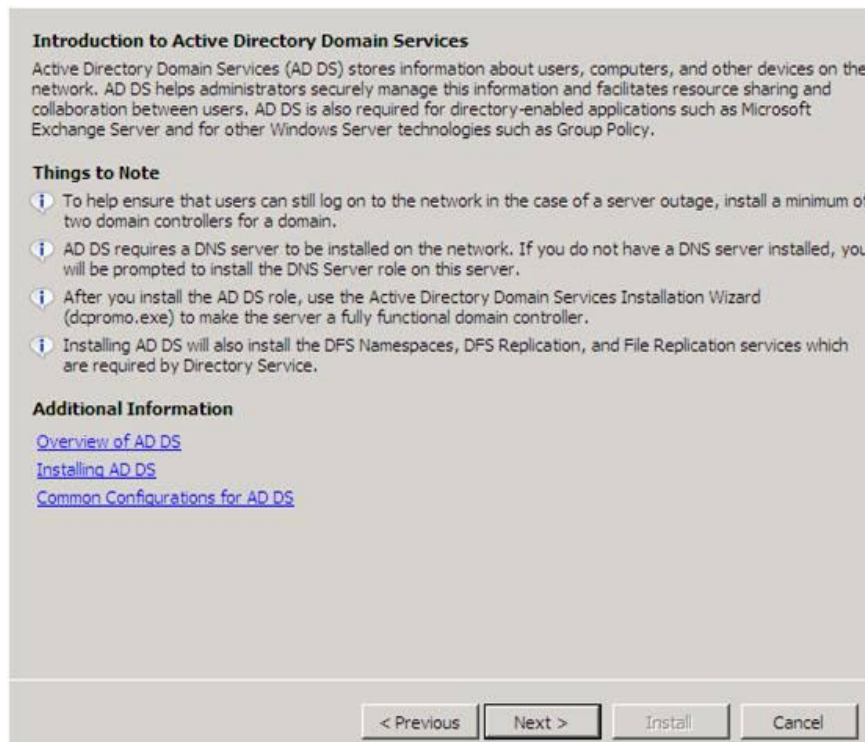
4. Спочатку встановити роль контролера домену (DC).

5. Вибрати Active Directory Domain Services, при цьому відзначити відповідну опцію, майстер відобразить ряд функцій, які будуть встановлені поряд з роллю Active Directory Server Role.

6. Натиснути кнопку Додати потрібні функції (Add Required Features), щоб встановити ці функції під час установки ролі Active Directory Server.

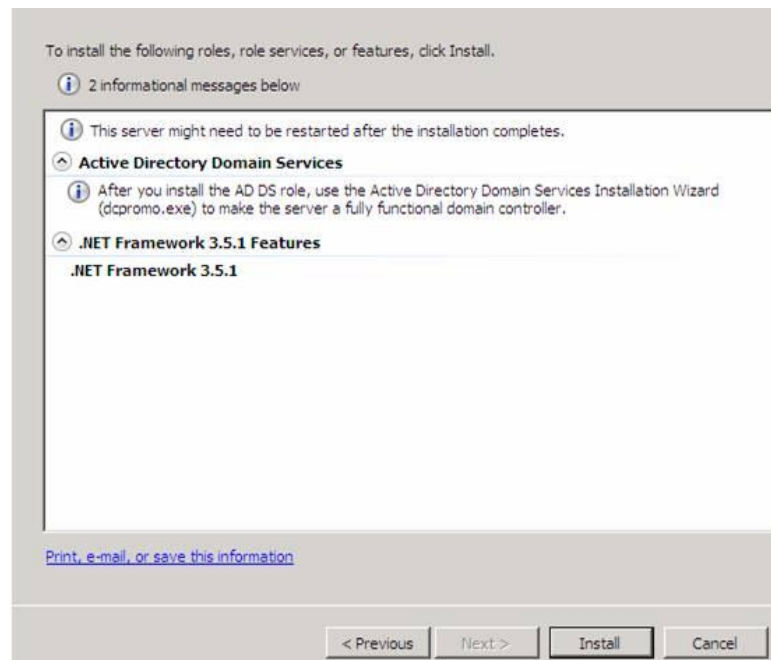


Після вибору ролі Active Directory DC Server, буде відображено інформацію про цю роль сервера.

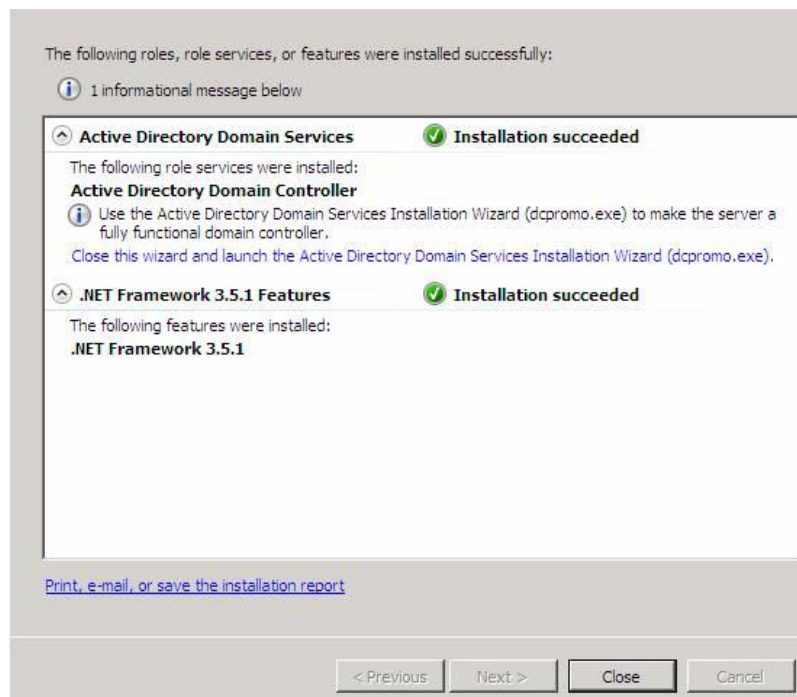


Під час установки ролі Active Directory Domain Services також встановлюються служби DFS простору імен, DFS реплікації і реплікації файлів. Всі ці служби використовуються службами Active Directory Domain Services, тому встановлюються автоматично.

7. Натиснути Встановити, для установки файлів, необхідних для запуску dcpromo.



8. Після успішної установки натиснути кнопку Закрити.



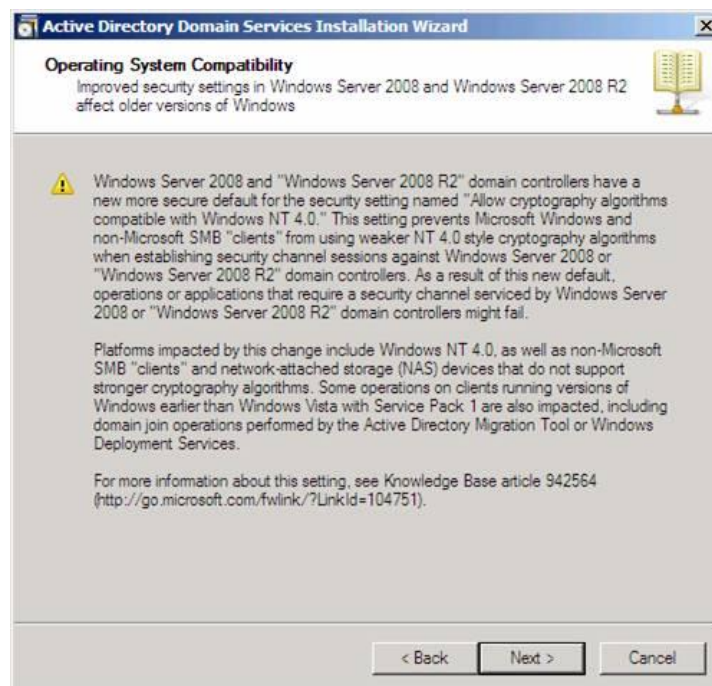
9. Перейти в меню Пуск і запустити dcpromo з команди Виконати і встановити роль DNS-сервера, що підтримує служби Active Directory.



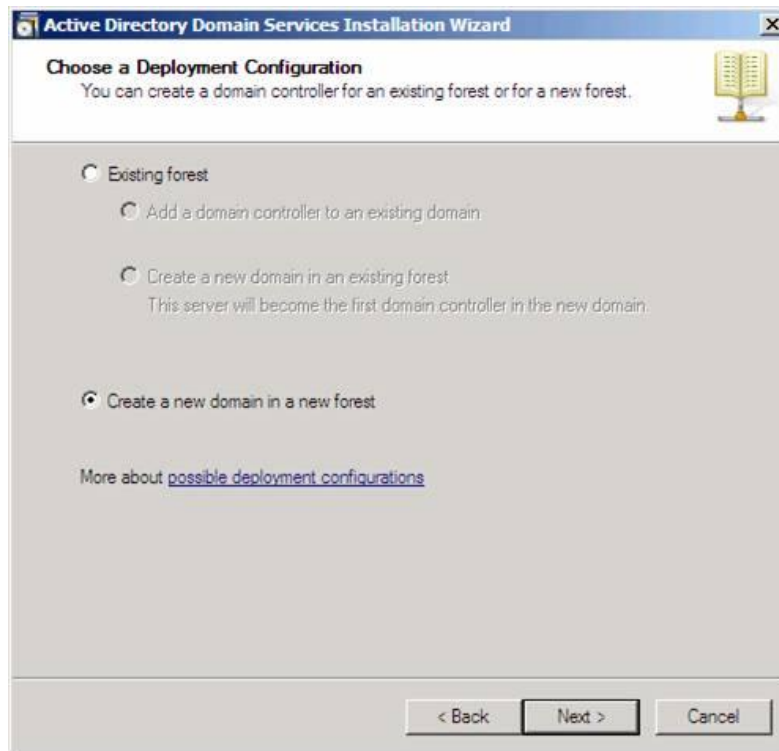
10. У результаті запуститься майстер Welcome to the Active Directory Domain Service Installation Wizard. Розширені опції у цьому сценарії непотрібні, тому просто натискаємо Далі.



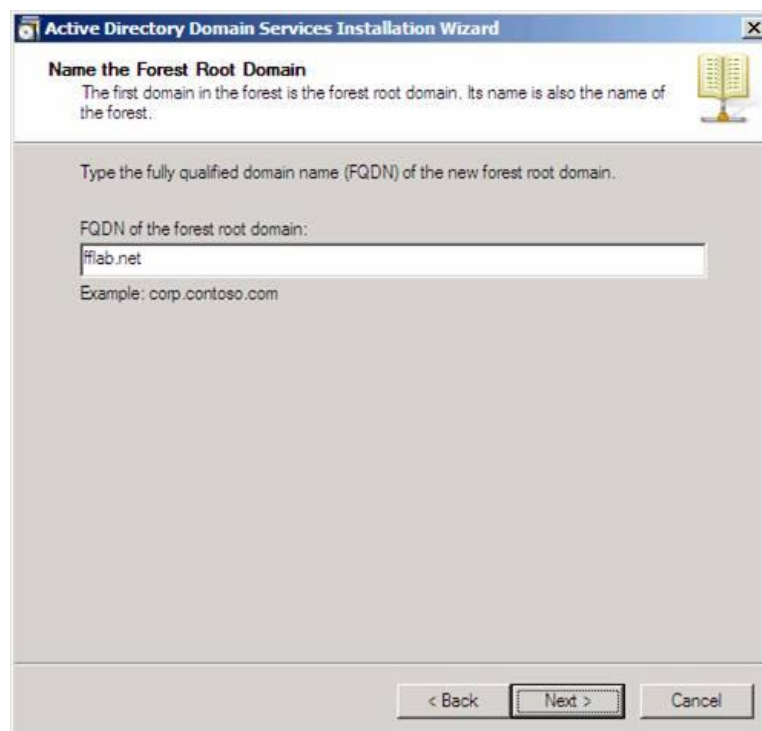
11. Майстер встановлення попереджає про те, що NT і non-Microsoft SMB клієнти будуть мати проблеми з деякими криптографічними алгоритмами, використовуваними в Windows Server 2008 R2. В даному випадку таких проблем немає, тому натискаємо Далі.



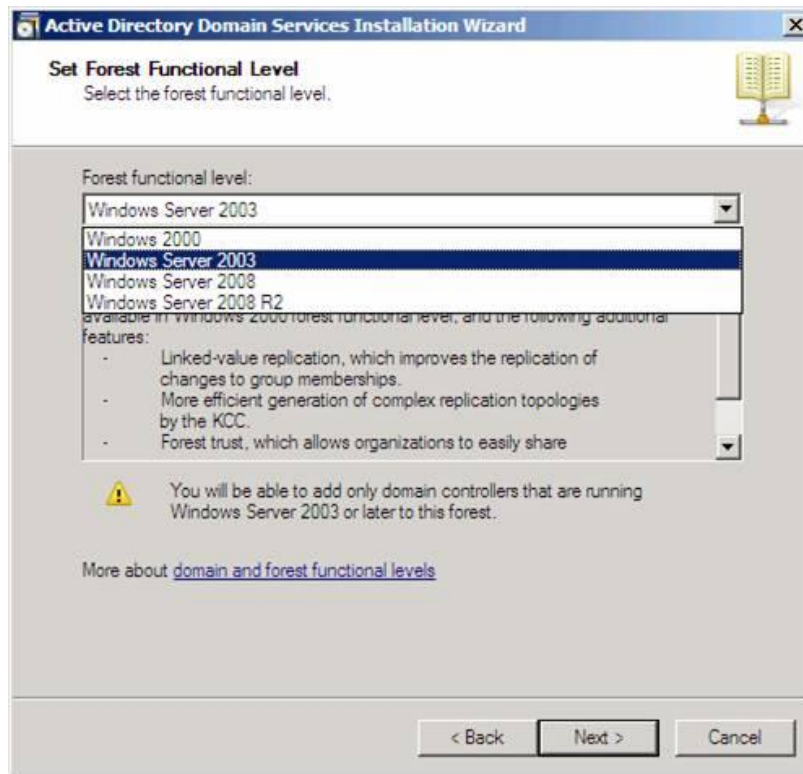
12. На сторінці Вибір конфігурації установки (Choose a Deployment Configuration) вибираю функцію Створення нового домену в лісі (Create a new domain in a new forest).



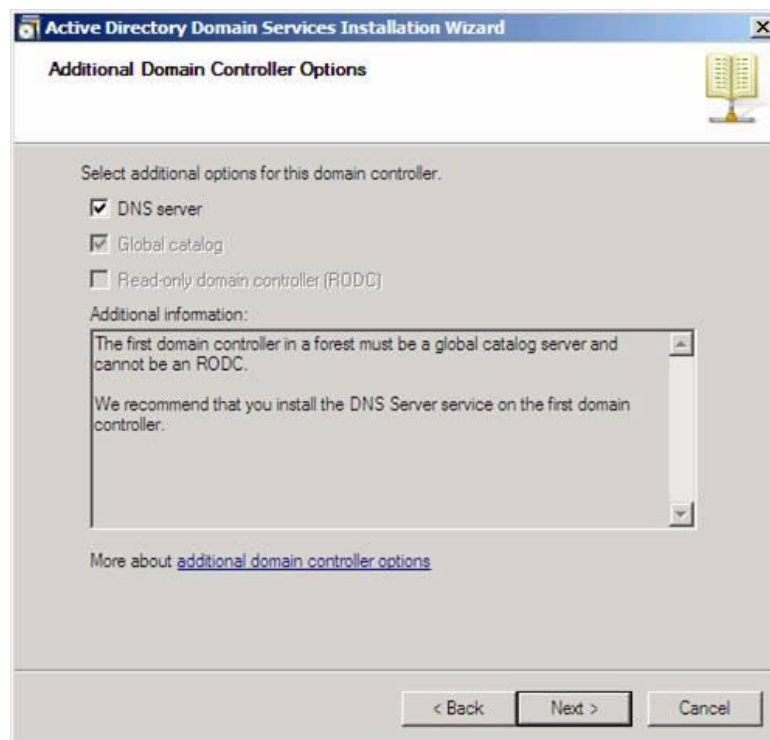
13. На сторінці Ім'я кореневого домену в лісі (Name the Forest Root Domain) ввести назву домену в текстове поле FQDN кореневого домену в лісі. Називаємо домен fflab.net і натискаємо Далі.



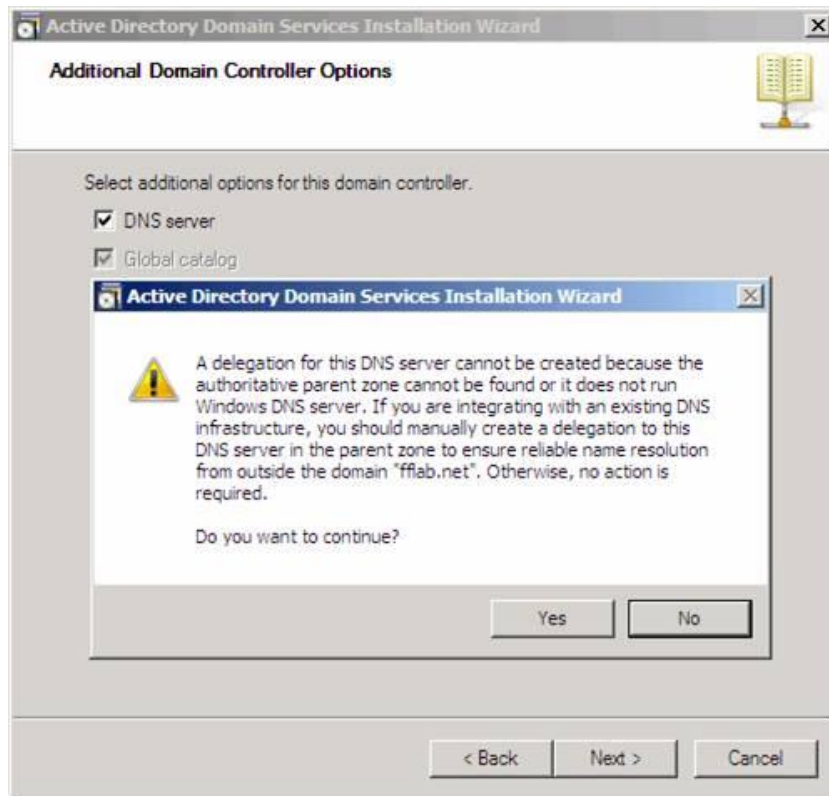
14. На сторінці Визначення функціонального рівня лісу (Set Forest Functional Level) вибираємо опцію Windows Server 2008 R2, яка дозволяє скористатися всіма новими можливостями, які є у Windows Server 2008 R2, натискаємо Далі.



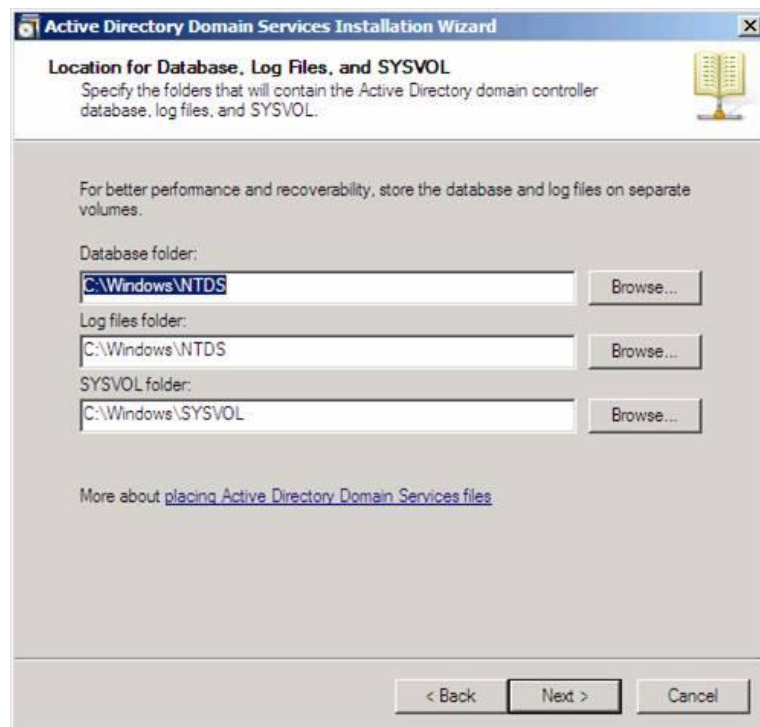
15. На сторінці Додаткові опції контролера домену (Additional Domain Controller Options) вибрати опцію DNS сервер і натиснути Далі.



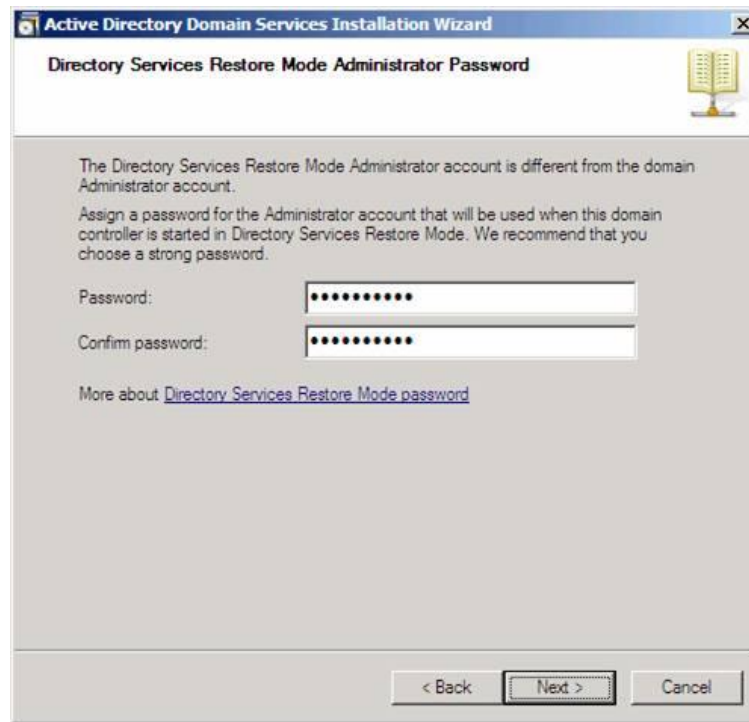
16. З'явиться діалогове вікно з інформацією, що неможливо створити делегування для цього сервера DNS. Причина в тому, що це перший DC в мережі. Натискаємо Так, щоб продовжити.



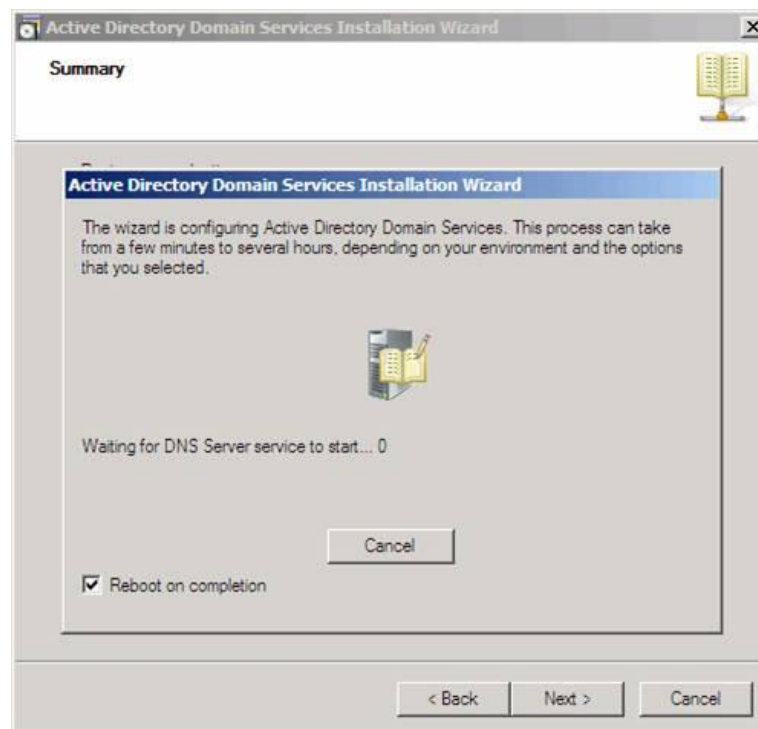
17. Залишаємо папки для Database, Log Files і SYSVOL за замовчуванням і натискаємо Далі.



18. На сторінці Directory Service Restore Mode Administrator Password потрібно ввести надійний пароль у текстові поля Пароль (Password) і Підтвердження (Confirm password).



19. Відзначаємо опцію Перезавантажити по закінченні (Reboot on completion), щоб машина автоматично перезавантажилась після установки DC.



Установка DC буде завершена після того, як буде виконано вхід в систему.

ЛАБОРАТОРНА РОБОТА №12

Тема: Налаштування служби NAT та проксі-сервера для виходу в Інтернет (ОС Windows 2003 Server, ОС Linux)

Мета: оволодіти основними навиками налаштування служби NAT та проксі сервера для виходу в Інтернет.

Теоретичні відомості

Для роботи в мережі Internet необхідно:

- фізично приєднати комп'ютер до одного з вузлів мережі Internet;
- одержати IP-адресу на постійній або тимчасовій основі;
- встановити і настроїти програмне забезпечення - програми-клієнти тих сервісів, послугами яких мається намір скористатися.

Організаційно доступ до мережі користувачі дістають через провайдерів. **Провайдер** - це організація (юридична особа), що надає послуги у приєднанні користувачів до мережі Internet. Як правило, провайдер має постійно ввімкнений досить продуктивний сервер, сполучений з іншими вузлами каналами з відповідною пропускною здатністю, і засоби для одночасного підключення кількох користувачів (багатоканальний телефон, багатопортова плата тощо).

Як правило, користувачі навчальних закладів, великих організацій, фірм, підприємств приєднуються до мережі Internet через свою локальну мережу. На один із комп'ютерів локальної мережі покладається вирішення завдань проху-сервера - управління локальною мережею й виконання функцій "посередника" між комп'ютерами користувачів та мережею Internet (проху - представник, довірена особа).

Всі технічні й організаційні питання взаємодії з провайдером вирішує адміністратор мережі. Для користувачів розробляється інструкція, в якій наводиться перелік дій, які треба виконати для приєднання до мережі Internet. Технічно для приєднання до комп'ютера провайдера потрібні ПК, відповідне програмне забезпечення й модем - пристрій, що перетворює цифрові сигнали від комп'ютера на сигнали для передачі по телефонних лініях і навпаки. Комп'ютер провайдера може виконувати функції хост-машини або звертатися до більш потужних хост-машин для доступу до глобальних ресурсів мережі Internet через високопродуктивний канал передачі даних - магістраль.

Хост-машина (від англ. host - господар) - це комп'ютер, що виконує мережеві функції, реалізуючи повний набір протоколів. Крім мережевих функцій, хост-машина може виконувати завдання користувача (програми, розрахунки, обчислення). Деякі хост-машини можуть виконувати функції шлюзів - апаратних і програмних засобів для передачі даних між несумісними мережами, наприклад, між мережею Internet та мережами FidoNet. Роль шлюзу між мережею Internet і локальними мережами відіграє проху-сервер.

Розглянемо три варіанти підключення локальної мережі до Інтернету:

- «пряме» IP-підключення;
- підключення через NAT;
- підключення через проксі-сервер.

Вибір конкретного способу підключення залежить від потреб користувача, мети підключення і, в деякій мірі, фінансових можливостей.

Отже, для початку нам потрібні:

- комп'ютер локальної мережі, підключений до Інтернету. У нього є доступ як до Інтернету, так і до локальної мережі;
- локальна мережа, в яку включений цей комп'ютер.

Наше завдання – дати комп'ютерам локальної мережі доступ до Інтернету через підключений до нього комп'ютер. Надалі цей комп'ютер ми будемо називати шлюзом чи маршрутизатором.

«Пряме» IP-підключення до Internet

Для того, щоб локальна мережа була повноцінно підключена до Інтернету, повинні виконуватися, як мінімум, три умови:

- кожна машина в локальній мережі повинна мати «реальну» інтернетівську IP-адресу;

- ці адреси повинні бути не будь-якими, а виділеними провайдером для локальної мережі (швидше за все, це буде підмережа класу С);
- на комп'ютері-шлюзі, підключеному до двох мереж – локальної мережі та мережі провайдера, повинна бути організована IP-маршрутизація, тобто передача пакетів із однієї мережі в іншу.

В цьому випадку наша локальна мережа стає ніби частиною Інтернету. Власне, це той спосіб підключення, яким підключені до Інтернету самі Інтернет-провайдери і хостинг-провайдери.

На відміну від звичайного підключення, розрахованого на один комп'ютер, при такому підключенні «під клієнта» виділяється не одна IP-адреса, а кілька, так звана «IP-підмережа». В прайсах провайдера, що виділяє підмережі, вказано вартість підмережі класу С (255 адрес). В такій підмережі перші три байти IP-адреси ідентифікують саму підмережу, а останнє число – комп'ютер в даній (нашій) підмережі.

В якості комп'ютера-шлюза провайдери рекомендують використовувати ПК під управлінням клону UNIX (Linux, FreeBSD), оскільки, по-перше, багато їх реалізацій безкоштовні і містять всі необхідні компоненти для організації IP-маршрутизатора і FireWall, а також багато інших необхідних чи корисних сервісів (які у випадку використання Windows, можна знайти тільки в NT чи навіть 2000), а, по-друге, ці ОС менш вимогливі до ресурсів ПК (у випадку відмови від графічних інтерфейсів).

При такому способі підключення можна організувати у своїй мережі сервіси, доступні з Інтернету – адже при даному підключенні не тільки Інтернет повністю доступний з нашої мережі, але і наша мережа – з Інтернету, оскільки є його частиною.

Однак така «прозорість» мережі різко знижує її захищеність – адже будь-які сервіси в локальній мережі, навіть призначені для «внутрішнього» користування, стануть доступними ззовні через Інтернет. Щоб це не мало місця, доступ в локальну мережу ззовні дещо обмежують. Звичайно це робиться установкою на шлюзі програми-firewall. Це своєрідний фільтр пакетів, що проходять із однієї мережі в іншу. Шляхом його налаштування можна заборонити вхід-вихід із локальної мережі пакетів, що відповідають певним критеріям – типу IP-пакету, IP-адресі призначення, TCP/UDP-порту і т. п.

Незважаючи на універсальність такого методу підключення локальної мережі до Інтернету, він (метод) має недоліки. Головний недолік полягає в високій вартості виділення IP-адрес і тим більше IP-підмереж, до того ж цю плату треба вносити періодично.

Якщо нема необхідності в установці Інтернет-серверів, а підключення локальної мережі потрібне із звичайними «клієнтськими» намірами, то використовуються описані далі способи, які не потребують таких великих затрат і, що найголовніше, дозволяють підключити локальну мережу через звичайне підключення із однією зовнішньою IP-адресою.

Підключення через NAT

Технологія Network Address Translation (NAT) – трансляція мережевих адрес – дозволяє кільком машинам локальної мережі мати доступ до Інтернету через одне підключення і одну реальну зовнішню IP-адресу.

Розглянемо теоретично, як це все працює. Для того, щоб комп'ютери локальної мережі могли встановлювати з'єднання з серверами мережі Інтернет, потрібно, щоб:

- IP-пакети, адресовані серверу в Інтернеті, могли його досягнути;
- IP-пакети, що йдуть від сервера Інтернету на машину в локальній мережі, також могли її досягнути.

Із першою умовою не виникає проблем, а щодо іншої є певні труднощі, адже комп'ютери локальної мережі не мають своєї «реальної» інтернетівської IP-адреси. Як вони можуть отримувати IP-пакети з Інтернету?

Працює це наступним чином: на комп'ютері-шлюзі стоїть програма NAT-сервера. Комп'ютер-шлюз прописаний на машинах локальної мережі як «основний шлюз», і на нього поступають усі пакети, що йдуть в Інтернет (не адресовані самій локальній мережі). Перед передачею цих IP-пакетів в Інтернет NAT-сервер замінює в них IP-адресу відправника на свою, одночасно запам'ятовуючи в себе, з якої машини локальної мережі прийшов цей IP-пакет. Коли приходить пакет у відповідь (на адресу шлюзу, звичайно), NAT визначає, на яку машину локальної

мережі його потрібно направити. Потім в отриманому пакеті міняється адреса одержувача на адресу потрібної машини, і пакет доставляється цій машині через локальну мережу.

Як видно, робота NAT-сервера прозора для машин локальної мережі (як і робота звичайного IP-маршрутизатора). Єдиним принциповим обмеженням цього методу підключення локальної мережі до Інтернет є неможливість встановити Вхідне TCP-з'єднання з Інтернету на машину локальної мережі. Однак для «клієнтських» мереж цей недолік перетворюється в перевагу, що різко підвищує (в порівнянні з першим методом підключення) їх захищеність і безпеку. Адміністратори деяких провайдерів навіть вживають слова NAT і Firewall як синоніми.

Підключення через проксі-сервер

Це найпростіший тип підключення. При цьому ніякої маршрутизації IP-пакетів між локальною мережею та мережею Інтернет не відбувається. Машини локальної мережі працюють з Інтернетом через програму-посередник, так званий проксі-сервер, встановлений на комп'ютері-шлюзі.

Головною особливістю цього методу є його «непрозорість». Якщо, скажімо, у випадку NAT програма-клієнт просто звертається до Інтернет-сервера, не «задумуючись», в якій мережі і через яку маршрутизацію вона працює, то у випадку роботи через проксі-сервер програма повинна явно звертатись до проксі-сервера. Крім того, клієнтська програма повинна вміти працювати через проксі-сервер. Однак проблем з цим не виникає – всі сучасні і не дуже браузері вміють працювати через проксі-сервери.

Іншою особливістю є те, що проксі-сервер працює на більш високому рівні, ніж, скажімо, NAT. Тут уже обмін з Інтернетом не йде на рівні маршрутизації пакетів, а на рівні роботи по конкретних прикладних протоколах (HTTP, FTP, POP3...). Відповідно для кожного протоколу, по яких повинні «вміти» працювати машини локальної мережі, на шлюзі має працювати свій проксі-сервер.

Деякі HTTP проксі-сервери вміють також працювати з FTP-серверами. При цьому клієнт користується звичайним браузером і сам працює з таким проксі, як і звичайно, по протоколу HTTP. Однак такі проксі-сервери дозволяють тільки скачувати файли з FTP-серверів і не дозволяють їх закачувати на сам сервер. Тому, якщо робота по FTP потрібна, наприклад, для оновлення веб-сайту, то доведеться використовувати спеціальний FTP-проксі і працювати через нього за допомогою FTP-клієнта (FTP Explorer, CuteFTP і т.п.). Ця «протокольна залежність» є основним недоліком цього методу підключення як самостійного.

Майже кожен Інтернет-провайдер має один чи кілька проксі-серверів, через які рекомендує працювати своїм клієнтам. Незважаючи на те, що це зовсім необов'язково (як правило, клієнт провайдера може звертатися до Інтернету напряму), це дає вигоду у продуктивності, а при почасовій оплаті, відповідно, економить час он-лайн. Це відбувається тому, що проксі-сервери здатні кешувати (запам'ятовувати) запитовані користувачем документи, і при наступних до них звертань видавати копію з кешу, що є швидшим, аніж повторний запит з Інтернет-сервера. Крім того, проксі-сервери можуть бути налаштовані так, що будуть блокувати завантаження баннерів найбільш поширених баннерних служб, тим самим також прискорюючи завантаження веб-сторінок.

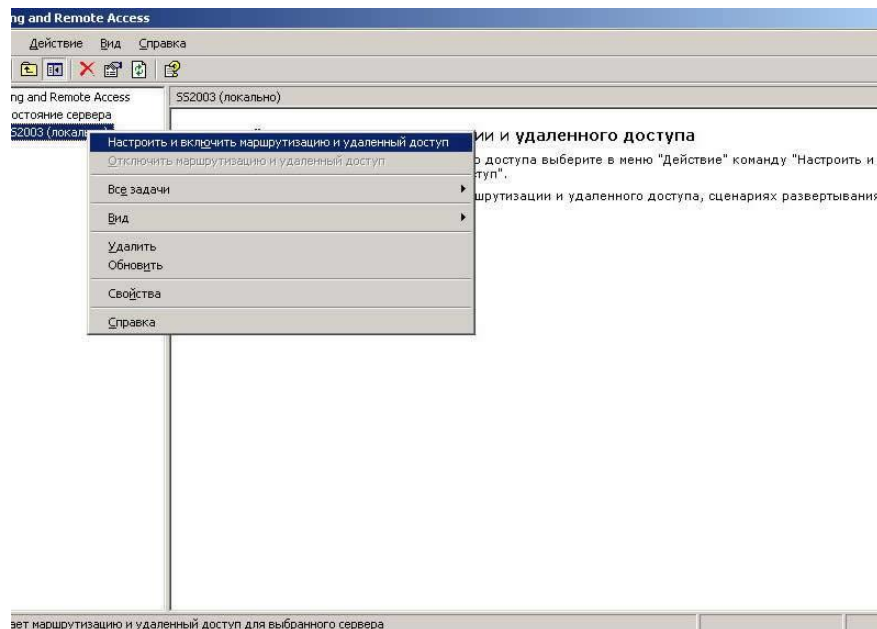
При установці HTTP проксі-сервера в локальній мережі і роботі через нього за рахунок кешування економиться не лише час, але і трафік – тому що кешування відбувається в самій локальній мережі, «до» каналу з провайдером, в якому обчислюється трафік (при оплаті за об'єм перекачаної інформації).

Вибір проксі-серверів для локальної мережі сьогодні досить широкий. Є програмні продукти, що об'єднують в собі кілька проксі-серверів для роботи по різних протоколах. До них відносяться, наприклад, EServ і WinGate.

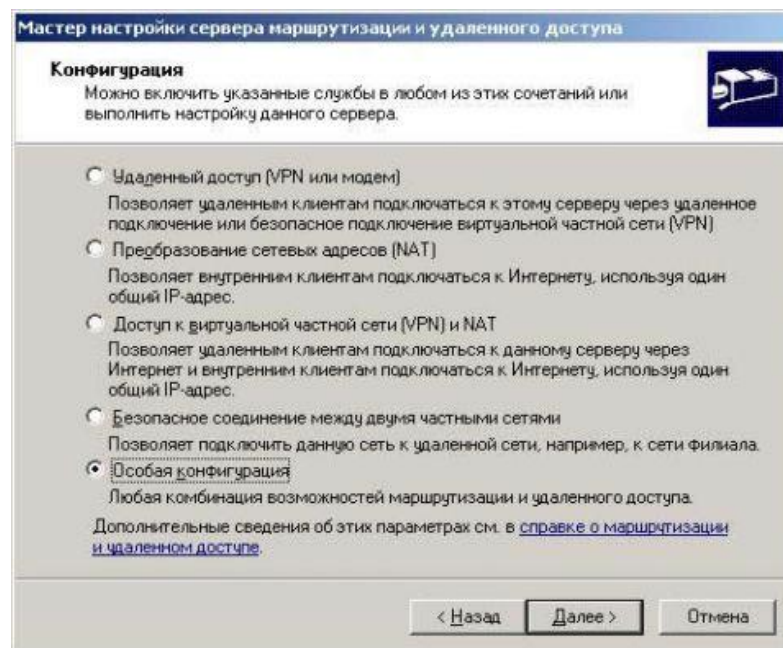
Порядок виконання роботи

1. Пуск – Програми – Адміністрування – Маршрутизація та віддалений доступ (Routing and Remote Access).

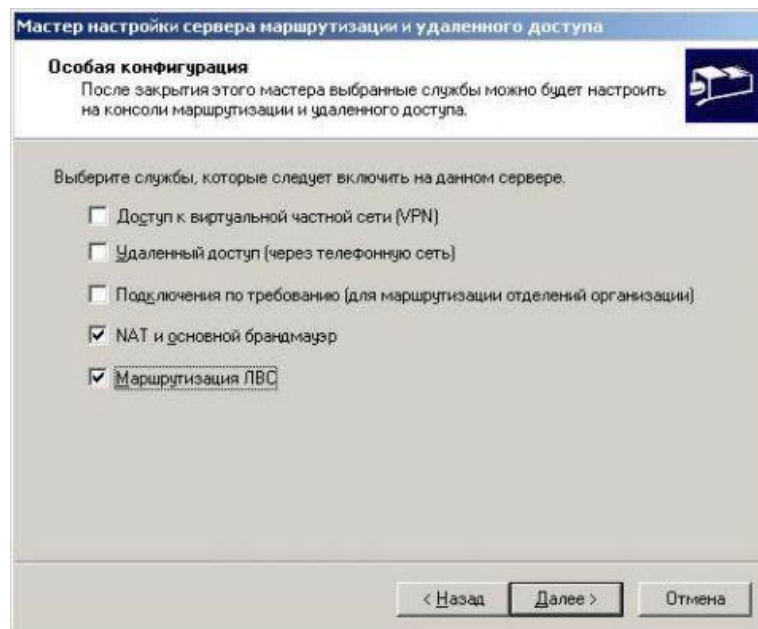
2. У контекстному меню вибрати пункт Налаштувати і включити маршрутизацію та віддалений доступ (Configure and Enable Routing and Remote Access)



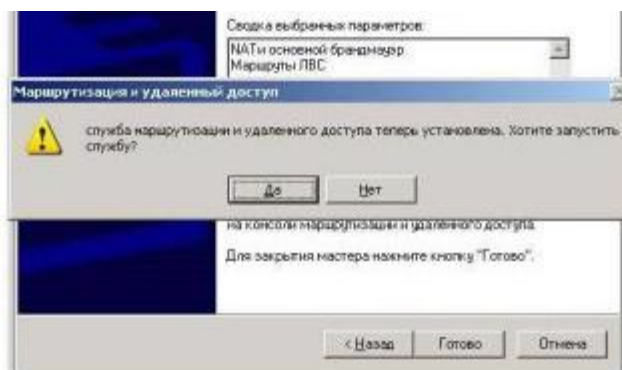
3. В Майстрі настроювання сервера маршрутизації та віддаленого доступу можна вибрати різні конфігурації для Routing and Remote Access (RRAS). RRAS може бути настроєний як захоче адміністратор, але Microsoft включив кілька шаблонів, щоб зробити процес установки для основних типів установки простішим. Вибрати Особлива конфігурація (Custom configuration).



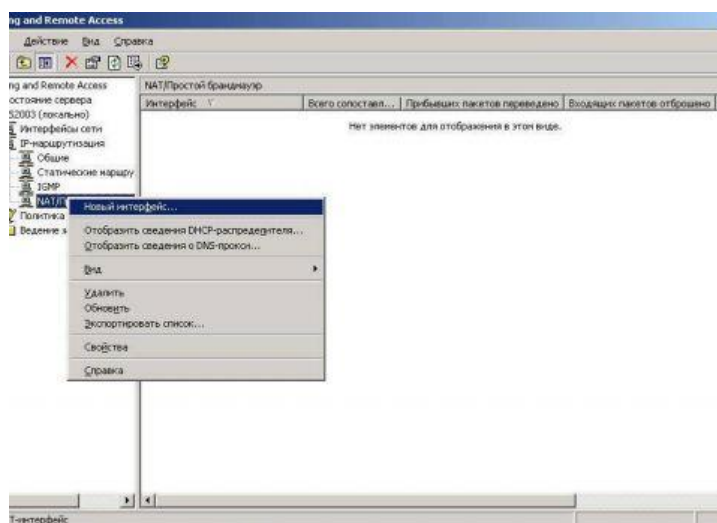
4. Вибрати NAT і основний брандмауер і Маршрутизація ЛВС (NAT and basic firewall і LAN routing).



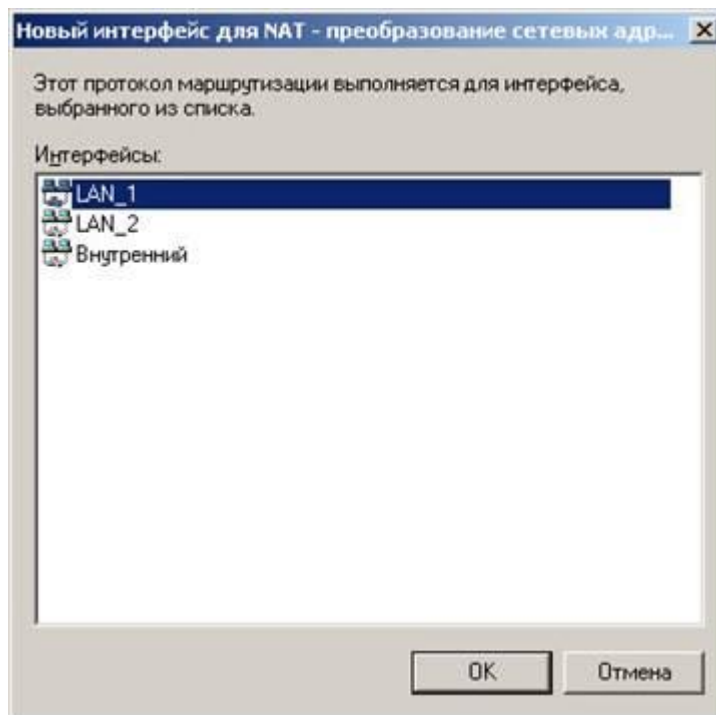
5. Вкінці натиснути Готово (Finish) на запитання Хотите запустить службу? (Do you want to start the service?), натиснути Так (Yes).



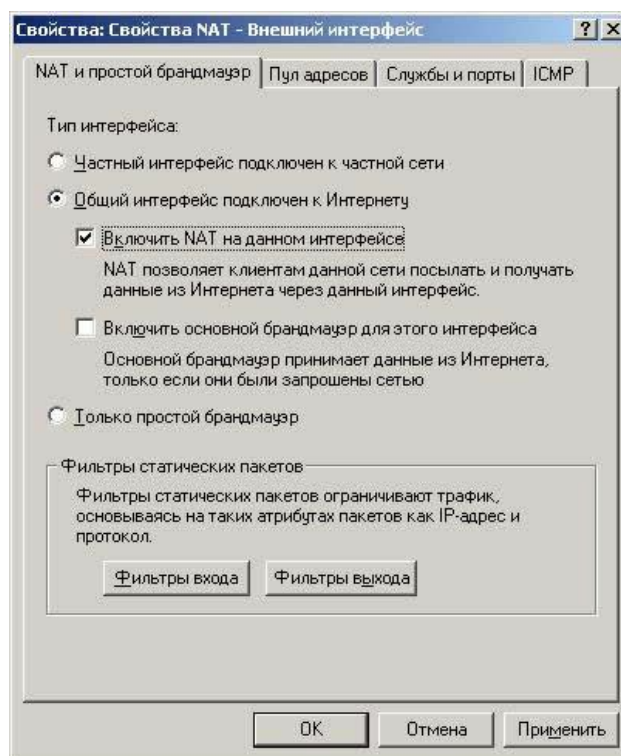
6. Перейти до пункту меню NAT – Простий брандмауер (NAT / Basic Firewall). Для роботи NAT необхідно додати публічний (підключений до Інтернету) і приватний (локальний) інтерфейс. У контекстному меню вибрати Новий інтерфейс (New Interface)



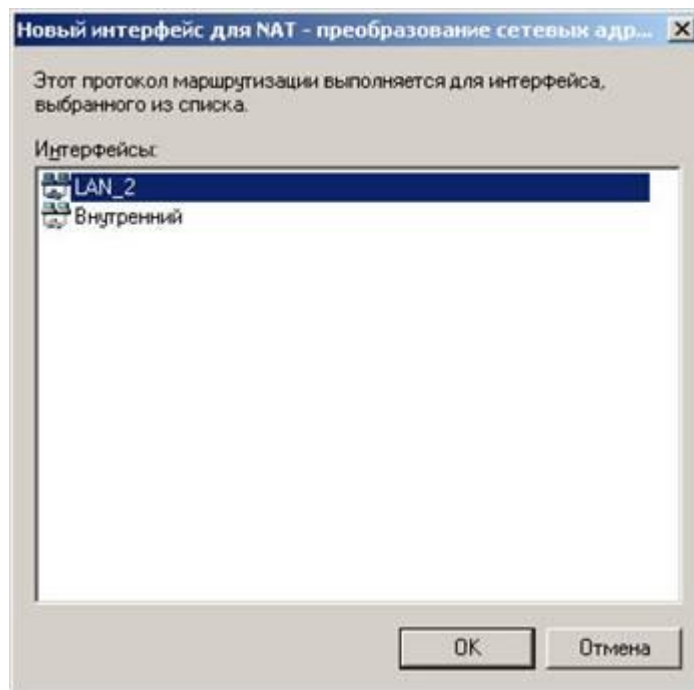
7. У списку інтерфейсів вибрати інтерфейс, підключений до Інтернету. В даному випадку це LAN_1.



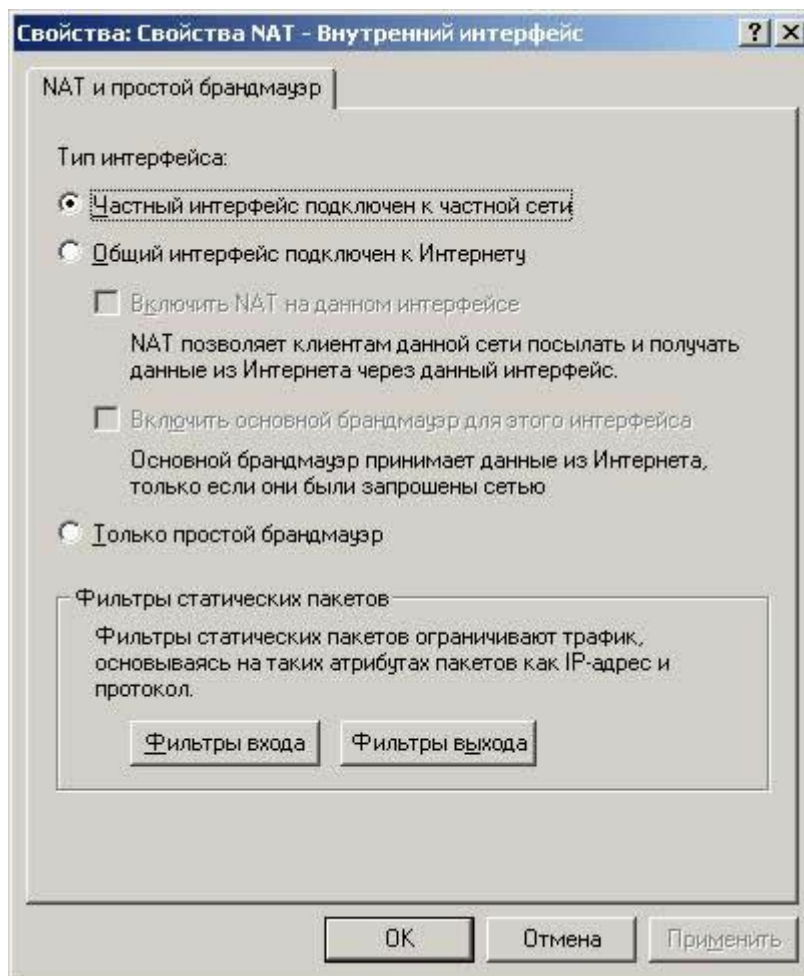
8. У наступному вікні вибрати пункт Загальний інтерфейс підключення до Інтернету (Public interface connected to the Internet) і поставити галочку Включити NAT на даному інтерфейсі (Enable NAT on this interface).



9. Знову перейти до пункту меню NAT – Простий брандмауер (NAT / Basic Firewall) і в контекстному меню вибрати Новий інтерфейс (New Interface) і вибрати інтерфейс локальної або публічної мережі.

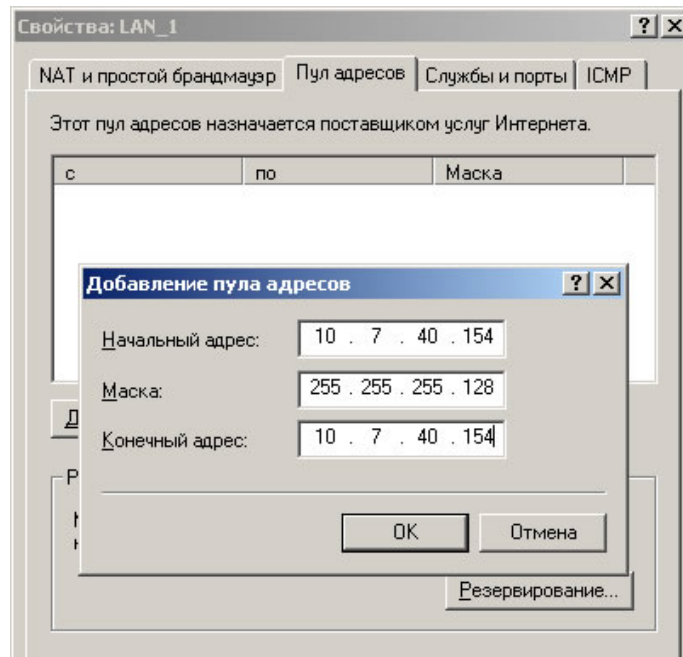


10. Наступні налаштування залишаємо без змін (за замовчуванням встановлено Приватний інтерфейс підключений до приватної мережі (Private interface connected to private network)). Натиснути ОК.

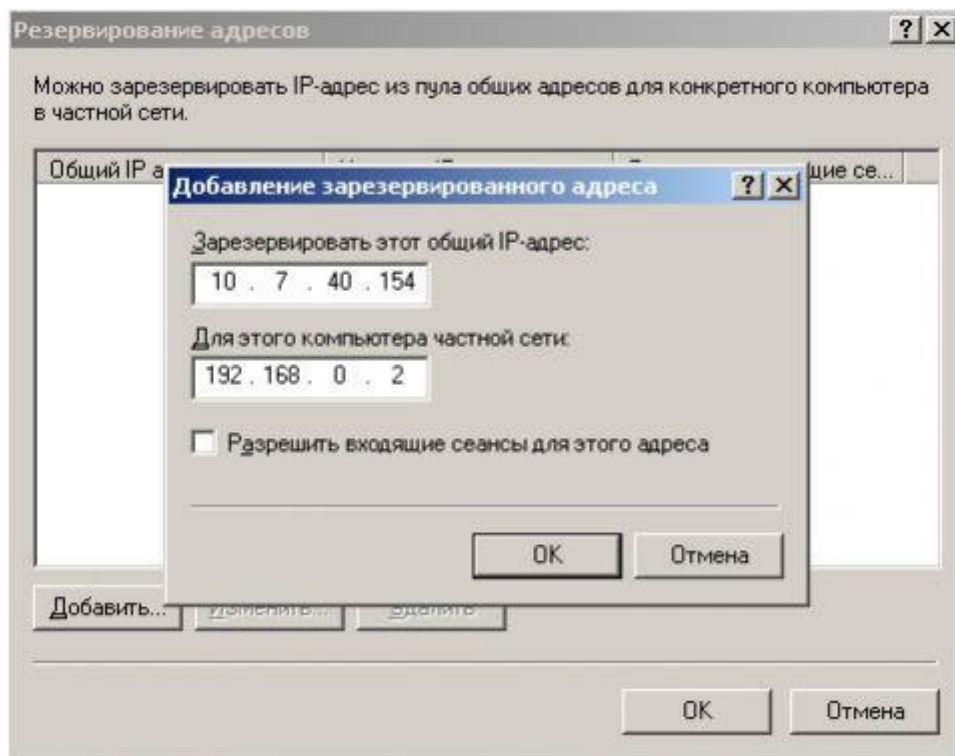


Налаштування NAT

1. Налаштувати IP-адреси і маску, для цього перейти до пункту меню NAT – Простий брандмауер (NAT / Basic Firewall), вибрати контекстне меню LAN_1 і перейти у Властивості (Prefences), вибрати Address Pool. Далі потрібно додати зовнішню IP-адресу і маску.



2. Зарезервувати IP-адреси, у вкладці (Address Pool) натиснути на кнопку Зарезервувати.



192.168.0.2 – IP-адреса користувача, який буде виходити в мережу через даний сервер;

10.7.40.154 – зовнішня IP-адреса сервера.

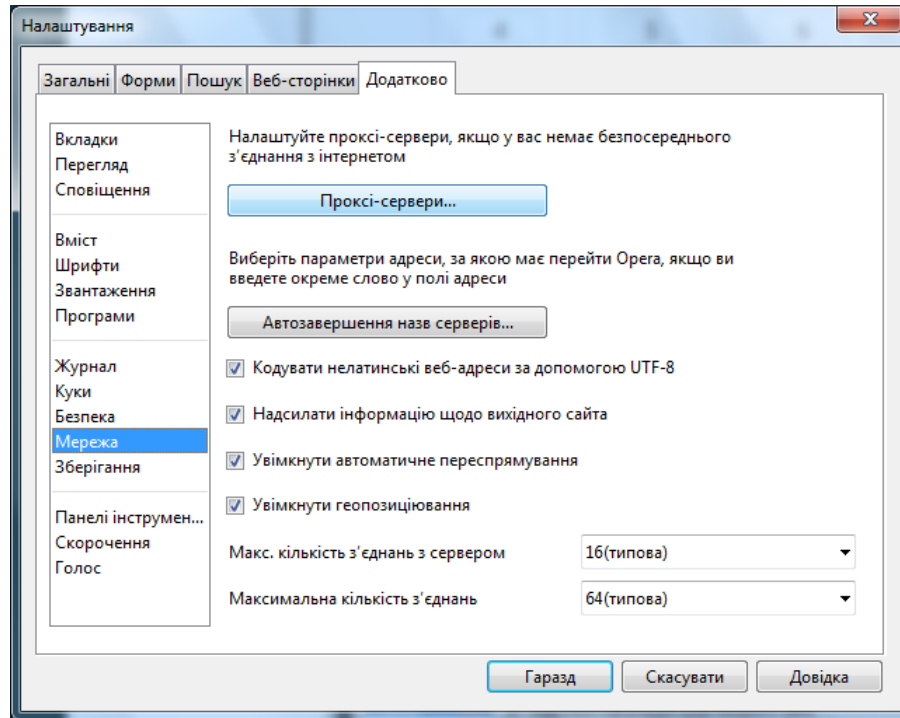
Є різні шляхи налаштування, можна кожній машині окремо резервувати адреси. В резервації можна вказувати не один діапазон адрес або не вказувати зовсім, тоді будь-яка IP в локальній мережі зможе бути в Інтернеті через сервер.

Налаштування клієнтської машини

1. Зайти у Властивості локальної мережевої карти, далі Властивості TCP/IP.
2. Прописати IP клієнта, маску до основного шлюзу (Default gateway), прописую IP-адреси сервера.
3. У полях DNS прописати IP-адреси DNS провайдера або IP-адреси встановленого локального DNS-сервера.

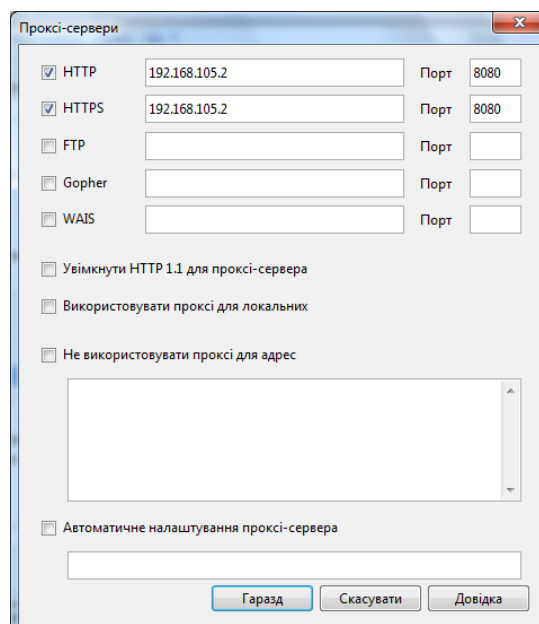
Налаштування проксі-серверу в браузері Opera

1. Відкрити діалог Налаштування в меню Інструменти-Налаштування або натиснути одночасно комбінацію клавіш Ctrl+F12.
2. Вибрати закладку Додатково, потім підрозділ Мережа і натиснути на кнопку Проксі-сервери.



4. Відмітити галочкою пункти HTTP та HTTPS.
5. В текстових полях ввести відповідну адресу проксі-серверу.
6. В текстове поле Порт: ввести номер порта даного проксі-сервера.
7. Переконатись в правильності вводу, закрити діалог налаштувань, натиснувши кнопку

Гаразд.



ЛАБОРАТОРНА РОБОТА №13

Тема: Знайомство із статичною маршрутизацією та з протоколами динамічної маршрутизації (ОС Windows 2003 Server, ОС Linux)

Мета: ознайомитись із статичною та динамічною маршрутизацією.

Теоретичні відомості

Задача маршрутизації вирішується на основі аналізу таблиць маршрутизації, розміщених в усіх маршрутизаторах і кінцевих вузлах мережі. Основна робота із створення таблиць маршрутизації виконується автоматично, але і можливість вручну скорегувати або доповнити таблицю теж, як правило, передбачається. Для автоматичної побудови таблиць маршрутизації маршрутизатори обмінюються інформацією про топологію складної мережі відповідно до спеціального службового протоколу. Протоколи цього типу **називаються протоколами маршрутизації** (чи маршрутизуючими протоколами).

Протоколи маршрутизації (наприклад, RIP, OSPF, NLSP) слід відрізнити від власне мережевих протоколів (наприклад, IP, IPX). І ті і інші виконують функції мережевого рівня моделі OSI. Але тоді як перші збирають і передають по мережі суто службову інформацію, другі призначені для передачі даних користувача.

Протоколи маршрутизації використовують мережеві протоколи як транспортний засіб. При обміні маршрутною інформацією пакети протоколу маршрутизації розміщуються в поле даних пакетів мережевого рівня або навіть транспортного рівня. У тому, що маршрутизатори для прийняття рішення про просування пакету звертаються до адресних таблиць, можна побачити їх деяку схожість з мостами і комутаторами. Проте природа використовуваних ними адресних таблиць дуже відрізняється. Замість MAC-адрес в таблицях маршрутизації вказуються номери мереж, які з'єднуються в інтермережу.

Ще однією відмінністю таблиць маршрутизації від адресних таблиць мостів є спосіб їх створення. Тоді як міст будує таблицю, пасивно спостерігаючи за посланими кінцевими вузлами мережі інформаційними кадрами, що проходять через нього, маршрутизатори за власною ініціативою обмінюються спеціальними службовими пакетами, повідомляючи сусідів про відомі їм мережі в інтермережі, маршрутизатори і про зв'язки цих мереж з маршрутизаторами. Зазвичай враховується не лише топологія зв'язків, але і їх пропускна здатність і стан. При зміні конфігурації мережі деякі записи в таблиці стають недійсними. Від того, наскільки швидко протокол маршрутизації приводить у відповідність вміст таблиці до реального стану мережі, залежить якість роботи усєї мережі.

При виборі раціонального маршруту визначається тільки наступний (найближчий) маршрутизатор, а не уся послідовність маршрутизаторів від початкового до кінцевого вузла. Відповідно до цього підходу маршрутизація виконується за розподіленою схемою – кожен маршрутизатор відповідальний за вибір тільки одного кроку маршруту. Такі алгоритми маршрутизації називаються однокроковими. Існує і прямо протилежний, багатокроковий підхід – маршрутизація від джерела (Source Routing). Відповідно до нього початковий вузол (вузол-джерело) задає в пакеті, що відправляється в мережу, повний маршрут його проходження через усі проміжні маршрутизатори. При використанні багатокрокової маршрутизації немає необхідності будувати і аналізувати таблиці маршрутизації. Це прискорює проходження пакету по мережі, розвантажує маршрутизатори, але при цьому велике навантаження лягає на кінцеві вузли. Ця схема в обчислювальних мережах застосовується сьогодні набагато рідше, ніж схема розподіленої однокрокової маршрутизації.

Однокрокові алгоритми залежно від способу формування таблиць маршрутизації діляться на три класи:

- алгоритми фіксованої (чи статичної) маршрутизації;
- алгоритми простої маршрутизації;
- алгоритми адаптивної (чи динамічної) маршрутизації.

У алгоритмах **фіксованої маршрутизації** всі записи в таблиці маршрутизації є статичними. Адміністратор мережі сам вирішує, на які маршрутизатори потрібно передавати пакети з тими або іншими адресами, і вручну вносить відповідні записи в таблицю маршрутизації. Таблиця, як

правило, створюється в процесі завантаження, надалі вона використовується без змін до тих пір, поки її вміст не буде відредагований вручну.

Розрізняють **одномаршрутні таблиці**, в яких для кожного адресата заданий один шлях, і **багатомаршрутні таблиці**, що визначають декілька альтернативних шляхів для кожного адресата. У багатомаршрутних таблицях повинно бути задано правило вибору одного з маршрутів. Найчастіше один шлях є основним, а інші - резервними. Алгоритм фіксованої маршрутизації прийнятний тільки в невеликих мережах з простою топологією. Однак цей алгоритм може бути ефективно використаний і для роботи на магістралях великих мереж, оскільки сама магістраль може мати просту структуру.

У **алгоритмах простої маршрутизації** таблиця маршрутизації або взагалі не використовується, або будується без участі протоколів маршрутизації.

Виділяють три типи простої маршрутизації :

- випадкова маршрутизація, коли пакет, що надійшов, відсилається в випадковому напрямку, окрім початкового;
- лавинна маршрутизація, коли пакет ширококомовно посилається по усіх можливих напрямках, окрім початкового;
- маршрутизація за попереднім досвідом, коли вибір маршруту здійснюється за таблицею, але таблиця будується за принципом моста шляхом аналізу адресних полів пакетів, що з'являються на вхідних портах.

Найпоширенішими є **алгоритми адаптивної (чи динамічної) маршрутизації**. Ці алгоритми забезпечують автоматичне оновлення таблиць маршрутизації після зміни конфігурації мережі. Протоколи, побудовані на основі адаптивних алгоритмів, дозволяють усім маршрутизаторам збирати інформацію про топологію зв'язків в мережі, оперативно відпрацьовуючи всі зміни конфігурації зв'язків. У таблицях маршрутизації при адаптивній маршрутизації зазвичай є інформація про інтервал часу, протягом якого даний маршрут залишатиметься дійсним. Цей час називають часом життя маршруту (Time To Live, TTL). Адаптивні алгоритми зазвичай мають розподілений характер, який виражається в тому, що в мережі відсутні будь-які виділені маршрутизатори, які б збирали і узагальнювали топологічну інформацію: ця робота розподілена між усіма маршрутизаторами.

Адаптивні алгоритми маршрутизації повинні **відповідати кільком важливим вимогам**. По-перше, вони повинні забезпечувати хоча б раціональність маршруту. По-друге, алгоритми мають бути досить простими, зокрема, вони не повинні вимагати великого об'єму обчислень і породжувати інтенсивний службовий трафік. І, нарешті, алгоритми маршрутизації повинні мати властивість збіжності, тобто завжди призводити до однозначного результату за прийнятний час.

Адаптивні протоколи обміну маршрутною інформацією, що застосовуються на даний час в обчислювальних мережах, у свою чергу діляться на дві групи:

- дистанційно-векторні алгоритми (Distance Vector Algorithms, DVA);
- алгоритми стану зв'язків (Link State Algorithms; LSA).

У **алгоритмах дистанційно-векторного типу** кожен маршрутизатор періодично і ширококомовно розсилає по мережі вектор, компонентами якого є відстані від цього маршрутизатора до усіх відомих йому мереж (кількість хопів). При отриманні вектору від сусіда маршрутизатор нарощує відстані до вказаних у векторі мереж на відстань до даного сусіда. Отримавши вектор від сусіднього маршрутизатора, кожен маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він дізнався безпосередньо або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектору по мережі. Врешті-решт, кожен маршрутизатор дізнається інформацію про усі наявні в інтермережі мережі і про відстань до них через сусідні маршрутизатори.

Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах, оскільки вони «засмічують» лінії зв'язку інтенсивним ширококомовним трафіком, до того ж зміни конфігурації можуть відпрацьовуватися за цим алгоритмом не завжди коректно, тому що маршрутизатори не мають точного уявлення про топологію зв'язків в мережі. Його робота відповідно до дистанційно-векторного протоколу нагадує роботу моста, оскільки точної топологічної картини мережі такий маршрутизатор не має. Найбільш поширеним протоколом, що базується на дистанційно-векторному алгоритмі, є **протокол RIP**, який поширений в двох версіях: RIP IP, що працює з протоколом IP, і RIP IPX, що працює з протоколом IPX.

Алгоритми стану зв'язків забезпечують кожен маршрутизатор інформацією, достатньою для побудови точного графа зв'язків мережі. "Широкомовна" розсилка використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто. Вершинами графа є як маршрутизатори, так і об'єднані ними мережі. Щоб зрозуміти, в якому стані знаходяться лінії зв'язку, підключені до його портів, маршрутизатор періодично обмінюється короткими пакетами "HELLO" зі своїми найближчими сусідами. Цей службовий трафік також «засмічує» мережу, але не такою мірою як RIP-пакети, оскільки пакети "HELLO" мають набагато менший об'єм. Протоколами, що базуються на алгоритмі стану зв'язків, є протоколи IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP і нещодавно реалізований протокол NLSP стека Novell.

Протоколи маршрутизації також поділяються на два види залежно від сфери застосування:

- протоколи міждоменної маршрутизації;
- протоколи внутрішньодоменої маршрутизації.

Порядок виконання роботи

Налаштування статичної маршрутизації виконується командою `route`. Перш ніж налаштувати маршрути, варто переглянути таблицю маршрутизації ядра за допомогою команди `netstat -n -r`.

```
rigon@ubuntu-comp:~$ netstat -n -r
```

1	2	3	4	5	6	7	8	9
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface	
0.0.0.0	192.168.254.0	0.0.0.0	U			255.255.255.0	eth1	0
0.0.0.0	192.168.254.0	0.0.0.0	U			255.255.255.0	eth0	0
0.0.0.0	169.254.0.0	0.0.0.0	U			255.255.0.0	eth1	0
0.0.0.0	0.0.0.0	192.168.254.1	UG			0.0.0.0	eth0	0
0.0.0.0	0.0.0.0	192.168.254.1	UG			0.0.0.0	eth1	0

Якщо таблиця порожня, то покаже тільки заголовки стовпців. Тоді треба використовувати `route`. За допомогою команди `route` можна додати або видалити один (за один раз) статичний маршрут.

```
1 | route -f операция -тип адресат шлюз интерфейс
```

Тут аргумент операції може приймати одне з двох значень: `add` (маршрут додається) або `delete` (маршрут віддаляється). Аргумент адресат може бути IP-адресою машини, IP-адресою мережі або ключовим словом `default`. Аргумент шлюз – це IP-адреса комп'ютера, на який слід пересилати пакет (цей комп'ютер повинен мати прямий зв'язок з вашим комп'ютером).

Команда

```
1 | route -f
```

видаляє з таблиці дані про всі шлюзи. Необов'язковий аргумент `тип` приймає значення `net` або `host`. У першому випадку в полі адресата вказується адреса мережі, а в другому – адреса конкретного комп'ютера (хоста).

Як правило, буває необхідно налаштувати маршрутизацію за згаданими вище трьома інтерфейсами:

- Локальний інтерфейс (lo);

- Інтерфейс для плати Ethernet (eth0);
- Інтерфейс для послідовного порту (PPP або SLIP).

Локальний інтерфейс підтримує мережу з IP-номером 127.0.0.1. Тому для маршрутизації пакетів з адресою 127 ... використовується команда:

```
1 | route add -net 127.0.0.1 lo
```

Якщо у вас для зв'язку з локальною мережею використовується одна плата Ethernet, і всі машини знаходяться у цій мережі (мережева маска 255.255.255.0), то для налаштування маршрутизації досить викликати:

```
1 | route add -net 192.168.36.0 netmask 255.255.255.0 eth0
```

Маршрут за замовчуванням налаштовується наступною командою:

```
1 | route add default gw 192.168.1.1 eth0
```

Опція gw вказує програмі route, що наступний аргумент – це IP-адреса або ім'я маршрутизатора, на який треба відправляти всі пакети, відповідні цьому рядку таблиці маршрутизації.

Протокол маршрутизації (RIP, OSPF, IGRP, EIGRP, IS-IS, BGP, HSRP тощо) може працювати тільки з пакетами, які належать до одного з маршрутизованих протоколів, наприклад, IP, IPX чи AppleTalk.

- RIP (Routing Information Protocol) – один із найрозповсюдженіших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію (напрямок і дальність в хопх), отримуючи її від сусідніх маршрутизаторів.

- OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху.

- EIGRP (Enhanced Interior Gateway Routing Protocol) – це дистанційно-векторний протокол маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора. EIGRP обчислює і враховує 5 параметрів для кожної ділянки маршруту між вузлами мережі:

- Total Delay – загальна затримка передачі (з точністю до мікросекунди);
- Minimum Bandwidth – мінімальна пропускна спроможність (в Кб/с);
- Reliability – надійність (оцінка від 1 до 255; 255 найбільш надійно);
- Load – завантаження (оцінка від 1 до 255; 255 найбільш завантажено);
- Maximum Transmission Unit (MTU) (не враховується при обчисленні оптимального маршруту, береться до уваги окремо) – максимальний розмір блоку, що можливо передати по ділянці маршруту.

- BGP (Border Gateway Protocol) – протокол граничного шлюзу, основний протокол динамічної маршрутизації в Інтернет.

BGP відрізняється від інших протоколів динамічною маршрутизацією, його призначення для обміну інформації про маршрути не між окремим маршрутизаторами, а між цілими автономними системами, і тому, крім інформації про маршрути в мережі, переносить також інформацію про маршрути на автономні системи. BGP не використовує технічні метрики, а здійснює вибір найкращого маршруту виходячи з правил, прийнятих в мережі.