КОМП'ЮТЕРНІ МЕРЕЖІ: архітектура, проектування, захист ПРАКТИКУМ

В. М. Ахрамович
В. М. Чегренець
А. М. Котенко

КОМП'ЮТЕРНІ МЕРЕЖІ

Архітектура
Проектування
Захист

Практикум

В.М. Ахрамович, В.М. Чегренець, А.М. Котенко

Комп'ютерні мережі. Архітектура, проектування, захист

Практикум

Київ 2018

УДК 004.7(075)

ББК 32. 884
А95

Схвалено Вченою радою Навчально-наукового інституту захисту інформації.
Державного університету телекомунікацій
(протокол № 2 від 3 вересня 2018 р.).

Ахрамович В.М., Чегренець В.М, Котенко А.М. Комп'ютерні мережі. Практикум /
А95 В.М. Ахрамович, В.М. Чегренець, А.М. Котенко // Державний університет телекомунікацій.
– К.: ДУТ, 2018. – 412 с. іл. – Бібліограф.: 404 с.

ISBN 978-617-571-028-9

Основна частина лабораторного практикуму присвячена розв'язку практичних завдань з ознайомлення й дослідження особливостей роботи програмного й апаратного забезпечення в сучасних інфокомунікаційних мережах. Вивчення лабораторних робіт покликано поставити студента в ситуацію схожу з виробничою, коли потрібно налагодити й підтримувати обчислювальну мережу в рамках квартири, лабораторії, будинку, підприємства. Лабораторні роботи знайомлять студента не тільки із правильними сценаріями розв'язку того або іншого завдання, але й дозволяють побачити основні ознаки й симптоми можливого некоректного налагодження мережевого встаткування й програмного забезпечення в результаті тих або інших розповсюджених помилок.

Усі лабораторні роботи розбиті на три розділи. У першому розділі: показані приклади створення мережі: з двох комп'ютерів; за топологією «зірка» на базі комутатора; Fast Ethernet; безпроводової; налагодження різного встаткування; використання спеціальних мережевих утиліт; забезпечення роботи локальних мереж за допомогою можливостей різного технічного забезпечення, операційних систем та програмного забезпечення; у другому – вивчення структури IP-адрес; монтаж та налагодження бездротової та кабельної корпоративних мереж; показані приклади розрахунку, розмноження та моделювання мереж; можливості комутаторів; дослідження роботи DNS сервера; створення, налагодження та роботу корпоративних мереж за допомогою можливостей різного технічного забезпечення, операційних систем та програмного забезпечення, у третьому: показані приклади моніторингу, перевірки різних показників мереж; розробки Web-сайтів мовою HTML; підключення, налагодження та роботи в глобальних мережах за допомогою можливостей різного технічного забезпечення, операційних систем та програмного забезпечення; приклади: відомих пошукових систем, пошуку потрібної інформації; закачування її за допомогою спеціальних програм; робота з FTP архівами; встановлення програмного забезпечення з глобальної мережі, роботи: з поштою, в телеконференціях, в пірінговій мережі а також за допомогою хмарних технологій.

У всіх розділах наведені приклади налагодження захисту мереж з використанням стандартного технічного та програмного забезпечення.

УДК 004.7(075)

ББК 32. 884

ISBN 978-617-571-028-9

ЗМІСТ

Вступ **10**

РОЗДІЛ 1. ЛОКАЛЬНІ МЕРЕЖІ **13**

ЛАБОРАТОРНА РОБОТА 1. СТВОРЕННЯ З'ЄДНАННЯ ДВОХ КОМП'ЮТЕРІВ **13**

1. Теорія 13
   1.1. Порт послідовної передачі даних (RS-232) 14
2. Хід роботи: 17
   2.1. Підготовка до виконання лабораторної роботи 17
   2.2. Виконання лабораторної роботи 19
3. Контрольні питання 23

ЛАБОРАТОРНА РОБОТА 2. ПОБУДОВА МЕРЕЖІ ЗА ТОПОЛОГІЄЮ «ЗІРКА» НА БАЗІ КОМУТАТОРА **24**

1. Завдання для роботи 24
2. Необхідне встаткування: 24
3. Хід роботи 24
4. Контрольні питання 28

ЛАБОРАТОРНА РОБОТА 3. ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ FAST ETHERNET **29**

1. Завдання для роботи 29
2. Перелік засобів, що забезпечують роботу 29
3. Теорія 29
   3.1. Технологія Fastethernet 29
   3.2. Монтаж мережевих розеток 30
   3.3. Прокладання локальної мережі Fastethernet 30
4. Хід роботи 32
5. Контрольні питання 34

ЛАБОРАТОРНА РОБОТА 4. НАЛАШТУВАННЯ МЕРЕЖІ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS 7 ..... **35**

1. Теорія 35
   1.1. Відкриття компонента «Центр управління мережами і загальним доступом» 37
   1.2. Поняття мережевого розташування 37
   1.3. Карта мережі 39
   1.4. Мережеві підключення. 41
   1.5. Підключення до мережі для Windows 7 46
2. Хід роботи 50
3. Контрольні питання 50

ЛАБОРАТОРНА РОБОТА 5. НАЛАГОДЖЕННЯ ПАРАМЕТРІВ ЛОКАЛЬНОЇ МЕРЕЖІ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS XP **51**

1. Теорія 51
   1.1. Налагодження параметрів локальної мережі 51
   1.2. Підключення мереженого принтера 56
2. Хід виконання роботи 58
3. Контрольні питання 58

ЛАБОРАТОРНА РОБОТА 6. НАЛАГОДЖЕННЯ БЕЗПРОВОДОВОЇ МЕРЕЖІ **59**

1. Теорія 59
   1.1. Беспроводовий маршрутизатор 59
   1.2. Розміщення безпроводового маршрутизатора 59
   1.3. Безпека безпроводової мережі 60
2. Хід роботи 61
   2.1. Підключення до безпроводової мережі за допомогою адаптера в ОС Windows 7 61
   2.1.1. Додавання комп'ютерів до мережі 61
   2.1.2. Підключення до мережі за віддаленим з'єднанням. 62
   2.2. Підключення до безпроводової мережі за допомогою модему в ОС Windows XP 64
3. Контрольні питання 65

АБОРАТОРНА РОБОТА 7. НАЛАГОДЖЕННЯ В ЛОКАЛЬНІЙ МЕРЕЖІ ТА РОБОТА З РІЗНИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ. **66**

1. Теорія 66

1.1. Домашня мережа Windows. 66
1.2. Об'єднання в мережу домашніх комп'ютерів, що працюють під управлінням різних версій Windows 70
1.3. Пошук імені та Ip-Адреси комп'ютера 73
1.4. Призначення загального каталогу 75
1.5. Установка принтера в мережі 76
1.6. Установлення мережевого диска 77
1.7. Визначення завантаження ресурсів комп'ютера та мережі 81
1.8. Приклади роботи у локальній мережі Windows за допомогою різноманітного програмного забезпечення 81
2. Хід роботи: 85
3. Контрольні питання: 85

ЛАБОРАТОРНА РОБОТА 8. КОМУНІКАЦІЙНІ УТИЛІТИ ДЛЯ РОБОТИ В МЕРЕЖІ 86
1. Теорія 86
1.1. Утиліта IPconfig 86
1.2. Утиліта Ping 89
1.3. Утиліта Tracert 90
1.4. Утиліта Netstat 90
1.5. Утиліта Pathping 92
1.6. Утиліта Route 93
1.7. Команда Ivconfig для пристрою «Ноутбук» 95
1.8. Утиліта ARP 95
2. Хід роботи 96
3. Контрольні питання 100

РОЗДІЛ 2. КОРПОРАТИВНІ МЕРЕЖІ 102

ЛАБОРАТОРНА РОБОТА 9. МОНТАЖ І НАЛАГОДЖЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI 102
1. Теорія 102
2. Хід роботи 102
2.1. Налагодження мережі зі статичною адресою комп'ютера клієнта. 102
2.2. Налагодження крапки доступу Wi-Fi і DHCP-Сервера. 104
2.3. Перевірка працездатності бездротової мережі. 106
2.4. Налагодження мережі з динамічною адресою комп'ютера клієнта. 106
2.5. Перевірка роботи бездротової мережі. 107
3. Контрольні питання 108

ЛАБОРАТОРНА РОБОТА 10. НАЛАГОДЖЕННЯ WI-FI РОУТЕРА 109
1. Теорія 109
2. Хід роботи 111
2. 1. Установлення паролю на доступ до налагодження Wi-Fi роутера 112
2.2. Установлення паролю на Wi-Fi мережу й установлення типу шифрування 112
2.3. Приховування імені мережі (SSID) 112
2. 4. Включення фільтрації пристроїв за MAC адресами 113
2. 5. Відключення служби QSS (WPS) 113
3. Контрольні питання 113

ЛАБОРАТОРНА РОБОТА 11. НАЛАГОДЖЕННЯМ МЕРЕЖЕВИХ ПАРАМЕТРІВ ОС CISCO IOS, МАРШРУТИЗАТОРА CISCO 2811 114
1. Теорія 114
2. Хід роботи 119
2.1. Налагодження мережевих параметрів ОС Cisco IOS маршрутизатора Cisco 2811 з робочої станції адміністратора мережі. 119

ЛАБОРАТОРНА РОБОТА 12. ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ КОМУТАТОРІВ ВІД D-LINK 122
1. Теорія 122
2. Хід роботи 122
2.1. Необхідне встаткування: 122
2.2. Визначення та надання параметрів 122
2.3. Підключення до Web-Інтерфейсу комутатора 123
3. Контрольні питання 124

ЛАБОРАТОРНА РОБОТА 13. ВИВЧЕННЯ СТРУКТУРИ IP-АДРЕС 125
1. Теорія 125
1.1. Типи адрес стека TCP/IP 125
1.2. Класи Ip-Адрес 125
1.3. Особливі Ip-Адреси 126
1.4. Використання масок в Ip-Адресації 127
2. Хід роботи 131
2.1. Завдання на лабораторну роботу 131
3. Контрольні питання 131

ЛАБОРАТОРНА РОБОТА 14. СЛУЖБА ДОМЕННИХ ІМЕН (DNS). УСТАНОВКА ТА НАЛАГОДЖЕННЯ DNS-СЕРВЕРА НА БАЗІ WINDOWS 2003 SERVER 132
1. Теорія 132
1.1. Доменні імена 132
1.2. Служба трансляції імен в Internet 133
1.3. Функції DNS 133
1.4. Загальні принципи функціонування DNS 134
2. Установка й налагодження DNS сервера на базі ОС Windows 2003 Server 136
3. Контрольні питання 136
4. Завдання на лабораторну роботу 136

ЛАБОРАТОРНА РОБОТА 15. БАЗИ ДАНИХ DNS СЕРВЕРА 143
1. Теорія 143
1.1. Режими роботи DNS сервера 143
1.2. Записи ресурсів у базі даних домену 143
1.3. Особливості розміщення й конфігурування серверів для корпоративної мережі 147
1.4. Установка ПЗ сервера DNS 148
1.5. Конфігурування сервера DNS 149
1.6. Тестування роботи сервера імен 151
2. Хід роботи 153
3. Контрольні питання 153

ЛАБОРАТОРНА РОБОТА 16. РЕЗЕРВНЕ КОПІЮВАННЯ В WINDOWS SERVER 2012 .. 154
1. Теорія 154
1.1. Створення копії 154
1.2. Організація резервного копіювання за розкладом. 157
1.3. Відновлення даних 159
2. Хід роботи 160
3. Контрольні питання 161

ЛАБОРАТОРНА РОБОТА 17. УСТАНОВКА НОВОГО ЯДРА LINUX 162
1. Теорія 162
1.1. Вступ 162
1.2. Загальні відомості 162
2. Хід роботи 172
3. Контрольні питання 172

ЛАБОРАТОРНА РОБОТА 18. ПОБУДОВА МЕРЕЖІ В ОС LINUX» 173
1. Побудова мережі 173
1.1. Вивчення vlan. 173
I.2. Будуємо мережу між vm1, vm2 в одному vlan. 174
1.3. Розбиваємо vm1 vm2 на різні vlan. Набудовуємо intervlan routing за допомогою R1. 179
2. Хід роботи 184
3. Контрольні питання 184

ЛАБОРАТОРНА РОБОТА 19. МЕТОДИКА РОЗРАХУНКУ КОНФІГУРАЦІЇ МЕРЕЖІ ETHERNET 185
1. Теорія 185
1.1. Розрахунок мереж Ethernet 185
1.2. Розрахунок PDV 186
1.3. Розрахунок PW 189
1.4. Розрахунок мережі Fast Ethernet 189
2. Хід роботи 191
3. Контрольні питання 194

ЛАБОРАТОРНА РОБОТА 20. МОДЕЛЮВАННЯ МЕРЕЖІ, ЗНАЙОМСТВО ІЗ СЕРЕДОВИЩЕМ CISCO PACKET TRACER 195
1. Хід роботи 195
1.1. Побудова топології мережі 195
1.2. Побудова топології мережі, що складається із двох підмереж 205
2. Контрольні питання 206

ЛАБОРАТОРНА РОБОТА 21. КЛОНУВАННЯ РОБОЧИХ СТАНЦІЙ 207
1. Хід роботи 207
1.1. Установка програми GHOST на сервер 207
1.2. Створення завантажувальної дискети 207
1.3. Створення образу диска 208
1.4. Розгортання образу диску 208
1.5. Symantec Ghost 11.5 208
2. Контрольні питання 213

РОЗДІЛ 3. ГЛОБАЛЬНІ МЕРЕЖІ 214

ЛАБОРАТОРНА РОБОТА 22. НАЛАГОДЖЕННЯ ПІДКЛЮЧЕННЯ ДО INTERNET В WINDOWS 10, D-LINK ТА CISCO 214
1. Хід роботи 214
1.1. Налагодження підключення до Internet в Windows 10 214
1.1.1. Ethernet: підключення до Internet в Windows 10 за мережевім кабелю (роутер, модем) 214
1.1.2. Налаштування високошвидкісного з'єднання (Pppoe) в Windows 10 216
1.1.3. Підключення до Internet за Wi-Fi 217
1.1.4. Налаштування Internet через 3G/4G модем в Windows 10 218
1.2. Налагодження підключення до Internet в D-Link 220
1.3. Налагодження доступу до Internet через маршрутизатор Cisco 226
2. Контрольні питання 229

ЛАБОРАТОРНА РОБОТА 23. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ INTERNET В ОС WINDOWS XP. 230
1. Хід роботи 230
1.1 Установка драйверів дата-кабелю й модему Huawei 230
2. Контрольні питання 238

ЛАБОРАТОРНА РОБОТА 24. НАЛАГОДЖЕННЯ ДОСТУПУ ДО МЕРЕЖІ INTERNET З ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ WIN 2003 SERVER. 239
1. Теорія 239
2. Хід роботи: 241
2.1. Налагодження підключення через Win2003 Server. NAT 241
2.2. Налагодження підключення через Winxp. Internet Connection Sharing. 243
2.3. Налагодження підключення через Winxp. Проксі-Сервер 245
3. Контрольні питання 245

ЛАБОРАТОРНА РОБОТА 25. НАЛАГОДЖЕННЯ ВІДДАЛЕНОГО З'ЄДНАННЯ ІЗ СЕРВЕРОМ 246
1.Теорія 246
1.1. Загальні відомості 246
1.2. MNP- протоколи 246
1.3. Протокол V90 247
1.4. Режими MNP-модемів 248
1.5. Внутрішні і зовнішні модеми 248
1.6. Марки модемів 250
2. Хід роботи 251
3. Контрольні питання 253

ЛАБОРАТОРНА РОБОТА 26. СТВОРЕННЯ INTERNET ПІДКЛЮЧЕННЯ НА ПРИКЛАДІ АБОНЕНТІВ CDMA WLL, З'ЄДНАННЯ ЧЕРЕЗ РАДІОМОДЕМ, В MICROSOFT WINDOWS XP ТА WINDOWS 7 254
1. Хід роботи 254
1.1. Створення Internet підключення в Microsoft Windows XP 254
1.2. Створення Internet підключення в Microsoft Windows 7 257
2. Контрольні питання 258

ЛАБОРАТОРНА РОБОТА 27. МОНІТОРИНГ МЕРЕЖ 259
1. Теорія 259
1.1. Вступ 259
1.2. Wireshark Network Analyzer 259
2. Хід роботи 262
3. Контрольні питання 263

ЛАБОРАТОРНА РОБОТА 28. СКАНУВАННЯ МЕРЕЖ 264
1. Теорія 264
1.1. Опис програми 264
1.1.1. Основне призначення програми: 264
1.1.2. Можливості програми: 265
1.2. Початок роботи із програмою 265
1.3. Створення списку хостів мережі 267
1.4. Видалення хосту 271
1.5. Включення комп'ютерів за мережею 274
1.6. Інформація про систему 274
1.7. Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP 280
1.8. Робота з папками 281
1.9. Пінг 282
1.10. Трасування маршруту 282
1.11. Мережевий трафік 282
2. Хід роботи 283
3. Контрольні питання 283

ЛАБОРАТОРНА РОБОТА 29. ЗНАЙОМСТВО З ПРОГРАМАМИ КОНТРОЛЮ ТРАФІКУ МЕРЕЖ 284
1. Теорія 284
1.1. Поняття трафіку мереж 284
1.2. Лічильники трафіку 285
1.3. Приклади програмного забезпечення контролю трафіка 285
2. Хід роботи 293
3. Контрольні питання 294

ЛАБОРАТОРНА РОБОТА 30. УСТАНОВЛЕННЯ MICROSOFT OFFICE 2016 ЗА ГЛОБАЛЬНОЮ МЕРЕЖЕЮ 295
1. Хід роботи 295
1.1. Закачування установочних файлів 295
1.2. Встановлення компонентів Microsoft Office 2016 298
1.3. Перевірка працездатності компонентів Microsoft Office 2016 300
1.4. Активування компонентів 303
2. Контрольні питання 309

ЛАБОРАТОРНА РОБОТА 31. ПРОГРАМА ЕЛЕКТРОННОЇ ПОШТИ OUTLOOK EXPRESS 310
1. Теорія 310
1.1. Налагоджування Outlook Express 310
1.2. Користувальницький інтерфейс пошти Outlook Express 312
1.3. Формування нового повідомлення 314
1.4. Пересилання вкладених файлів за E-Mail 315
1.5. Одержання вхідної пошти 317
1.6. Адресна книга Outlook Express 317
1.7. Деякі додаткові можливості програми 319
1.8. Протокол відправлення електронної пошти SMTP 319
1.9. Протокол одержання електронної пошти POP3 320
2. Хід роботи: 321
3. Контрольні питання 321

ЛАБОРАТОРНА РОБОТА 32. РОБОТА З FTP АРХІВАМИ 322
1. Теорія 322
1.1. Файлові архіви і їх роль 322
1.2. Утиліта FTP і основні FTP-команди 322
1.3. Приклад використання утиліти FTP 324
1.4 Доступ до FTP-серверів за допомогою браузера 325

1.5. Пошук файлів у FTP-Архівах 326
2. Варіанти виконання завдань. 327
3. Контрольні питання 330

ЛАБОРАТОРНА РОБОТА 33. ЗАКАЧУВАННЯ ФАЙЛІВ ЗА ДОПОМОГОЮ ПРОГРАМ TELEPORT PRO ТА FLASHGET 331
1. Теорія 331
1.1. Закачування файлів за допомогою програми Teleport Pro 331
1.2. Створення нового проекту 331
1.3. Збереження проекту 334
1.4. Запуск проекту 334
1.5. Перегляд результатів 335
1.6. Закачування файлів за допомогою програми FlashGet 337
1.7. Головне меню програми FlashGet 340
2. Хід роботи 341
3. Контрольні питання 342

ЛАБОРАТОРНА РОБОТА 34. РОБОТА З БРАУЗЕРОМ MICROSOFT INTERNET EXPLORER 343
1. Теорія 343
1.1. Способи запуску програми Internet Explorer. 343
1.2. Пошук інформації у мережі Internet 343
1.3. Засоби пошуку 345
1.4. Методика пошуку 345
1.5. Управління процесом пошуку 346
1.6. Результати пошуку 347
1.7. Обмеження доступу 347
1.8. Робота в Internet Explorer з поштою 347
2. Хід роботи 351
3. Контрольні питання 352
Додаток 1 352

ЛАБОРАТОРНА РОБОТА 35. СТВОРЕННЯ WEB-СТОРІНОК 354
1. Теорія 354
1.1 Мова HTML 354
1.2 Мова HTML і WEB- дизайн 356
1.3 Вставляння звуку і відеозображення. 360
1.4 . Поняття про динамічні ефекти. 361
1.5 Web-компоузери. 361
1.6 Розміщення WEB-сайту в Інтернеті 362
2. Хід роботи 364
3. Контрольні питання 364

ЛАБОРАТОРНА РОБОТА 36. РОБОТА З ГРУПАМИ НОВИН 365
1. Теорія 365
1.1. Загальні відомості про групи новин (телеконференції) 365
1.2. Підписка на групи новин 365
1.3. Завантаження, перегляд, сортування, фільтрація та пошук повідомлень 366
1.4. Підготовка і відправлення повідомлень у групу новин 366
2. Хід роботи 367
3. Контрольні питання 367

ЛАБОРАТОРНА РОБОТА 37. РОБОТА В ПІРІНГОВІЙ МЕРЕЖІ 368
1. Теорія 368
1.1. Вступ 368
1.2. Програма BitComet 369
1.3. Програма µTorrent 372
2. Хід роботи 375
3. Контрольні питання 375

ЛАБОРАТОРНА РОБОТА 38. ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ 376
1. Теорія 376
1.1. Загальні поняття 376
1.2. Огляд хмарних технологій 378

2. Хід роботи 382
2.1. Реєстрація акаунта 382
2.2. Робота в акаунті 383
3. Контрольні питання. 388
Додаток 1. Види кабелів 391
Додаток 2. Модеми 393
Додаток 3. Радіомодеми 396
Додаток 4. Список відкритих FTP серверів з коротким описом: 398
Додаток 5. Список пошукових систем Internet з коротким описом: 402
СПИСОК ВИКОРИСТОВАННОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 410

ВСТУП

Роль комп'ютерних мереж у наш час переоцінити важко. Це й робота в команді роз'єднаних територіально розроблювачів. Це й зберігання даних у мережевих сховищах. Це, нарешті, звичайне людське спілкування – чат, електронна пошта, живе on-line відеоспілкування партнерів і друзів. В практикумі розбираються проблеми побудови, роботи й обслуговування комп'ютерних мереж як необхідного елемента підготовки IT-фахівця.

Базовими знаннями в області сучасних інфокомунікаційних мереж можна вважати розуміння її апаратної і програмної частин. До апаратної частини слід віднести різні мережеві пристрої для створення локальних, муніципальних, корпоративних, регіональних і глобальних мереж, середовища передачі даних. До програмної складової відносять алгоритми й програмні засоби, функціонуючі за допомогою цієї апаратури.

Разом зі здешевленням електронно-обчислювальних машин на початку 60-х років з'явилися нові способи організації обчислювального процесу, які дозволили врахувати інтереси користувачів. Почали розвиватися інтерактивні багатотермінальні системи. У таких системах комп'ютер віддавався в розпорядження відразу декільком користувачам. Кожен користувач отримував у своє розпорядження термінал, за допомогою якого він міг вести діалог із комп'ютером. При цьому користувачеві була помітна паралельна робота з комп'ютером інших користувачів. Розділяючи, таким чином, комп'ютер, користувачі дістали можливість за порівняно невелику плату користуватися перевагами комп'ютеризації.

Термінали, вийшовши за межі обчислювального центру, розповсюдились на території підприємства. І хоча обчислювальна потужність залишалася повністю централізованою, деякі функції – такі як введення й виведення даних – стали розподіленими. Такі багатотермінальні централізовані системи зовні вже були дуже схожі на локальні обчислювальні мережі. Дійсно, рядовий користувач роботу за терміналом мейнфрейма сприймав приблизно так само, як зараз він сприймає роботу за підключеним до мережі персональним комп'ютером. Користувач міг дістати доступ до спільних файлів і периферійних пристроїв, при цьому в нього підтримувалася повна ілюзія одноосібного володіння комп'ютером, оскільки він міг запустити потрібну йому програму в будь-який момент, і майже відразу ж отримати результат.

Комп'ютерні мережі передачі даних являють собою результат еволюції комп'ютерних технологій і в цей час утворюють основний засіб комунікації. Створення комп'ютерних мереж викликане потребою спільного використання інформації на віддалених один від одного комп'ютерах. Основне призначення комп'ютерних мереж – спільне використання ресурсів і здійснення зв'язків як усередині однієї організації, так і за її межами.

Базові компоненти й технології, пов'язані з архітектурою локальних або глобальних мереж, можуть містити в собі: сервери, концентратори, комутатори, маршрутизатори, комп'ютери, засоби зв'язку між пристроями. Таким чином, комп'ютерна мережа являє собою комплекс розподіленої комп'ютерної техніки, з'єднаної між собою системою передачі даних, що містить комунікаційне встаткування й канали зв'язку.

На підставі відкритих систем (OSI) Міжнародний інститут стандартів (ISO) розробив семирівневу модель у комп'ютерній мережі. Відповідно до цієї моделі взаємодія користувачів через мережу відбувається за допомогою мережевих протоколів, кожний з яких працює на конкретному рівні. Під мережевим протоколом розуміється суворо формалізована процедура взаємодії користувачів мережі.

У процесі навчання технологіям комп'ютерних мереж викликає утруднення практична частина дослідження телекомунікаційних систем: побудова топології мережі, налаштування інтерфейсів, взаємодія мережевих протоколів і т.п.

Навіть у результаті достатнього поверхневого розгляду роботи в мережі стає ясно, що обчислювальна мережа – це складний комплекс взаємозв'язаних і погоджено

функціонуючих програмних і апаратних компонентів. Вивчення мережі в цілому вимагає знання принципів роботи її окремих елементів:

- комп'ютерів;
- операційних систем;
- спеціального мережевого та комунікаційного обладнання;
- мережевих програмних систем .

Увесь комплекс програмно-апаратних засобів мережі може бути описаний багатошаровою моделлю. В основі будь-якої мережі лежить апаратний шар стандартних комп'ютерних платформ. У даний час в мережах широко і успішно застосовуються комп'ютери різних класів – від персональних комп'ютерів до мейнфреймів і СуперЕОМ. Набір комп'ютерів у мережі повинен відповідати набору різноманітних задач, що вирішуються мережею.

Другий шар – це комунікаційне устаткування. Хоча комп'ютери і є центральними елементами обробки даних у мережах, останнім часом не менш важливу роль почали грати комунікаційні пристрої. Кабельні системи, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори з допоміжних компонентів мережі перетворилися на основних разом із комп'ютерами й системним програмним забезпеченням як за впливом на характеристики мережі, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим мультипроцесором, який потрібно конфігурувати, оптимізувати й адмініструвати. Вивчення принципів роботи комунікаційного устаткування вимагає знайомства з великою кількістю протоколів, які використовуються як у локальних, так і глобальних мережах.

Третій шар, який створює програмну платформу мережі, – операційні системи (ОС). Від того, які концепції управління локальними й розподіленими ресурсами покладені в основу мережевої ОС, залежить ефективність роботи всієї мережі. При проектуванні мережі важливо враховувати, наскільки просто дана операційна система може взаємодіяти з іншими ОС мережі, наскільки вона гарантує безпеку й захищеність даних, наскільки вона дозволяє нарощувати число користувачів, чи можна перенести її на комп'ютер іншого типу й багато інших міркувань.

Найвищий шар мережевих засобів – різні мережеві програмні системи, такі як мережеві бази даних, поштові системи, засоби архівації даних, системи автоматизації колективної роботи, програми перевірки параметрів мережі, захисту від вторгнень та ін.

У практикуму відображено створення та налагодження локальних, корпоративних мереж; налагодження глобальних мереж; наведена необхідна теорія до них (в деяких випадках наведені характеристики спеціального програмного та технічного забезпечення, яке використовується) та зроблені висновки, розкриті проблеми, пов’язані з рішеннями вказаних задач.

Вивчення дисципліни «Комп'ютерні мережі» сприяє формуванню у студентів системи знань у галузі теорії та практики застосування і проектування сучасних мереж різних рівнів, програмних продуктів, технічних засобів, в тому числі, у сфері захисту інформації.

В результаті вивчення дисципліни студенти повинні знати: архітектуру комп'ютерних мереж, технічні засоби мереж, мережеві операційні системи та спеціальне програмне забезпечення.

Студенти повинні оволодіти навичками роботи в локальних та глобальних комп‘ютерних мережах з метою використання їх можливостей для отримання вихідних даних для розв'язання фахових задач, аналізу, володіти методами проектування, побудови та використання комп’ютерних мереж і захисту інформації в них.

Автори виражають подяку за виконаний обсяг робіт та допомогу в оформлення рукопису студентам групи СЗД-41 – Вовку М.О, групи БСД – 22 – Драгунцову Р.І.

Практикум буде корисним студентам при вивченні наступних навчальних дисциплін: «Комп’ютерні мережі», «Комп’ютерні мережі та телекомунікації», «Інтернет –

технології», «Операційні системи комп'ютерних мереж», «Пошук, обробка та аналіз інформації», «Глобальна інформаційна інфраструктура», «Хмарні технології», «Телекомунікаційні системи передачі», «Прикладні аспекти побудови комплексів технічного захисту інформації», «Засоби передачі та прийому сигналів в системах технічного захисту інформації», «Теорія захисту інформаційних ресурсів обмеженого доступу», «Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності», «Системи управління та контролю захистом інформації реального часу» і т.п.

РОЗДІЛ 1. ЛОКАЛЬНІ МЕРЕЖІ

ЛАБОРАТОРНА РОБОТА 1. СТВОРЕННЯ З'ЄДНАННЯ ДВОХ КОМП'ЮТЕРІВ

Мета роботи: навчитися будувати найпростішу мережу із двох ПК

Зміст

1. Теорія
1.1. Порт послідовної передачі даних (RS-232)
2. Хід роботи:
2.1. Підготовка до виконання лабораторної роботи
2.2. Виконання лабораторної роботи
3. Контрольні питання

1. Теорія

Для того щоб підключені до мережі комп'ютери, що мають, у загальному випадку, різну апаратну й програмну начинку, могли обмінюватися повідомленнями, необхідно щоб усі вони дотримувалися деяких загальних для всіх правил і процедур. Для розв'язку цієї проблеми на початку 80-х рр. XX ст. міжнародні організації за стандартизацією розробили модель, яка зіграла значну роль у розвитку інформаційно-обчислювальних мереж. Ця модель називається ***моделлю взаємодії відкритих систем*** або моделлю OSI *(Open System Interconnection)* і показана на рис. 1. Вона визначає різні рівні взаємодії відкритих систем, дає їм стандартні імена й указує, які функції повинен виконувати кожний рівень. Загальновідомим прикладом відкритої системи є Internet.

Модель OSI дозволяє розробляти нове апаратне й програмне мережеве забезпечення за загальними правилами, а також створювати програмно-апаратні комплекси із продуктів різних виробників.

Увесь процес взаємодії комп'ютерів в інформаційно-обчислювальних мережах представляється як ієрархія рівнів. Кожний із семи рівнів має власний звід правил (протоколів) і відповідну назву. У табл. 1 перераховані назви цих рівнів і коротко зазначені їхні функції.

Охарактеризуємо більш докладно канальний і фізичний рівні моделі OSI.

Канальний рівень або рівень керування каналом організує канал передачі інформаційних даних. Канальне з'єднання будується на одному або декількох фізичних з'єднаннях.

Таблиця 1

Коротка характеристика рівнів моделі OSI

Назва рівня	Виконувані рівнем функції
Прикладний	Забезпечує доступ прикладних програм користувачів до ресурсів, що поділяються (файлам, принтерам, Web-сторінкам). Завдання цього рівня – перенос файлів, обмін поштовими повідомленнями й керування мережею
Представницький	Забезпечує таємність обміну даними, долає синтаксичні відмінності у представленні даних або відмінності в кодах символів
Сеансовий	Установлює, підтримує й розриває сеанси зв'язку; синхронізує обмін даними; вставляє контрольні крапки (крапки «відкату») у довгі передачі
Транспортний	Ділить потоки інформації на досить малі фрагменти (пакети) для передачі їх на мережевий рівень; забезпечує необхідну надійність передачі даних, виявляє й виправляє такі помилки передачі як викривлення, втрата й дублювання пакетів

Мережевий	Забезпечує маршрутизацію, тобто вибір найкращого шляху передачі пакета; управляє інформаційними потоками й відповідає також за зв'язок між мережами
Канальний	Організує канал передачі інформаційних даних (у тому числі перевірку доступності каналу зв'язку); групує біти в кадри, обчислює для кадрів контрольну суму; забезпечує коректність передачі кадру
Фізичний	Характеризує фізичне середовище для передачі даних, включаючи смугу пропускання, швидкість передачі й ін., тип кабелю й призначення контактів роз'ємів; параметри використовуваних сигналів

1.1. Порт послідовної передачі даних (RS-232)

Порт послідовної передачі даних (RS-232) використовується для:

* підключення миші;
* підключення графобудівників (плотерів), сканерів, принтерів;
* Організації зв'язку двох комп'ютерів;
* підключення модемів для передачі даних за телефонними лініями;
* підключення до мережі персональних комп'ютерів;
* реалізації інших функцій.

Послідовна передача даних припускає, що дані передаються з використанням однієї пари проводів. У послідовному порту передача даних носить асинхронний характер. ЕОМ посилає або ухвалює байти інформації порціями по одному байту. Тимчасові інтервали між байтами при цьому несуттєві, але дуже важливі інтервали між окремими бітами байта.

Для синхронізації групі битів звичайно передує спеціальний стартовий біт. Після групи битів даних випливає, як правило, біт перевірки на парність і один або два стопові біти як показано на рис. 1.

Вихідний стан лінії послідовної передачі даних – рівень логічної одиниці. Стартовий біт сигналізує про початок передачі даних. Далі передаються біти даних: спочатку молодші, потім старші. Якщо використовується біт парності, то передається й він. Цей біт використовується для контролю правильності передачі й пошуку помилок. Біт парності має таке значення, щоб у пакеті загальна кількість одиниць була парною (контроль на парність) або непарною (контроль на непарність).

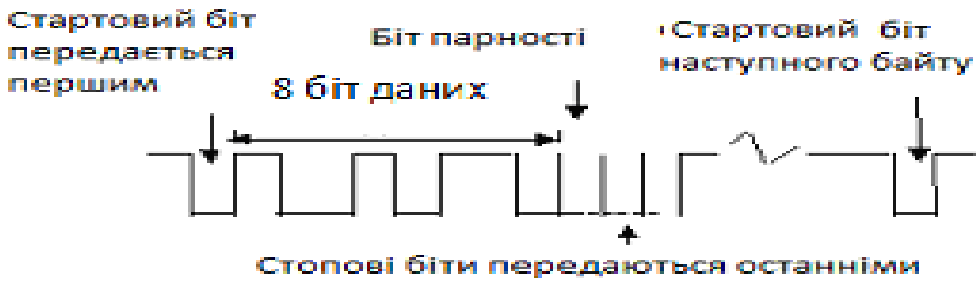


Рис. 1. Передача одного байта послідовних даних

Завершують передачу байта один або два стопові біти. Потім рівень лінії передачі знову встановлюється в одиницю до приходу наступного стартового біта.

Сукупність стартового, стопового (стопових) і біта парності визначає протокол передачі даних (або протокол обміну). Передавач і приймач даних повинні використовувати той самий протокол обміну.

Швидкість передачі даних звичайно виміряється в бодах. *Боди* – це загальна кількість переданих біт у секунду. При цьому враховуються й старт/стопові біти, а також біт парності. Ефективна швидкість передачі виміряється в кількості корисних битів у секунду (bps) без обліку витрат на передачу службових битів.

Зовнішні пристрої підключаються до порту RS-232 через 25-контактний (COM2) або 9-контактний (COM1) роз'єм.

Як правило, комп'ютери постачаються з більш ніж одним портом зв'язку типу RS-232. Для їхнього позначення використовуються абревіатури COM1, COM2**,** COM3 і т.д. Як правило, до порту COM1 підключається «миша». Звертання до порту здійснюється через його адреси. Кожний порт має діапазон використовуваних адрес. Для портів COM1 і COM2 вони наведені в табл. 2 (адреси для COM2 зазначені в дужках).

Таблиця 2

Призначення регістрів портів COM1 і COM2

Адреса регістру	Призначення регістру
3F8H (2F8H)	Регістр даних
3F9H (2F9H)	Регістр керування перериваннями
3FAH (2FAH)	Регістр ідентифікації переривання
3FBH (2FBH)	Регістр керування
3FDH (2FDH)	Регістр стану лінії
3FEH (2FEH)	Регістр стану модему

Найменування й призначення різних провідників стандартного 25-контактного рознімання COM1 (COM2) наведені в табл. 3. Поряд з 25-контактним рознімання часто використовується 9-контактне рознімання, найменування й призначення різних провідників якого наведені в табл. 4.

Таблиця 3

Найменування й призначення провідників стандартного 25-контактного роз'єму COM1 (COM2)

Номер контакту	Призначення контакту	Вхід або вихід
1	Захисне заземлення	–
2	Передані дані	Вихід
3	Прийняті дані	Вхід
4	Запит для передачі	Вихід
5	Скидання для передачі	Вхід
6	Готовність даних	Вхід
7	Сигнальне заземлення	–
8	Детектор прийнятого з лінії сигналу	Вхід
20	Готовність вихідних даних	Вихід
22	Індикатор виклику	Вхід
9-19, 21, 23-25	Не використовується	–

Розглянемо роботу з деякими зі згаданих у табл. 2 регістрів.

Керування портами здійснюється записом у регістри або зчитуванням з них чисел. Це можна здійснювати програмно, наприклад, на мовах асемблер або C++, а також звертаючись до функцій базової системи введення-виводу BIOS.

Регістр керування (3FBH або 2FBH) доступний для читання й за записом**.** Його використовують для завдання протоколу передачі даних і швидкості передачі. Формат цього регістру представлений у табл. 5. Для установлення протоколу в регістр керування слід записати ціле число − байт, використовуючи функцію **outportb().**

Таблиця 4

Найменування й призначення провідників стандартного 9-контактного роз'єму COM1 (COM2)

Номер контакту	Призначення контакту	Вхід або вихід
1	Детектор прийнятого з лінії сигналу	Вхід
2	Прийняті дані	Вхід
3	Передані дані	Вихід
4	Готовність вихідних даних	Вихід
5	Сигнальне заземлення	–
6	Готовність даних	Вхід
7	Запит для передачі	Вихід
8	Скидання для передачі	Вхід
9	Індикатор виклику	Вхід

Регістр 3F8H (2F8H) можна використовувати для двох цілей: установлення швидкості передачі (для цього в 7-м битці регістру 3FBH (2FBH) повинна бути встановлено 1), і для приймання або передачі даних (для цього в 7-м битці регістру 3FBH (2FBH) повинен стояти 0 – він встановлений за замовчуванням). Для установлення швидкості передачі в регістр 3F8H (2F8H) слід записати (використовуючи функцію З++ **outportb()**, десяткове число відповідно до табл. 6.

Таблиця 5

Формат регістру керування 3FBH (2FBH)

Біти	Опис
0-1	Довжина слова в бітах: 00 – 5 біт; 01 – 6 біт; 10 – 7 біт; 11 – 8 біт
2	Кількість стопових біт: 0 – 1 біт; 1 – 2 біта
3-4	Парність: 00 – контроль не використовується; 01 – контроль на непарність; 11 – контроль на парність
5	Фіксація парності. При установці цього біта, біт парності завжди ухвалює значення 0 (якщо біти 3–4 рівні 11) або 1 (якщо біти 3–4 рівні 01)
6	Установка переривання. Викликає вивід рядка нулів як сигналу BREAK для підключеного пристрою
7	1 – регістри 3F8H (2F8H) використовуються для завантаження швидкості передачі; 0 – регістри 3F8H (2F8H) використовуються для приймання або передачі даних

Регістр стану лінії 3FDH (2FDH) використовується для організації й контролю правильності передачі даних. Його формат представлений у табл. 7.

Перед тем як відправити байт у порт 3F8H (2F8H) (а значить і в лінію зв'язку) або зчитати його з порту, використовуючи функцію **inportb()**, прочитати регістр 3FDH (2FDH). Потім, виділивши й проаналізувавши біт (чи рівний він одиниці) стану приймача (0-й) або передавача (5-й), можна (якщо біт дорівнює одиниці) записувати/зчитувати байт в/із регістру 3F8H (2F8H). Процес читання й аналізу вмісту регістру 3FDH (2FDH) слід організувати в циклі.

Таблиця 6

Залежність швидкості передачі даних від значення дільника частоти

Число	Швидкість передачі в бодах	Число	Швидкість передачі в бодах
1040	110	24	4800
768	150	12	9600
384	300	6	19200
192	600	3	38400
96	1200	2	57600
48	2400	1	115200

Таблиця 7

Формат регістру стану лінії 3FDH (2FDH)

Біти	Опис
0	Дані отримані й готові для читання. Біт скидається при читанні даних з регістру 3F8H (2F8H)
1	Помилка переповнення. Була прийнята нова порція даних, а попередня ще не була зчитана. Попередня порція загублена
2	Помилка парності. Скидається після читання стану лінії
3	Помилка синхронізації
4	Виявлений запит на переривання передачі BREAK: довгий рядок нулів
5	Регістр зберігання передавача порожній. У нього можна записувати нову порцію інформації для передачі
6	Регістр зрушення передавача порожній. Цей регістр одержує дані з регістру зберігання й перетворить їх у послідовний вид для передачі
7	Минув час очікування

2. Хід роботи:

2.1. Підготовка до виконання лабораторної роботи

1. Підготувати два ПК до побудови мережі.
2. Встановіть мережеві адаптери (рис. 2).

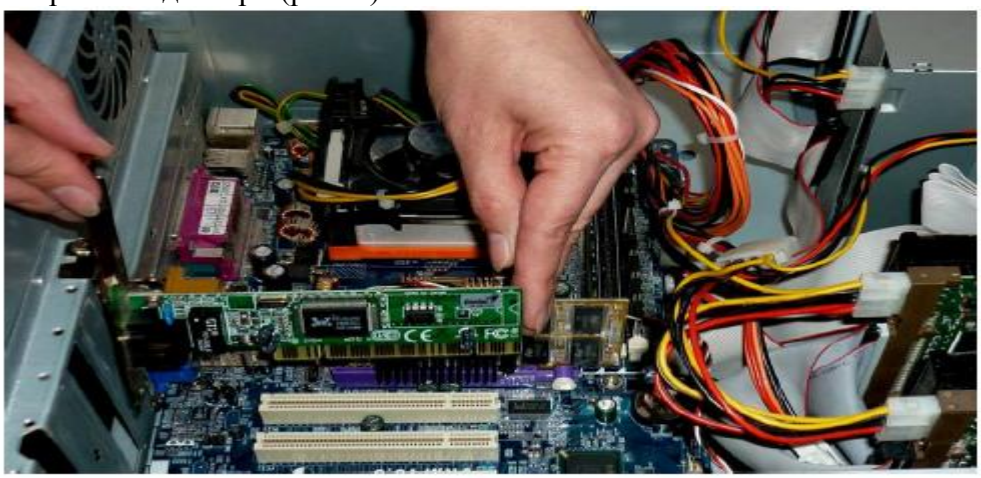


Рис. 2. Встановлення мережевого адаптера на материнську плату

3. Мережевий адаптер (мережна плата) – знаходиться всередині системного блоку і тому його параметри можна побачити, використовуючи засоби операційної системи.

Для цього слід правою кнопкою миші клацнути по значку **Мой компьютер** та обрати пункт **Свойства** контекстного меню. У вікні **Свойства** слід обрати вкладнику **Оборудование** та натиснути кнопку **Диспетчер устройств**. З'явиться вікно, в якому можна передивитись наявне обладнання (рис. 3)

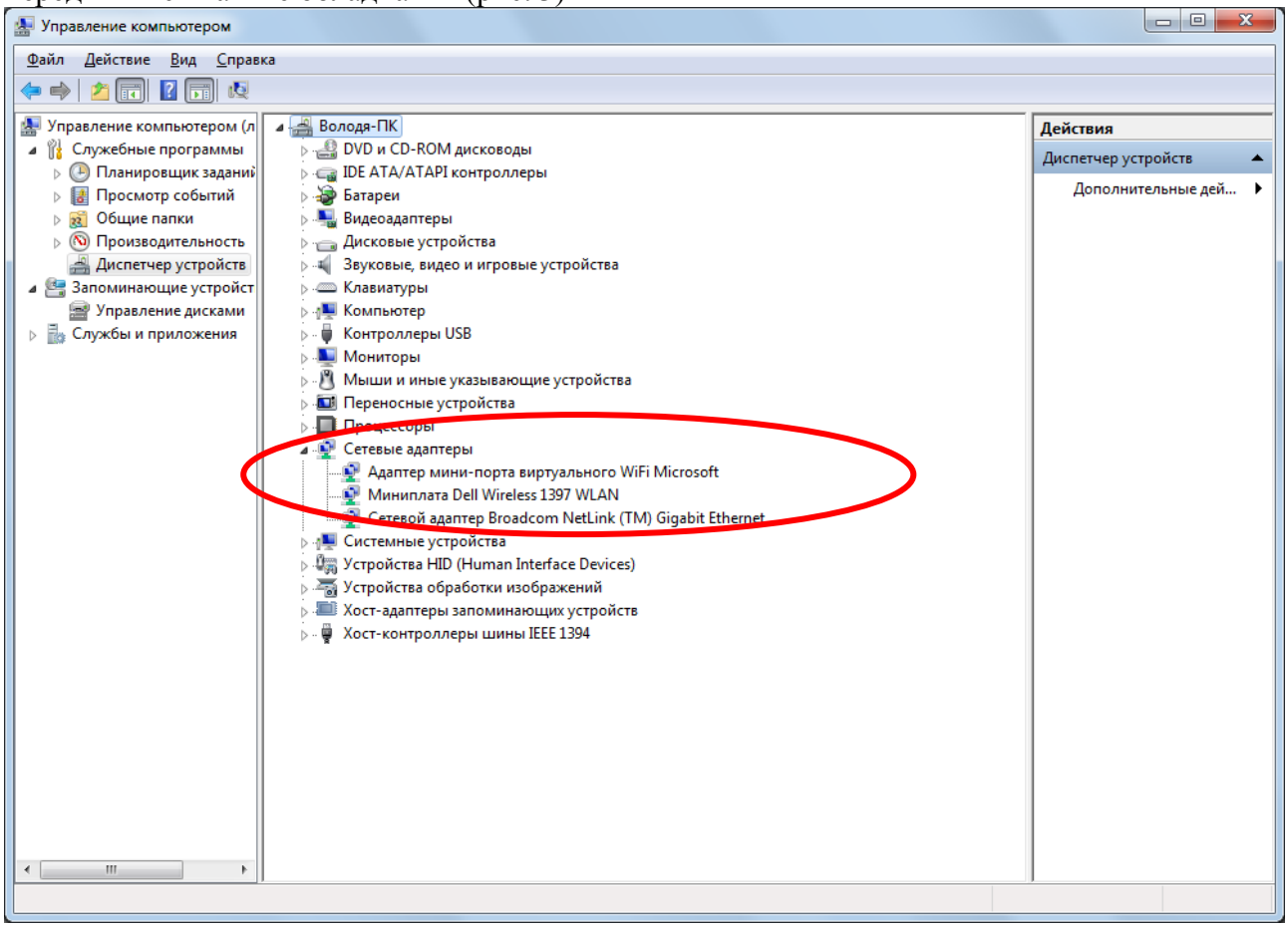
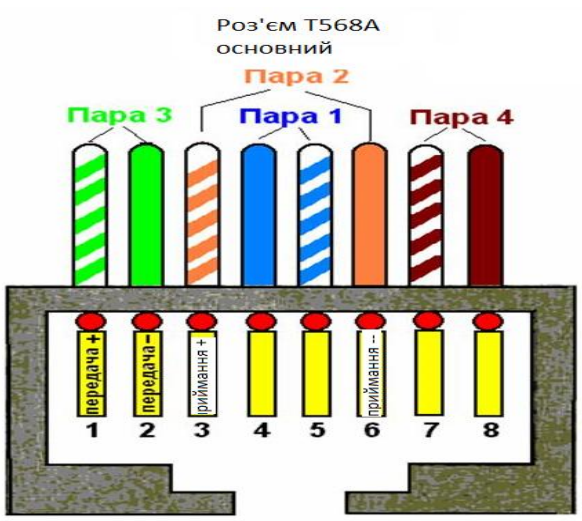


Рис. 3. Вікно **Диспетчер устройств**

Найчастіше в назві мережевого адаптера вказана мережева архітектура, за якою можна визначити швидкість (на малюнку не вказана).

В цьому вікні можна визначити і інше наявне мережеве обладнання.

4. Підготувати пачт-корд із роз'ємом RJ-45 (рис. 4), або кабель (рис. 5).



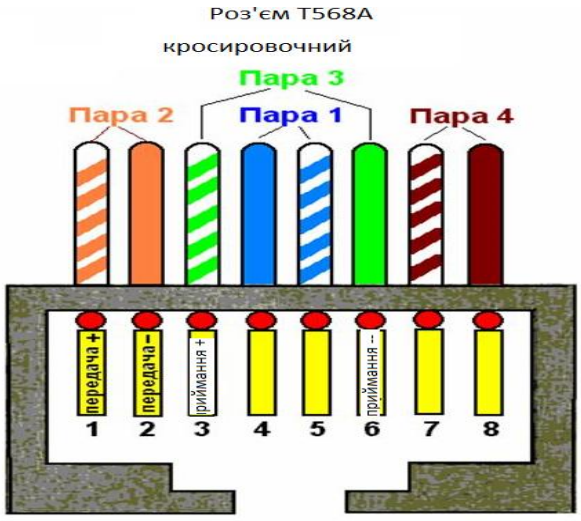


Рис. 4. Роз’єм RJ –45

Рис. 5. Кабель для з’єднання комп’ютерів

5. З'єднати два ПК згідно рис. 6.
6. Налагодити мережеве підключення.
7. Перевірити передачу даних у мережі.

Необхідні пристрої:

1. 1 ПК із ОС Windows7 з мережевим портом Ethernet.
2. 1 ПК із ОС Linux з мережевим портом Ethernet.
3. Кабель UTP 5 категорії, конектори RJ-45, обтискні кліщі й Lan-Тестер або готовий патч-корд.
4. Установлений драйвер мережевого інтерфейсу на кожному ПК.

2.2. Виконання лабораторної роботи

1. Включіть два персональних комп’ютери: комп'ютер А (Win7) і комп'ютер Б (Linux). Перевірте наявність мережевих портів Ethernet і драйверів мережевих інтерфейсів.
2. Потім підготуйте пачт-корд (обіжміть його за схемою Т568А) (рис. 7-10) або візьміть готовий патч-корд і виконаєте його перевірку Lan-Тестером. Перевірку необхідно обов'язково виконати, тому що саме неправильно обтиснутий кабель може стати причиною відсутності з'єднання між пристроями.
3. З'єднайте пачт-кордом обоє мережевих порти комп'ютерів.

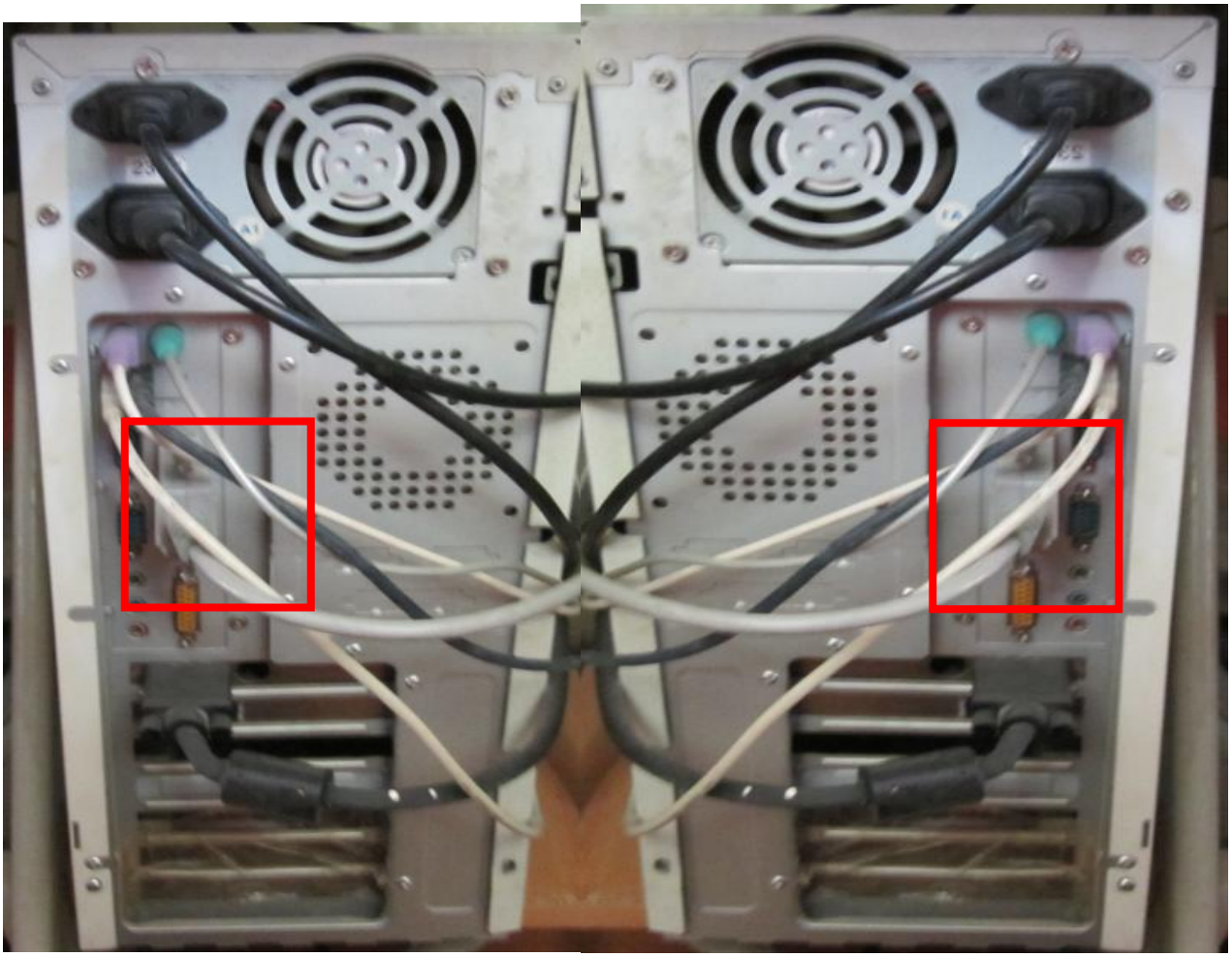


Рис. 6. Комп'ютерна мережа із двох ПК

4. Далі зайдіть на комп'ютері А в **Пуск->Панель управления->Центр управления сетями и общим доступом.** У лівій частині екрана натисніть на посилання **Изменение параметров адаптера** (рис. 11).

Кликніть правою кнопкою миші на вкладку **Сетевое подключение** (у нашім випадку Б). У контекстному меню виберіть **Свойства**. Потім натисніть лівою кнопкою миші на вкладку «**Протокол версии 4(TCP/IPV4).** Поставте галочку на пункт «**Использовать следующий Ір-Адрес**». Задайте **Ір-Адресу:192.168.1.1** і **Маску підмережі: 255.255.255.252.** (рис. 12). Інші поля залиште порожніми й натисніть **ОК**.

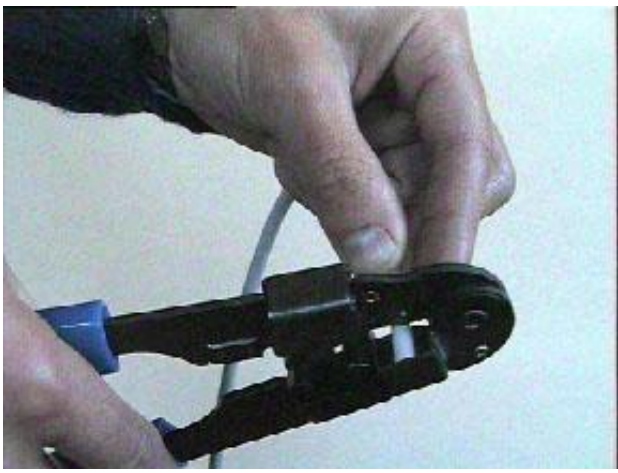


Рис. 7. Зачистка зовнішньої ізоляції

Рис. 8. Видалення зовнішньої ізоляції

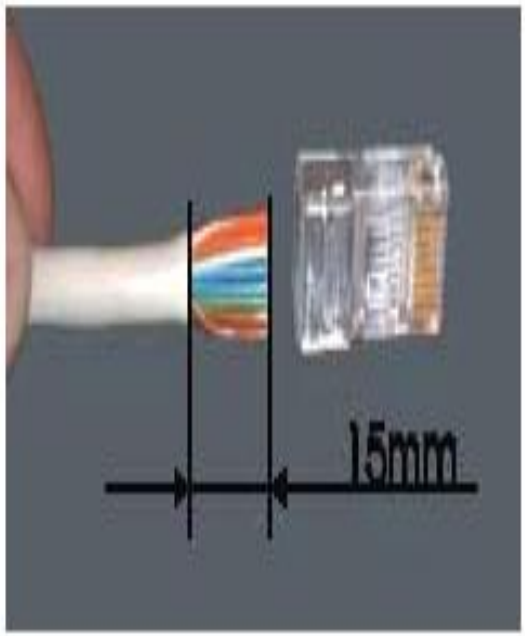


Рис. 9. Монтаж роз’єму

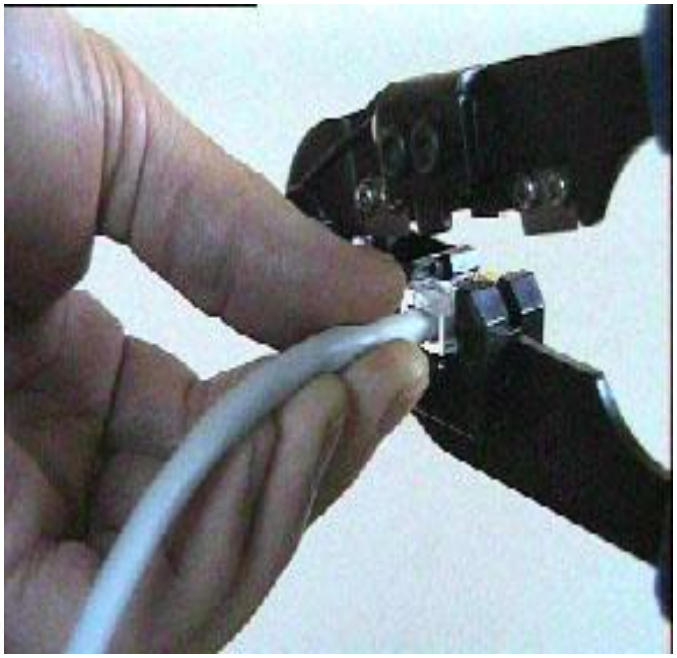


Рис. 10. Процес обжиму

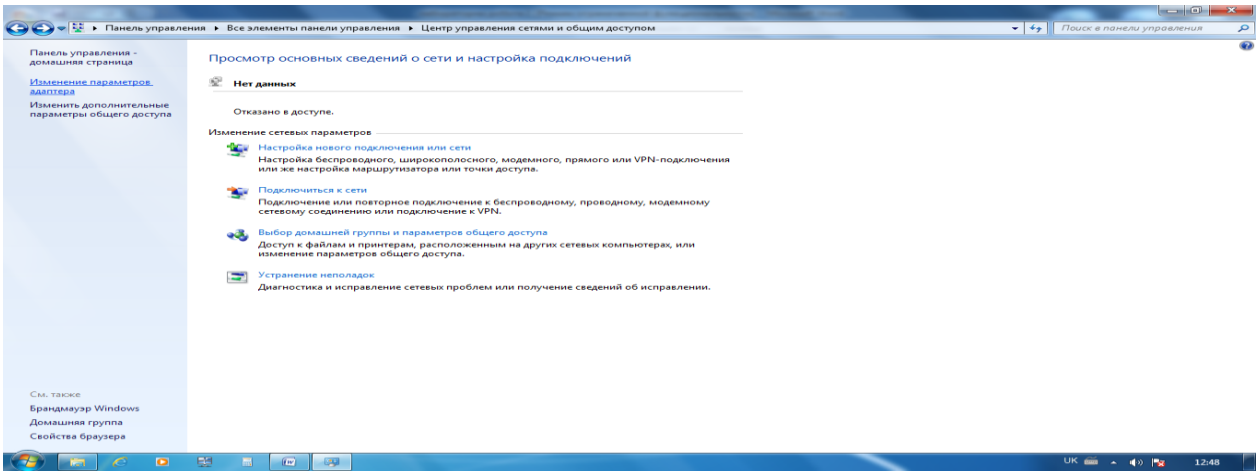


Рис. 11. Параметри адаптера

Пропишіть Ір-Адресу комп'ютеру Б (рис. 13). Натисніть у верхньому правому куті на **значок підключень**, потім натисніть на рядок “**Edit Connections**”. У таблиці, що з'явився, натисніть на “**Add**”. У наступній таблиці задайте тип підключення. У системі Б за замовчуванням налагоджений Ethernet, тому просто натисніть кнопку “**Create**” (рис. 14).

У наступнім вікні натисніть на вкладку **Ipv4 Settings**. У поле **Method** виберіть **Manual**. Далі натисніть на кнопку **Add** і задайте підходящі для нашої мережі налагодження **ip-адреси (192.168.1.3) й маски підмережі (: 255.255.255.252)**. Поле **gateway** залиште порожнім. Натисніть **Save.**

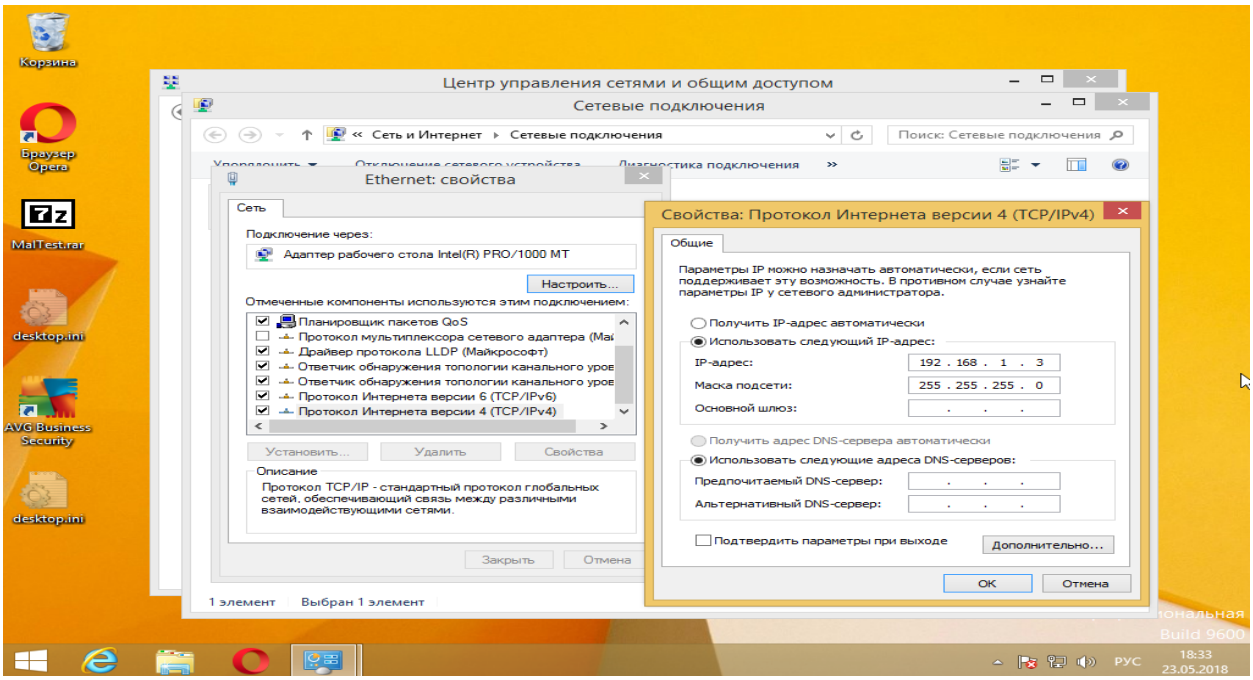


Рис. 12. Налаштування Ip-Адреса на ПК А

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:2a:8a:7c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.155/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2a:8a7c/64 scope link
       valid_lft forever preferred_lft forever
hax0r@poligon:~$ ip addr add 192.168.1.2 dev eth0
RTNETLINK answers: Operation not permitted
hax0r@poligon:~$ sudo ip addr add 192.168.1.2 dev eth0
-bash: sudo: command not found
hax0r@poligon:~$ su
Password:
root@poligon:/home/hax0r# ip addr add 192.168.1.2
Not enough information: "dev" argument is required.
root@poligon:/home/hax0r# ip addr add 192.168.1.2 dev eth0
root@poligon:/home/hax0r# ip link set eth0 up
root@poligon:/home/hax0r# _
```

Рис. 13. Налаштування ПК

1. Перевіряємо з'єднання командою ping. Для цього на комп'ютері А натискаємо комбінацію клавіш Windows +R у вікні, що з'явилося, пишемо cmd, натискаємо Enter. Потім прописуємо команду ping 192.168.1.3 (адреса комп'ютера Б). Почнеться обмін пакетами, якщо все пройде успішно, то відправлених і отриманих пакетів буде по 4 шт. (рис. 15).

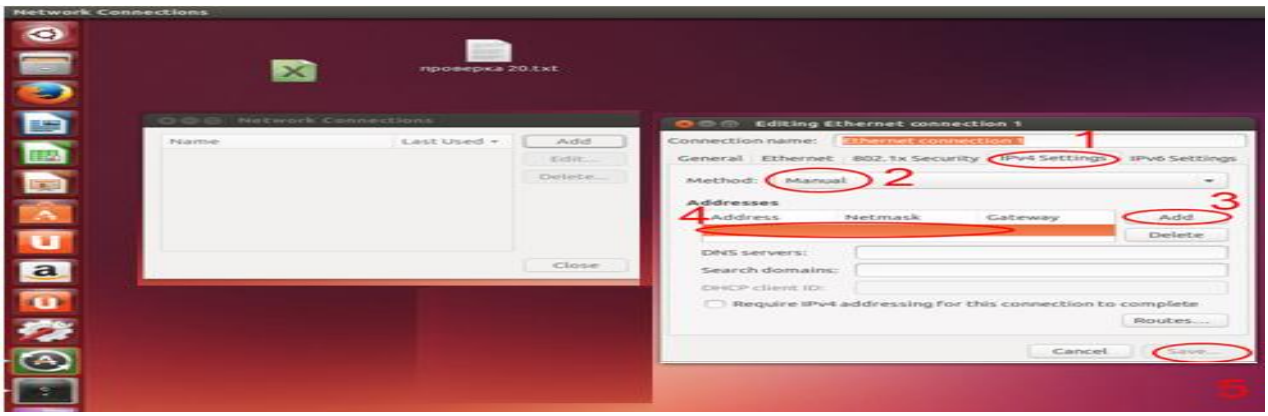


Рис. 14. Налаштування ip-адреси й маски під мережі

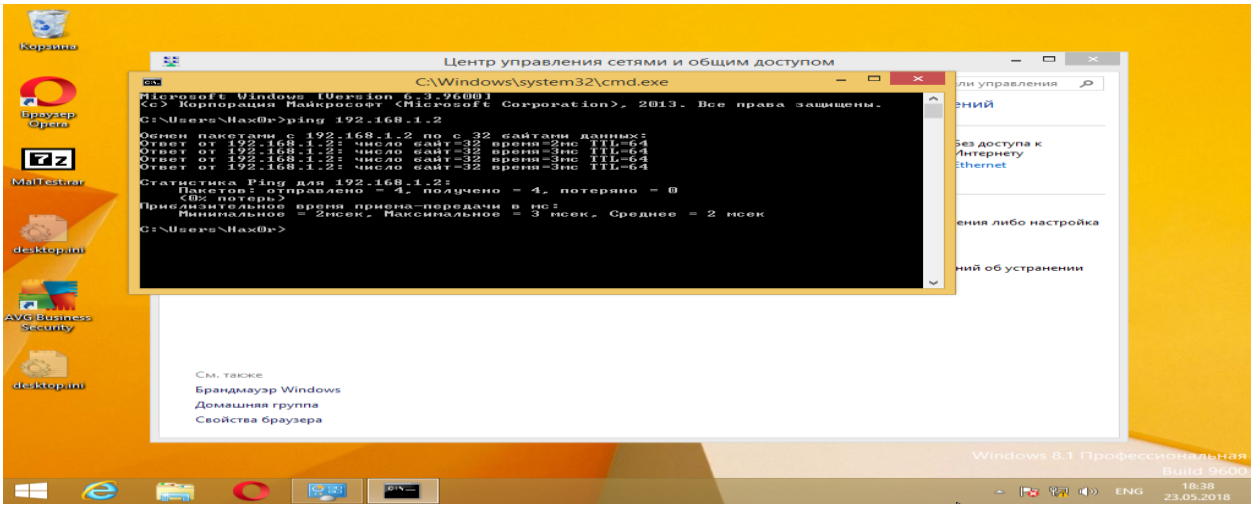


Рис. 15. Перевірка командою ping

2. Перевіряємо з'єднання командою ping. Для цього на комп'ютері А натискаємо комбінацію клавіш **Windows +R** у вікні, що з'явилося, пишемо **cmd**, натискаємо **Enter.** Потім прописуємо команду **ping 192.168.1.3** (адреса комп'ютера Б). Почнеться обмін пакетами, якщо все пройде успішно, то відправлених і отриманих пакетів буде по 4 шт. (рис. 15).

3. Користуючись програмою Total Commander, виміряти час передачі файлів між комп'ютерами (час передачі буде містити в собі час зчитування файлу з диска, час пересилання за лінією зв'язку й час запису файлу на диск). Для вимірів виберіть файл такої довжини, щоб повний час передачі файлу перебував у діапазоні 10-30 секунд. Обчислити ефективну швидкість передачі. Результат представити викладачеві.

3. Контрольні питання

1. Зобразіть модель взаємодії відкритих систем OSI.
2. У чому полягає призначення кожного з рівнів моделі OSI?
3. Аргументовано співвіднесіть апаратне й програмне (використане й розроблене) забезпечення з рівнями моделі OSI.
4. Поясніть сутність асинхронної передачі даних через послідовний порт.
5. Що таке протокол передачі даних?
6. Що таке контроль на парність (непарність)?
7. Що таке швидкість і ефективна швидкість передачі даних?
8. Який порядок організації зв'язку через послідовний порт RS-232?

ЛАБОРАТОРНА РОБОТА 2.
ПОБУДОВА МЕРЕЖІ ЗА ТОПОЛОГІЄЮ «ЗІРКА» НА БАЗІ КОМУТАТОРА

Мета роботи: навчитися будувати мережу на базі комутатора.

Зміст

1. Завдання
2. Необхідне встаткування:
3. Хід роботи
4. Контрольні питання

1. Завдання

5. Підключити чотири ПК до комутатора.
6. Налагодити мережу.
7. Перевірити мережу.

2. Необхідне встаткування

1. Чотири ПК із мережними портами Ethernet з ОС Win7, Winxp, Win8, Ubuntu.
2. Чотири відрізка кабелю UTP 5 категорії (див. додаток 1), конектори RJ-45 або чотири готові патч-корда.
3. Установлені на кожному ПК драйвери мережевого інтерфейсу.

3. Хід роботи

1. Включіть всі чотири комп'ютера: комп'ютер А (Windows 10), комп'ютер Б (Windows XP), комп'ютер В (Windows 8) комп'ютер Г(Linux). Також підключіть комутатор (свитч) у мережу електроживлення. Підберіть чотири готових патч-корди, обтиснутих за стандартом прямого обтиску (Т568В) і виконаєте з'єднання кожного комп'ютерного порту з портом комутатора як показано на рис.1.

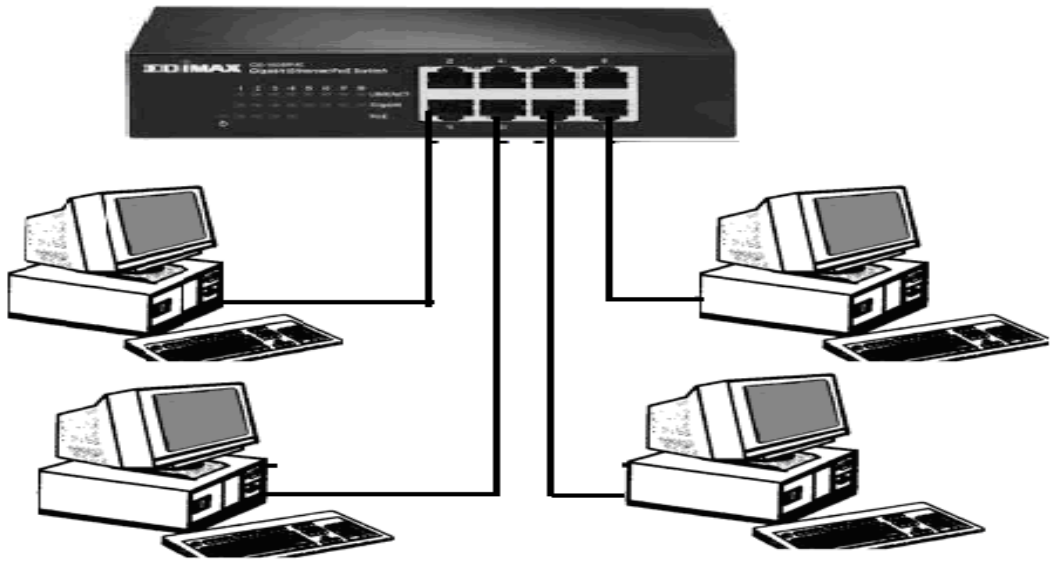


Рис. 1. Підключення ПК до свича

На комутаторі повинні загорітися 4 світлових індикатори. Далі за чергою налагодьте мережеві інтерфейси комп'ютерів. Приступіть до налагодження мережевих інтерфейсів на комп'ютері А. Зайдіть на комп'ютері А в **Пуск Панель управления Центр управления сетями и общим доступом**. У лівій частині екрана натисніть на **Изменение параметров адаптера** (рис.2).

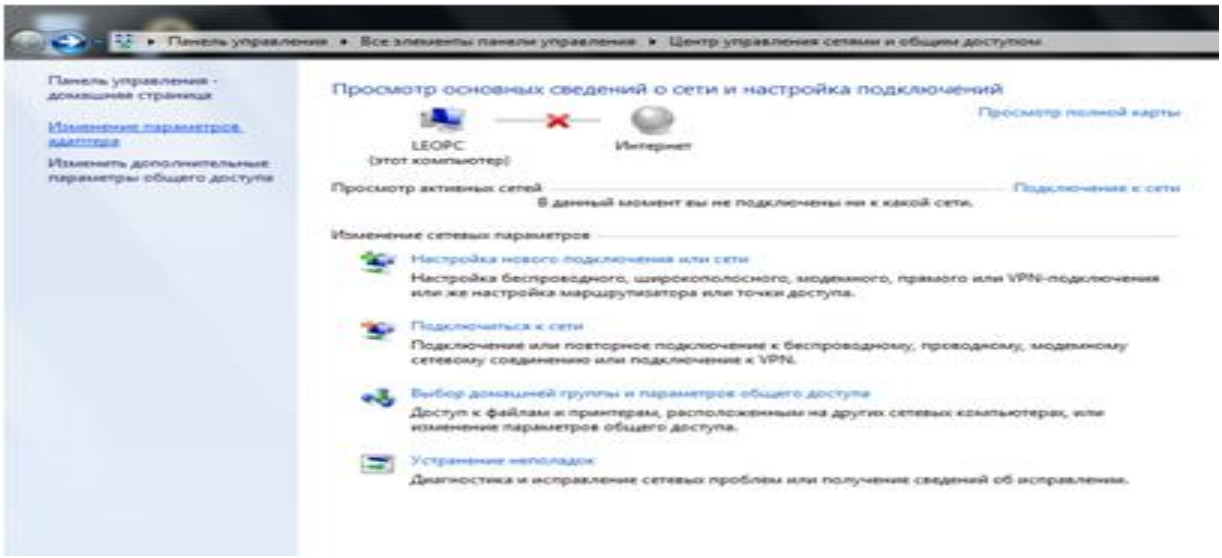


Рис. 2. Налагодження ПК А

Тому що в ПК А встановлено дві мережеві плати (карти), то на екрані відобразитися два мережеві підключення, одне з яких буде підключено. Друге покаже, що мережевий кабель не підключений. Натисніть праву клавішу миші, виберіть пункт **Свойства** й налагодьте з'єднання (рис. 3).

Примітка. Останні октети ip-адреси й маски підмережі встановіть самостійно.

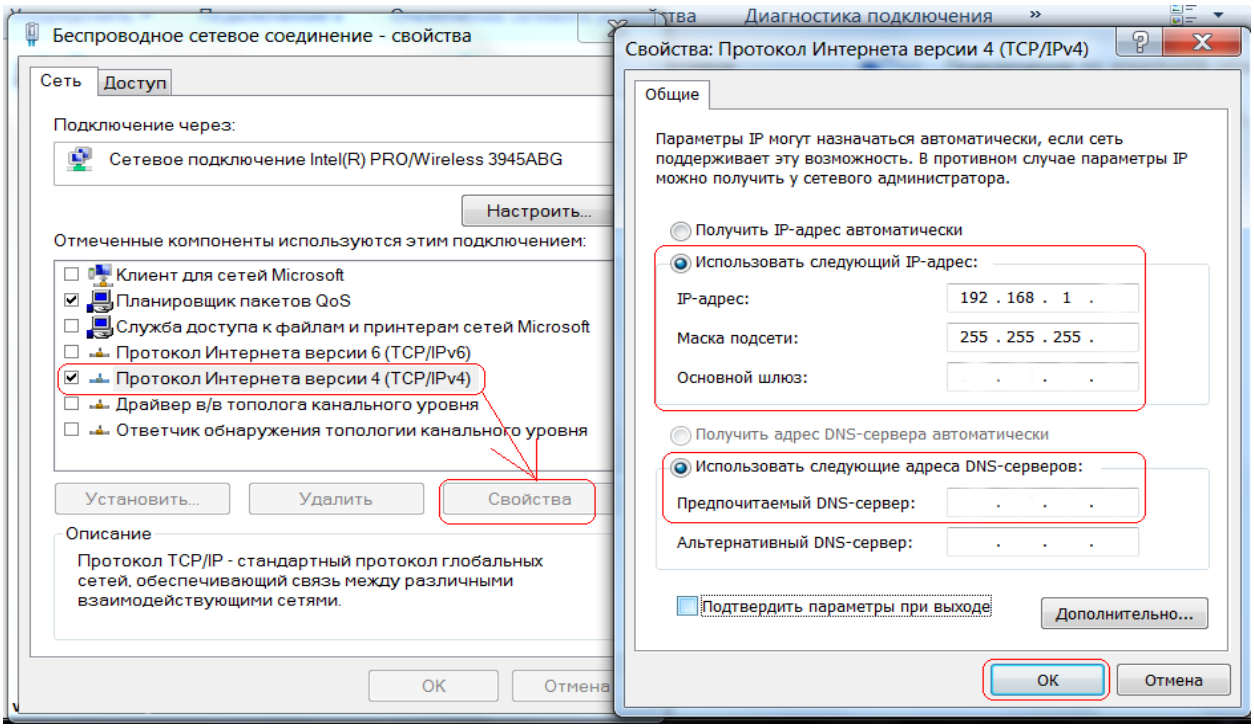


Рис. 3. Налагодження Ip-адреси

2. Перейдіть до налагодження комп'ютера Б: Натисніть правою кнопкою мишки у правому нижньому кутку на панелі задач на ярлик мережевого підключення і виберіть пункт «**Центр управления сетями и общим доступом**» (рис. 4).

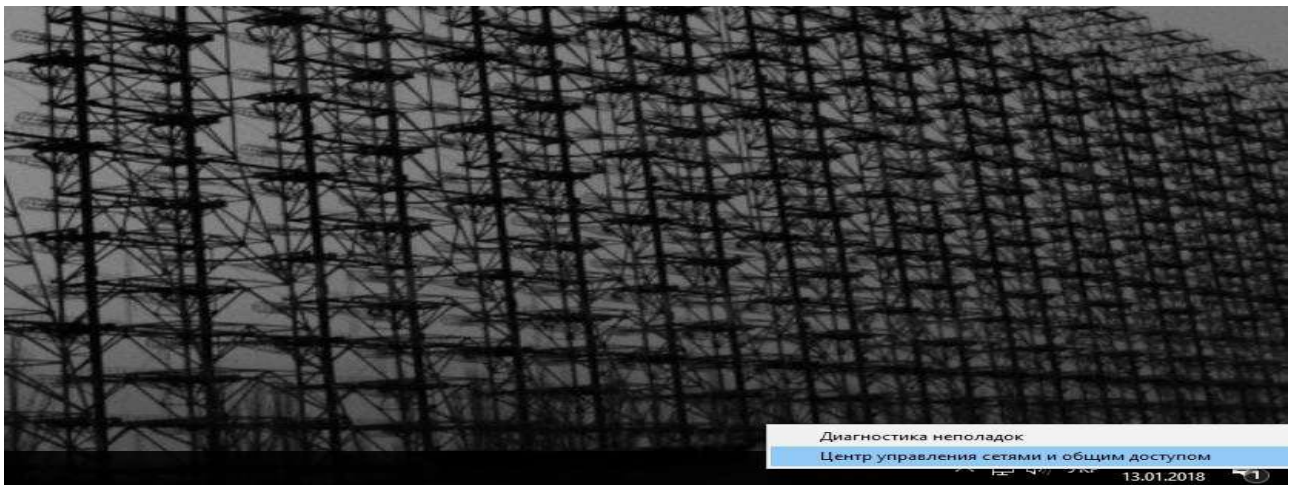


Рис. 4. Налагодження ПК Б

Кликніть правою кнопкою миші по мережевому підключенню (у нашім випадку Windows 10). Далі в контекстному меню виберіть **Свойства**. Далі натисніть лівою кнопкою миші по вкладці **Протокол версии 4(TCP/IPV4)**. Поставте галочку на **Использовать следующий Ip-Адрес**. Задайте Ip-Адресу й маску підмережі як показано (рис. 5).

Примітка. Останні октети ip-адреси й маски підмережі встановіть самостійно.

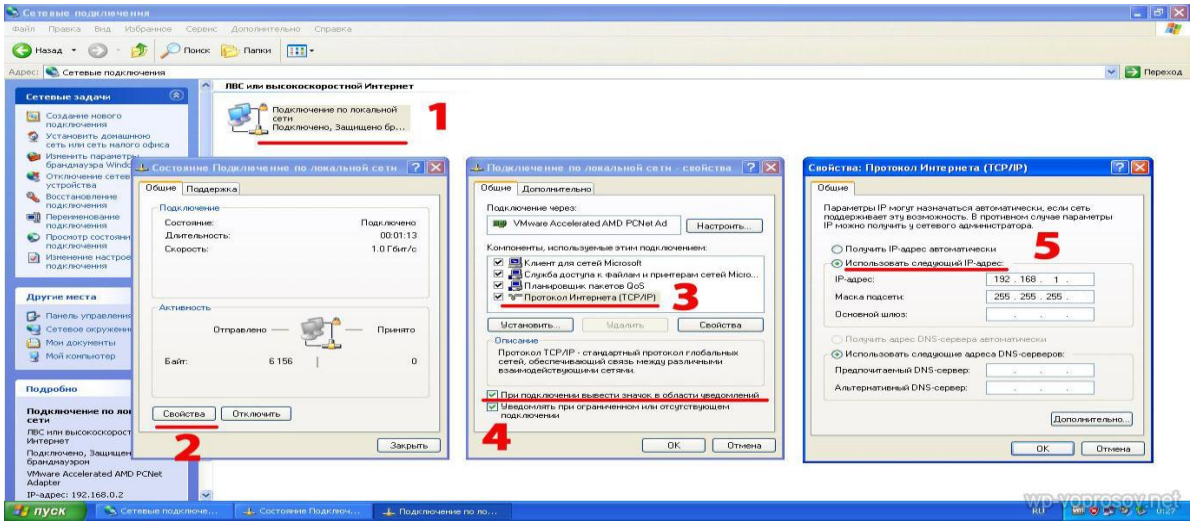


Рис. 5. Налагодження Ip-адреси

Налагодження комп'ютера В. **Натисніть лівою клавішею мишки у верхньому правому куті на значок підключень** потім натисніть на рядок **Edit Connections**. У таблиці, що з'явився, натисніть на **Add**. У наступній таблиці задайте тип підключення. У системі Linux за замовчуванням налагоджений Ethernet, тому просто натискаємо кнопку **Create**.

У наступнім вікні натисніть на вкладку **Ipv4 Settings**. У поле **Method** виберіть **Manual**. Далі натисніть на кнопку **Add** і задайте підходящі для нашої мережі налагодження **Ip-адреси й маски підмережі**. Поле **gateway** залиште порожнім. Натисніть **Save.**

Налагодьте комп'ютер Г. Наведіть курсор у нижній правий кут. У вікні, що з'явилося, виберіть **Параметры.**

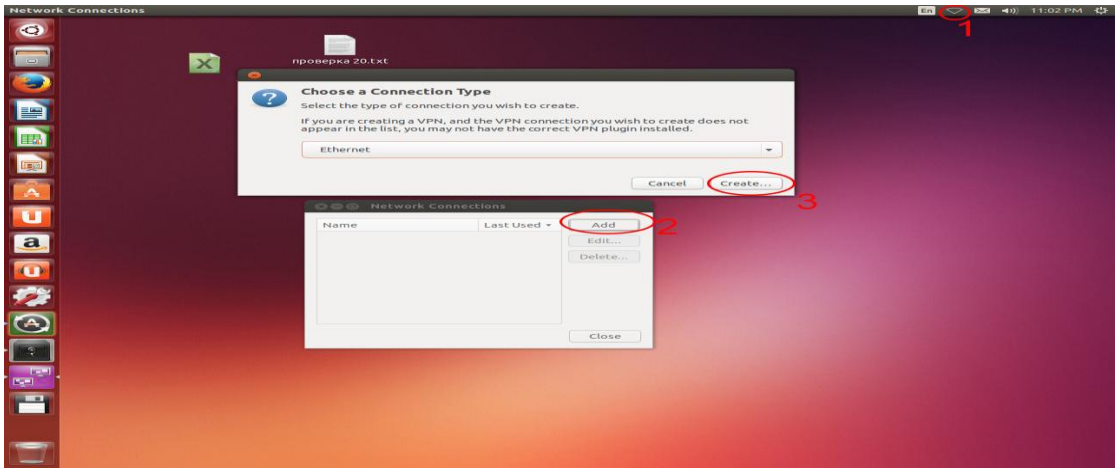


Рис. 6. Налагодження ПК В

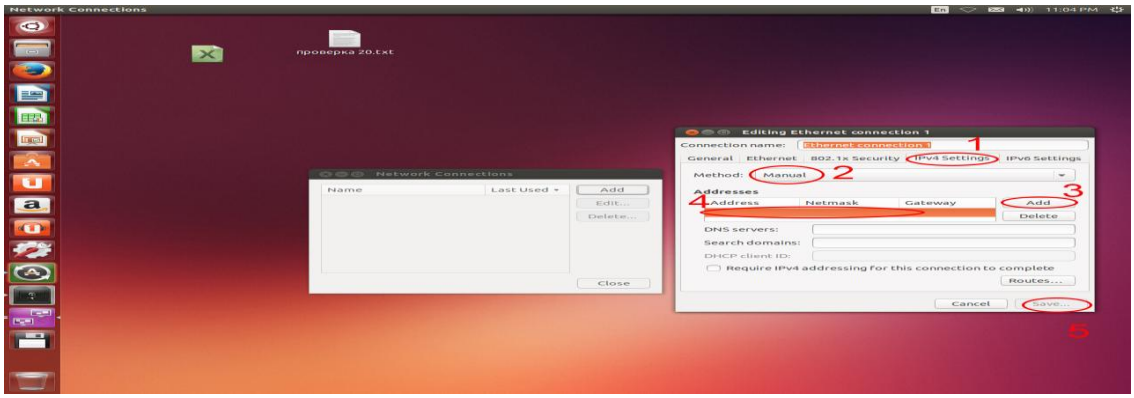


Рис. 7. Налагодження ip-адреси ПК В

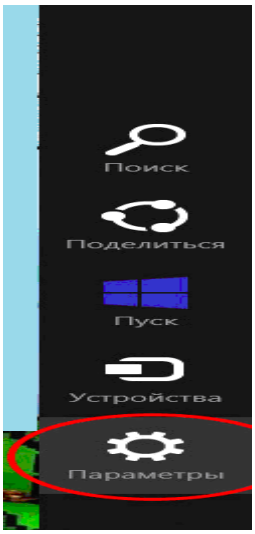


Рис. 8. Налагодження ПК Г

Зайдіть у **Пуск Панель управления Центр управления сетями и общим доступом**. Натисніть на **Изменение параметров**. Далі натисніть правою кнопкою миші на мережеве підключення в нашім випадку **Ethernet**. Натисніть на протокол Інтернету **версії 4(TCP/Ipv4).** Далі поставте галочку на **Исспользовать следующий Ip-Адрес**. Задайте налагодження Ip-адреси й маски підмережі (рис. 9).

Примітка. Останні октети ip-адреси й маски підмережі встановіть самостійно.

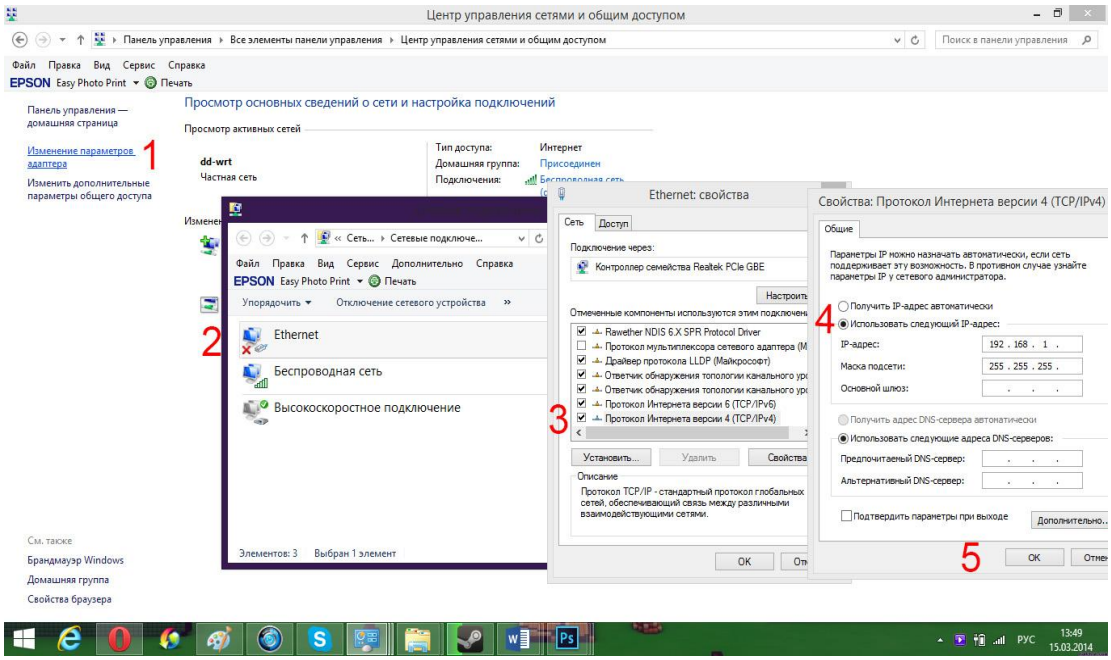


Рис. 9. Налагодження ip-адреси ПК Г

3. Перевірте з'єднання командою **ping**. Для цього на комп'ютері Б натисніть комбінацію клавіш Windows +R у вікні, що з'явилося, напишіть **cmd**, натисніть **Enter**. Потім пропишіть команду **ping 192.168.1.3** (адреса комп'ютера В). Почнеться обмін пакетами, якщо все пройде успішно, то відправлених і отриманих буде по 4 шт. За аналогією перевірте інші чотири адреси.

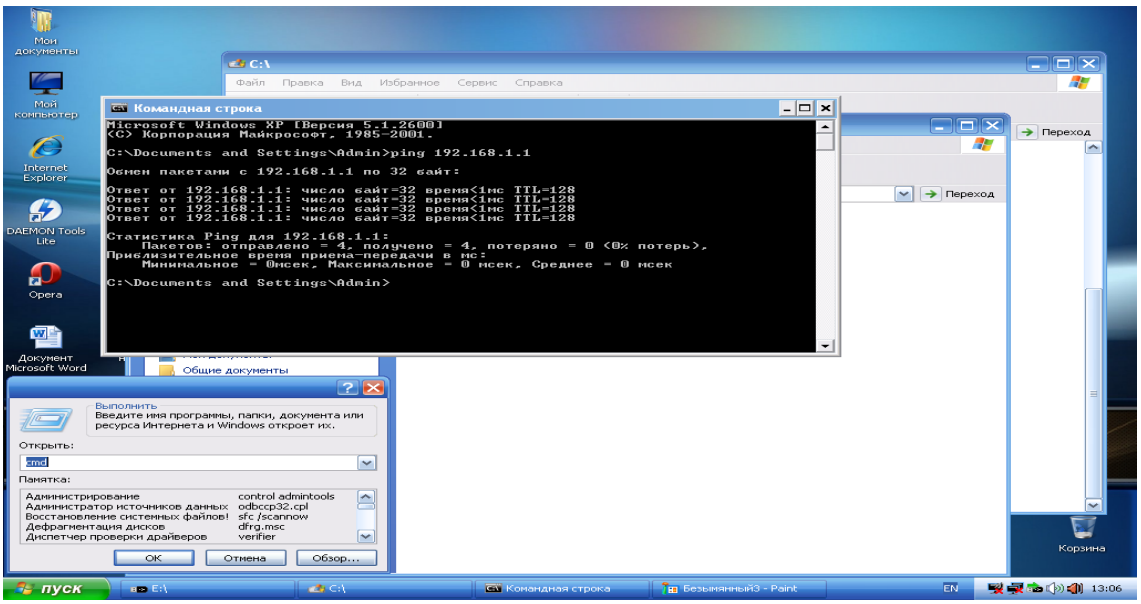


Рис. 10. Перевірка мережі

4. Контрольні питання

1. Як підключаються ПК до комутатора?
2. Як налагодити комп'ютер з операційною системою Windows 7 до роботи в мережі?
3. Як налагодити комп'ютер з операційною системою Windows XP до роботи в мережі?
4. Як налагодити комп'ютер з операційною системою Windows 8 до роботи в мережі?
5. Як налагодити комп'ютер з операційною системою Linux до роботи в мережі?
6. Як перевірити працездатність створеної мережі?

ЛАБОРАТОРНА РОБОТА 3.
ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ FAST ETHERNET

Мета роботи: побудова й налаштування локальної мережі Fastethernet.

Зміст

1. Завдання для роботи
2. Перелік засобів, що забезпечують роботу
3. Теорія
3.1. Технологія Fastethernet
3.2. Монтаж мережевих розеток
3.3. Прокладання локальної мережі Fastethernet
4. Хід роботи
5. Контрольні питання

1. Завдання для роботи

1. Навчитися здійснювати монтаж мережевих розеток.
2. Освоїти методи тестування кабельних ліній зв'язку.
3. Вивчити основи побудови локальної мережі Fastethernet.
4. Навчитися прокладати й набудовувати локальну мережу із шести комп'ютерів, використовуючи комунікаційний центр.

2. Перелік засобів, що забезпечують роботу

1. Мережеві розетки RJ-45.
2. Кабель «кручена пара» категорії 5 і 5E.
3. Кабелі Pathcord.
4. Концентратор Fastethernet.
5. Конектори RJ-45.
6. Кабельний тестер.
7. Шість ПК.

3. Теорія

3.1. Технологія Fastethernet

В 1995 р. був прийнятий стандарт Fastethernet (описаний у стандарті 802.3u), в 1998 р. прийнятий стандарт Gigabitethernet (802.3z). Більшість сучасних мереж будується по 100-мегабітній технології – Fastethernet, а також усе більшу популярність здобуває Gigabitethernet.

Технологія Fastethernet заснована на використанні кабелів типу «кручена пара» і волоконно-оптичного кабелю. Для даної технології характерна організація локальних мереж з топологією фізичних зв'язків «зірка», яка має на увазі підключення ПК до комунікаційного центру.

У якості комунікаційного центру можуть виступати концентратори або комутатори локальних мереж. На логічному рівні застосовується топологія «шина»: усі пристрої, підключені до мережі, рівноправні, тобто будь-яка станція може почати передачу даних у будь-який момент часу (якщо передавальне середовище вільне).

Цей метод доступу до середовища передачі даних називається CSMA/CD (Carrier Sense Multiple Access і Collision Detection).

Мережі стандарту Ethernet діляться на технологічні класи. Дані класи різняться, насамперед, пропускною здатністю, типом використовуваного кабелю, топологією й деякими характеристиками. Кожний з класів має власне позначення, що відбиває його технічні характеристики. Таке позначення має вигляд: Xbase/Broady, де X – пропускна здатність мережі, «Base» або «Broad» говорять про метод передачі сигналу.

«Base» – метод передачі на одній базовій частоті (baseband – основополосний), «Broad» – метод, що використовує кілька несучих частот (broadband – широкосмуговий). Число Y відображає максимальну довжину сегмента в сотнях метрів, або позначає тип

використовуваного кабелю (буква «Т» означає використання кабелю «кручена пара» (twistedpair), «F» – використання оптоволокна (Fiberoptic)).

Було створено кілька модифікацій стандарту Fastethernet: 100BaseTX, 100BaseT4, 100Basefx.

Технологія 100BaseTX має на увазі використання стандартної «кручений пари» 5 категорії або 5Е, у якій задіяно тільки чотири провідники з восьми наявних: два – для приймання даних, і два – для передачі.

Максимально припустима відстань між вузлами мережі 100BaseTX становить 100 м.

У мережах 100BaseT4 також використовується «кручена пара», однак у ній задіяні всі вісім жил провідника: одна пара працює тільки на приймання даних, одна – тільки на передачу, а, що залишилися дві забезпечують двонаправленний обмін інформацією. Оскільки технологія 100BaseT4 має на увазі поділ усіх трансльованих за мережею даних на три незалежних логічних канали (приймання, передача, приймання-передача), пропорційно зменшується частота сигналу, що дозволяє прокладати такі мережі з використанням менш якісного й, отже, більш дешевого кабелю 3 або 4 категорії.

Стандарт 100Basefx призначений для роботи з оптоволоконними лініями зв'язку, тут використовуються два волокна – на приймання й на передачу.

Для побудови мережі Fastethernet використовуються спеціальні мережеві розетки, комутатори або концентратори Fastethernet, мережеві адаптери Fastethernet мережевий кабель, конектори.

3.2. Монтаж мережевих розеток

Мережеві розетки Fastethernet під «кручену пару» являють собою пластмасовий короб зі знімною кришкою, у верхній частині якого змонтована відповідна частина роз’ємів RJ-45, оснащена вісьма підпружиненими контактами, а також є те або інше пристосування для підключення провідників мережевого кабелю.

Звичайно розетка має або спеціальний шар, що клеїть, або отвори під гвинти для кріплення до стіни.

Якщо розгорнути розетку рознімання до себе таким чином, щоб контакти виявилися внизу, то номери контактів відраховуються з 1 по 8 зправа наліво.

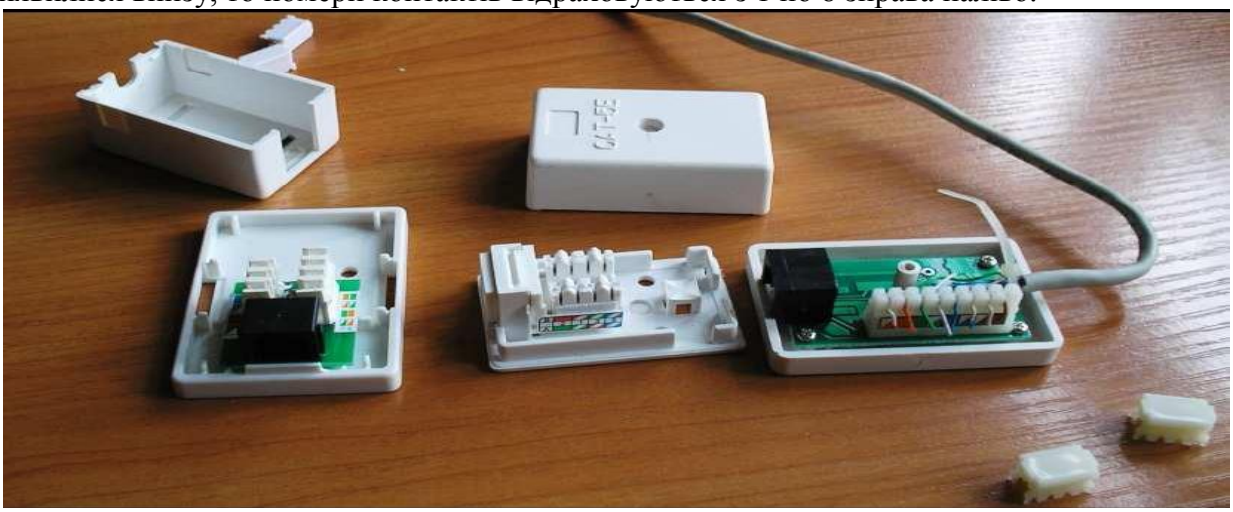


Рис. 1. Розетки RJ-45

Мережеві розетки різняться за категоріями, найбільше розповсюдженими з яких сьогодні є категорія 5 і 5Е (рис. 1). В сучасних розетках провідники крученому пари вставляються в щілині спеціальних контактних майданчиків, розташованих під кутом в 90° до площини роз’ємів RJ-45. При цьому видалення захисного шару із провідників не потрібно: щілини оснащені спеціальною ріжучою кромкою, яка сама прекрасно знімає з них ізоляцію.

Для надійної фіксації провідників у контактах розетки використовується спеціальний інструмент (рис. 2), що дозволяє помістити проводи на максимальну глибину (рис. 3). Усі контакти в розетках категорії 5, як правило, пронумеровані й постачені колірним маркуванням, тому ніяких проблем з розведенням кабелю виникнути не повинне.

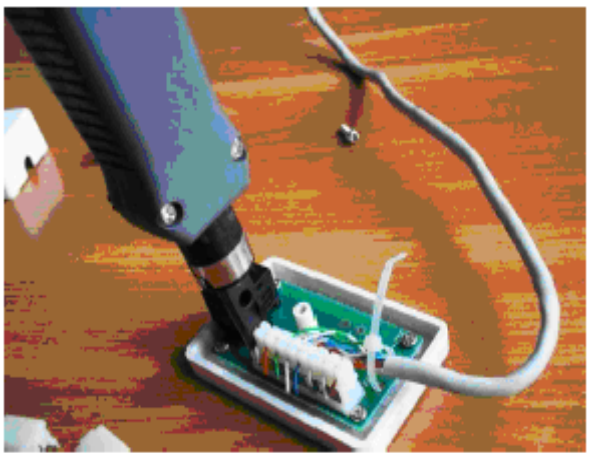


Рис. 2. Інструмент для монтажу розетки RJ-45 Рис. 3 Монтаж розетки RJ-45

3.3. Прокладання локальної мережі Fastethernet

Перш ніж приступитися до роботи з побудови локальної мережі, потрібно підготувати необхідний набір компонентів: мережевий кабель, патч-корди, мережеві розетки RJ-45, комунікаційний центр.

Для організації мережі за стандартом 100BaseTX комунікаційним центром може бути концентратор або комутатор Fastethernet.

Мережеві розетки монтуються на стіну в безпосередній близькості від комп'ютера, що підключається до локальної мережі. Кожна розетка з'єднується з роз'ємом RJ-45, розташованим на мережному адаптері ПК, за допомогою кабелю Pathcord. Довжина цього кабелю не повинна перевищувати 5м. Від кожної мережевої розетки відходить ще один відрізок кабелю «кручена пари», з однієї сторони змонтований безпосередньо в розетці, з іншого боку – оснащений роз'ємом RJ-45. Довжина кожного відрізка такого кабелю не може перевищувати 90 м. Кінцеві роз'єми всіх відрізків, що йдуть від мережевих розеток, кабелю приєднуються до комбінованої багатопортової мережевої розетки Pathpanel, або безпосередньо до комунікаційного центру.

Pathpanel застосовується, тільки виходячи зі зручності адміністрування локальної мережі. Кожне із гнізд Pathpanel можна промаркірувати, якщо концентратор розташований на значній віддалі від робочих місць (часом буває важко визначити, який із проводів веде до потрібного комп'ютера).

По-друге, використовуючи Pathpanel, можна легко перемістити кожен з проводів, швидко підключивши його у такий спосіб до іншого порту концентратора.

4. Хід роботи

За допомогою отриманих кабельних ліній зв'язку й комунікаційного центру об'єднати комп'ютери в мережу. У якості комунікаційного центру пропонується використовувати концентратор Fastethernet.

Після підключення комп'ютерів до концентратора включити живлення й налагодити роботу локальної мережі.

Щоб налагодити мережу, необхідно виконати наступні дії:

1) Задати мережеве ім'я комп'ютера для ідентифікації його в мережі, а також указати назву робочої групи. Для цього потрібно клацнути правою кнопкою миші на значку **Мой компьютер**, розташованому на робочому столі Windows, вибрати в меню, що з'явився, пункт **Свойства** й перейти к вкладки **Имя компьютера** та ввести мережеве ім'я комп'ютера, вибрати режим робочої групи й вибрати її назву (рис. 4);

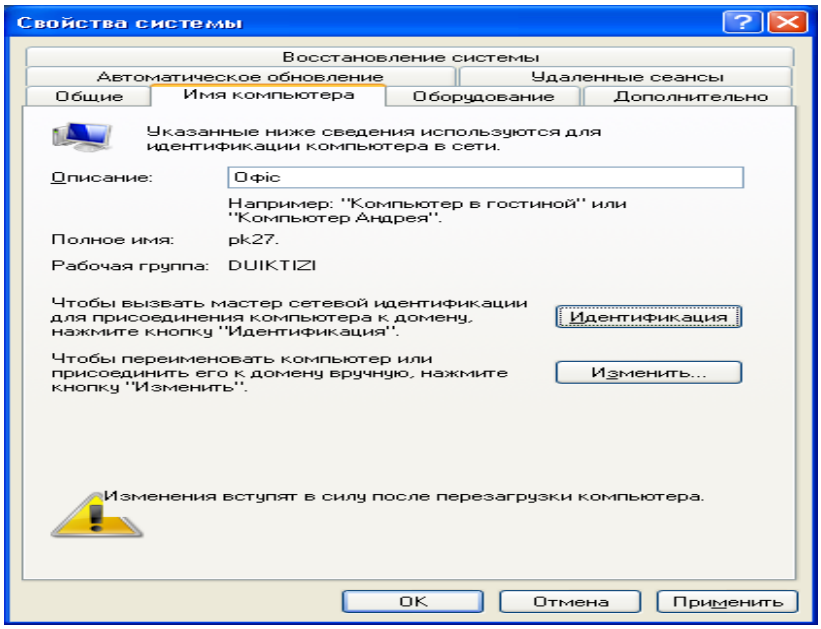


Рис. 4. Вкладка **Имя компьютера**

2) Налагодити комп'ютер для роботи в локальній мережі. Для цього (рис. 4) і натиснути кнопку **Идентификация.** На екрані з'явиться вікно майстра мережевої ідентифікації (рис. 5), слід натиснути на кнопку **Далее;**

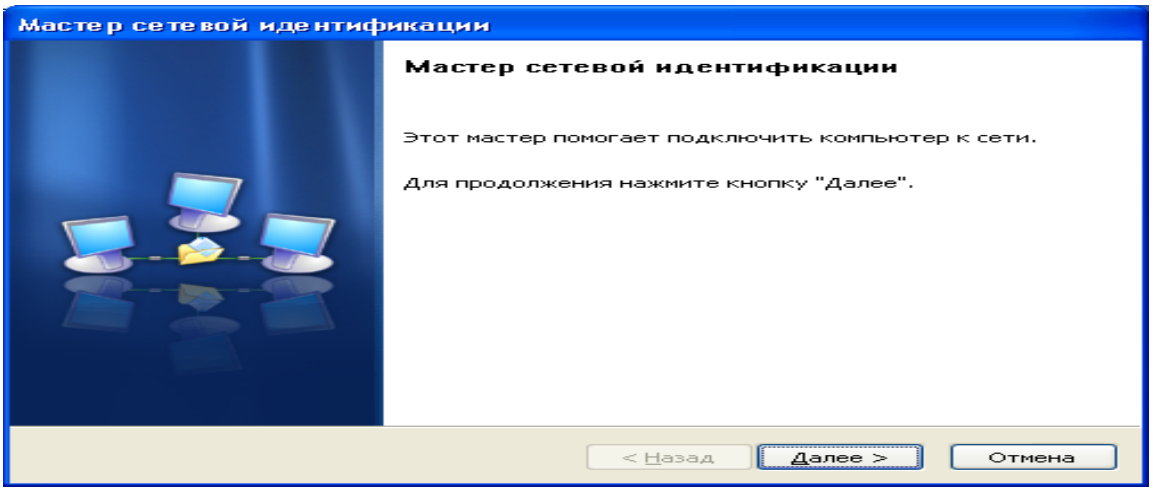


Рис. 5. Вікно майстра ідентифікації

3) У наступнім вікні буде запропоновано вибрати варіант підключення до локальної мережі: якщо комп'ютер є частиною великої корпоративної мережі й потрібно встановити з'єднання з іншими мережними комп'ютерами, то вибрати режим **Компьютер входит у корпоративную сеть и во время работы я использую его для соединения с другими комп'ютерами** (рис. 6). Якщо комп'ютер підключений до невеликої домашньої мережі, установити перемикач в положення **Компьютер предназначен для домашнього исспользования и не входит в корпоративную сеть;**

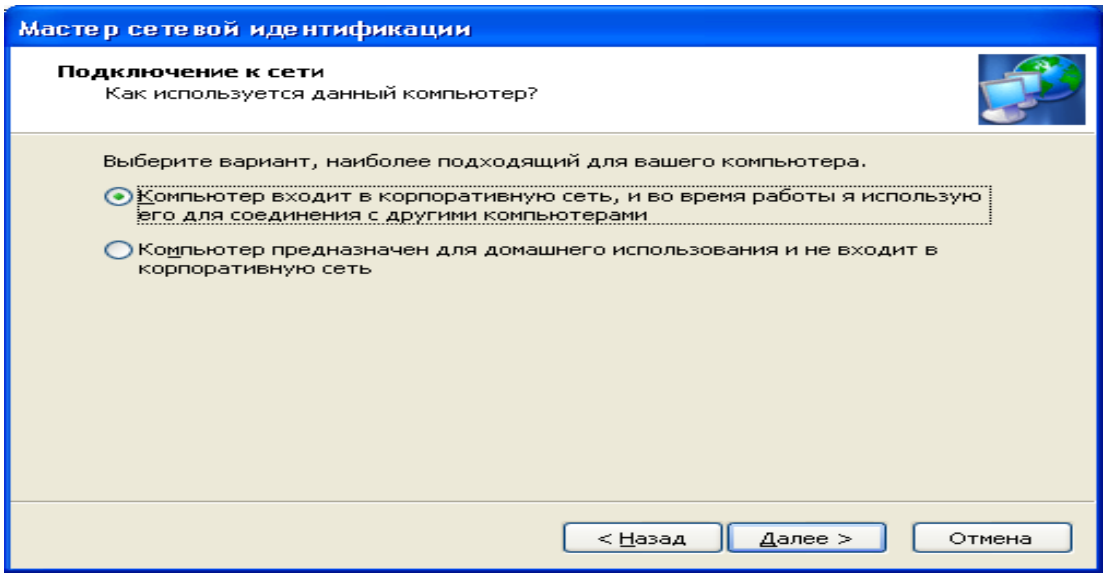


Рис. 6. Відбір параметрів мережі

4) У випадку підключення до домашньої мережі конфігурація комп'ютера на цьому буде закінчена: залишиться тільки натиснути на кнопку **Готово.**

При підключенні до корпоративної мережі буде потрібно вказати метод входу в мережу: якщо в ній використовується домен, установіть перемикач в режим **Моя организация исспользует сеть с доменамы** (рис. 7), а якщо потрібно підключитися до робочої групи, потрібно вибрати режим **Моя организация исспользует сеть без доменов.**

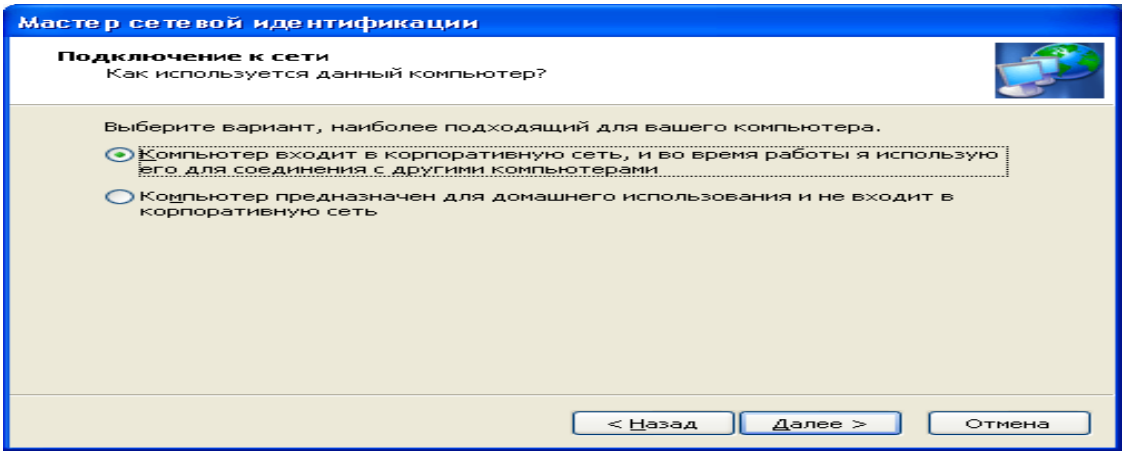


Рис. 7. Відбір параметрів мережі

У наступнім вікні потрібно ввести назву робочої групи (рис. 8, 9), в яку входить комп'ютер, і клацнути на кнопку **Готово (**рис. 9).

Потрібно перезавантажити комп'ютер, щоб усі зміни, внесені в налаштування мережі, набули чинності.

При налагодженні локальної мережі в Microsoft Windows XP можна використовувати майстра налаштування мережі. При використанні майстра налаштування мережі Windows XP автоматично протестує конфігурацію локальної мережі й налагодить мережеве підключення на комп'ютері.

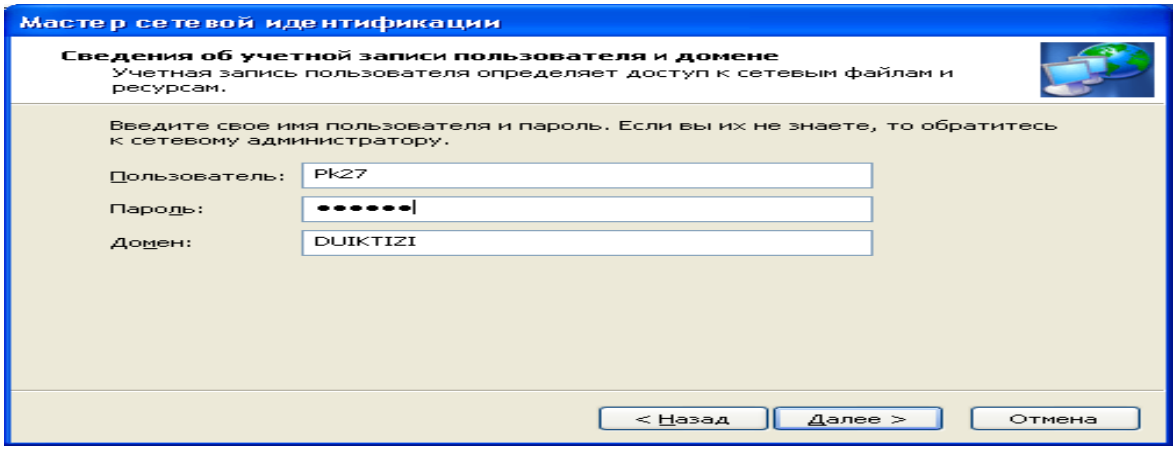


Рис. 8. Відбір параметрів мережі

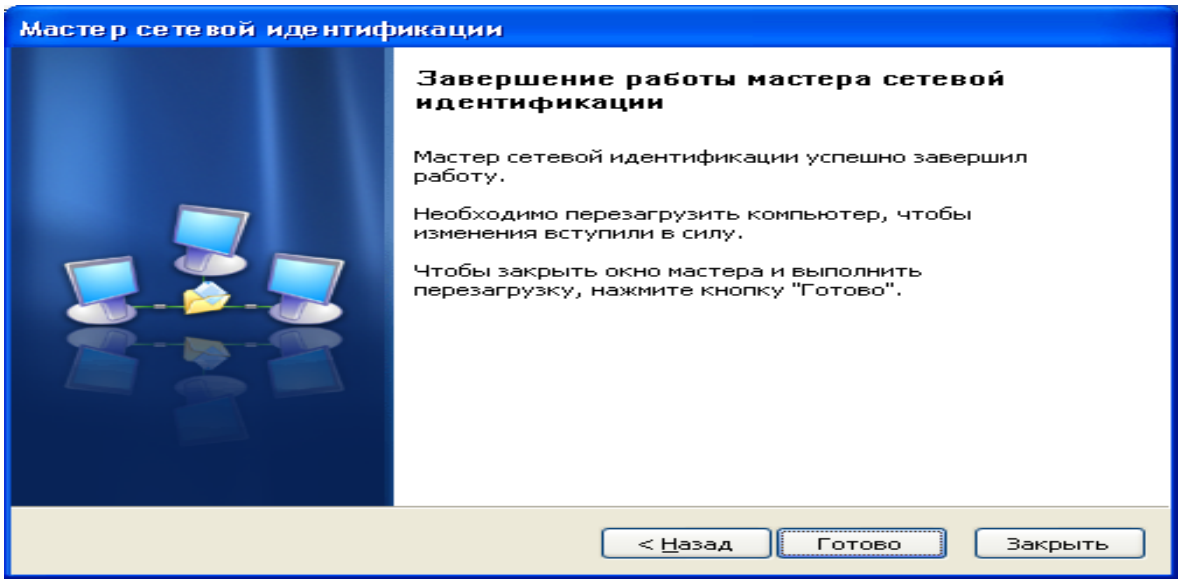


Рис. 9. Заключне вікно майстра

5. Контрольні питання

1. На які класи ділиться технологія Fastethernet?
2. Які фізичні й логічні топології використовуються в мережах Fastethernet?
3. Розетки якої категорії використовуються в сучасних мережах?
4. Які комунікаційні пристрої можна використовувати в мережах класу 100BaseTX?
5. Яким чином можна здійснити з'єднання комп'ютерів?
6. Яке встаткування необхідне для створення локальної мережі із декількох комп'ютерів?
7. Як налагодити локальну мережу?
8. Яка максимальна довжина сегмента на «крученому парі» рекомендована за стандартом Fastethernet?
10. Який пристрій використовується для подовження сегмента мережі?

ЛАБОРАТОРНА РОБОТА 4.
НАЛАШТУВАННЯ МЕРЕЖІ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS 7

Мета роботи: навчитись налаштовувати локальну мережу за допомогою операційної системи Windows 7

Зміст

1. Теорія
1.1. Відкриття компонента «Центр управління мережами і загальним доступом»
1.2. Поняття мережевого розташування
1.3. Карта мережі
1.4. Мережеві підключення
1.5. Підключення до мережі для Windows 7
2. Хід роботи
3. Контрольні питання

1. Теорія

Перегляд доступних безпроводових мереж і підключення до них

На ноутбуці можна бачити список доступних безпроводових мереж, до кожної з яких можна підключитися незалежно від місця розташування. Безпроводові мережі доступні тільки в тому випадку, якщо комп'ютер обладнаний адаптером безпроводової мережі.

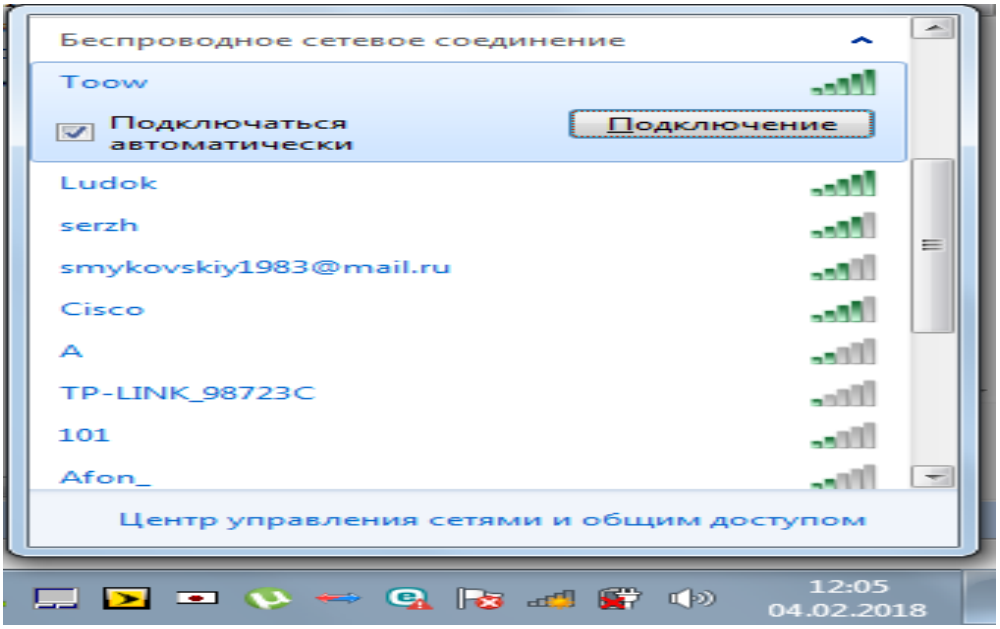


Рис. 1. Список доступнихих мереж

У списку доступних безпроводових мереж клацніть мережа, а потім натисніть кнопку **Подключение** (рис. 1).

У деяких мережах потрібен ключ безпеки мережі або парольна фраза. Для підключення до такої мережі необхідно спочатку звернутися за ключем безпеки або парольною фразою до адміністратора мережі або постачальника послуг.

Попередження:

При підключенні до небезпечної мережі майте на увазі, що всі дії, включаючи відвідування веб-сайтів, роботу з документами, а також паролі й імена облікових записів можуть проглядатися особами, що володіють необхідним інструментарієм. Зміна типу розташування мережі на «Публічна» може мінімізувати ризик несанкціонованого доступу.

На жаль, багато користувачів зазвичай намагаються налаштувати локальну мережу, не маючи навичок роботи з мережевими технологіями, і тому проводять налагодження навмання, через що у них виникає безліч проблем при подальшій роботі.

У вікні **Мой компьютер Свойства** можна визначити також повну назву комп'ютера. В ньому ж вікні вказана назва робочої групи, до якої належить комп'ютер (рис. 2).

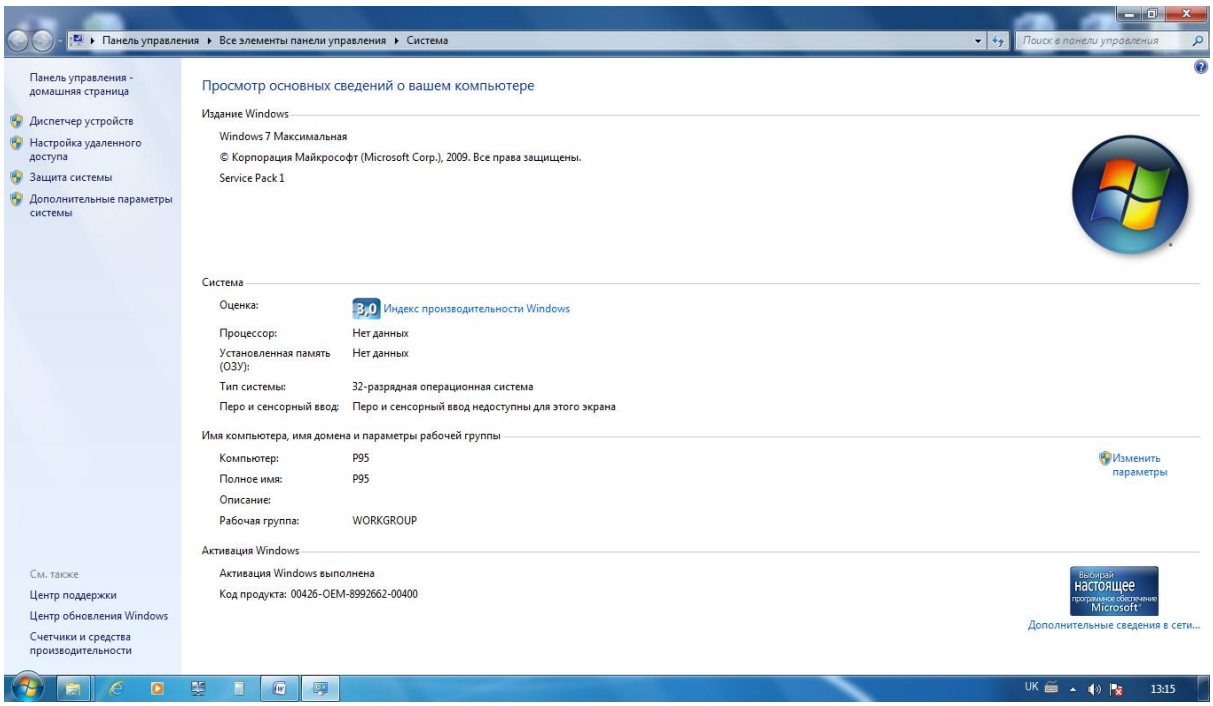


Рис. 2. Властивості комп’ютера

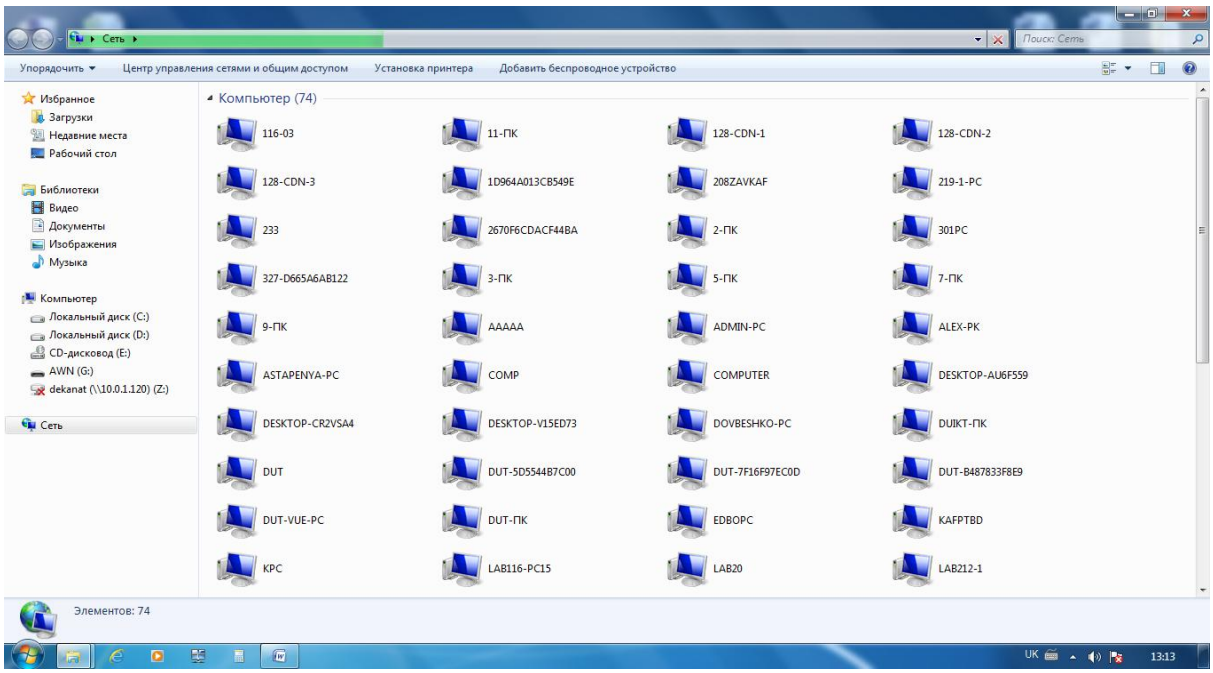


Рис. 3. Робоча група комп’ютерів

Для того, щоб визначити склад комп'ютерів в одній робочій групі та звернутися до них, потрібно зайти в **Сетевое окружение** та знайти свою робочу групу (рис. 2).

У вікні робочої групи відображаються комп'ютери, що ввімкнуті на даний час.

Звернутися до комп'ютера можна також коротшим шляхом: в рядку адреси стандартного вікна слід набрати: // ім'я комп'ютера.

Найчастіше, налагодження локальної мережі в операційних системах Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2012 починається з такої області конфігурування мережевих властивостей, як компонент «Центр управління мережами і загальним доступом». За допомогою даного засобу конфігурації мереж можна вибирати мережеве розміщення, переглядати карту мережі, налаштовувати мережеве виявлення, загальний доступ до файлів і принтерів, а також налаштовувати і переглядати стан ваших поточних мережевих підключень.

1.1. Відкриття компонента «Центр управління мережами і загальним доступом»

Для того щоб скористатися функціоналом засобу конфігурування мереж, потрібно для початку його відкрити. Щоб відкрити вікно «Центр управління мережами і загальним доступом», виконайте одну з таких дій:

1. В області робочого столу натисніть правою кнопкою миші на значку **Сеть** і з контекстного меню виберіть **Свойства** (рис. 4) з'явиться вікно Центру управління мережами та налаштування доступу (рис. 5).
2. Натисніть на кнопку **Пуск** для відкриття меню, в поле пошуку введіть **Центр управления сетями и общим доступом** У лівій частині екрана натисніть на посилання **Изменение параметров адаптера** (рис. 6) і в знайдених результатах відкрийте додаток **Центр управления сетями и общим доступом клацнувши двічі лівою клавішею миші по назві** (рис. 7).

1.2. Поняття мережевого розташування

Перед початком роботи з даним компонентом, слід розібратися з таким поняттям як мережеве розташування. Цей параметр задається для комп'ютерів при першому підключенні до мережі і під час підключення автоматично налаштовується брандмауер і параметри безпеки для того типу мережі, до якого здійснюється підключення. На відміну від операційної системи Windows Vista, де для всіх мережевих підключень використовується найсуворіший профіль брандмауера для мережевого розміщення, операційна система Windows 7 підтримує кілька активних профілів, що дозволяє найбільш безпечно використовувати кілька мережевих адаптерів, підключених до різних мереж. Існує чотири типи мережевого розташування:

Домашня мережа. Дане мережеве розташування призначено для використання комп'ютера в домашніх умовах або в таких мережах, де користувачі дуже добре знають один одного. Такі комп'ютери можуть приєднуватися до домашніх груп. Для домашніх мереж автоматично включається виявлення мережі.

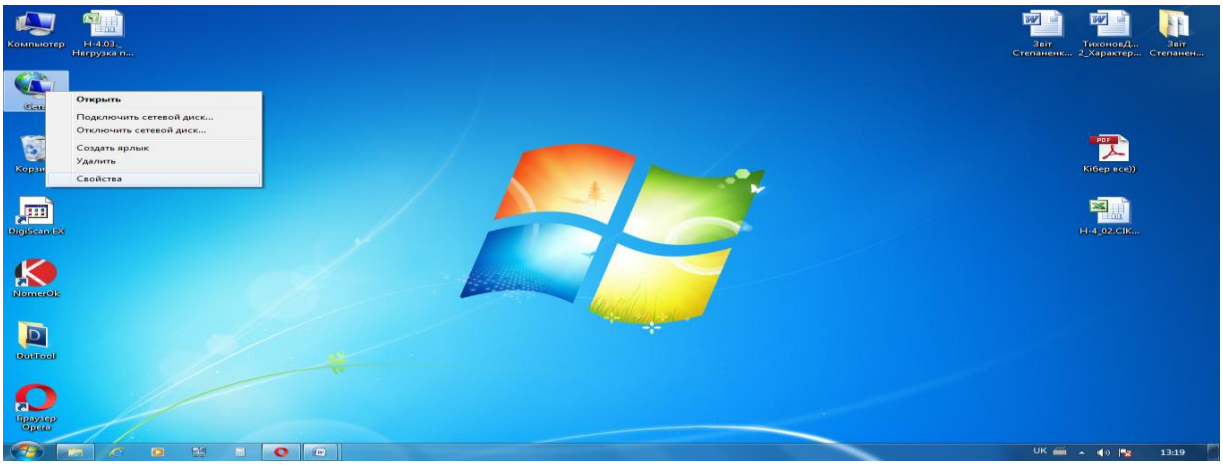


Рис. 4. Відбір властивостей мережі

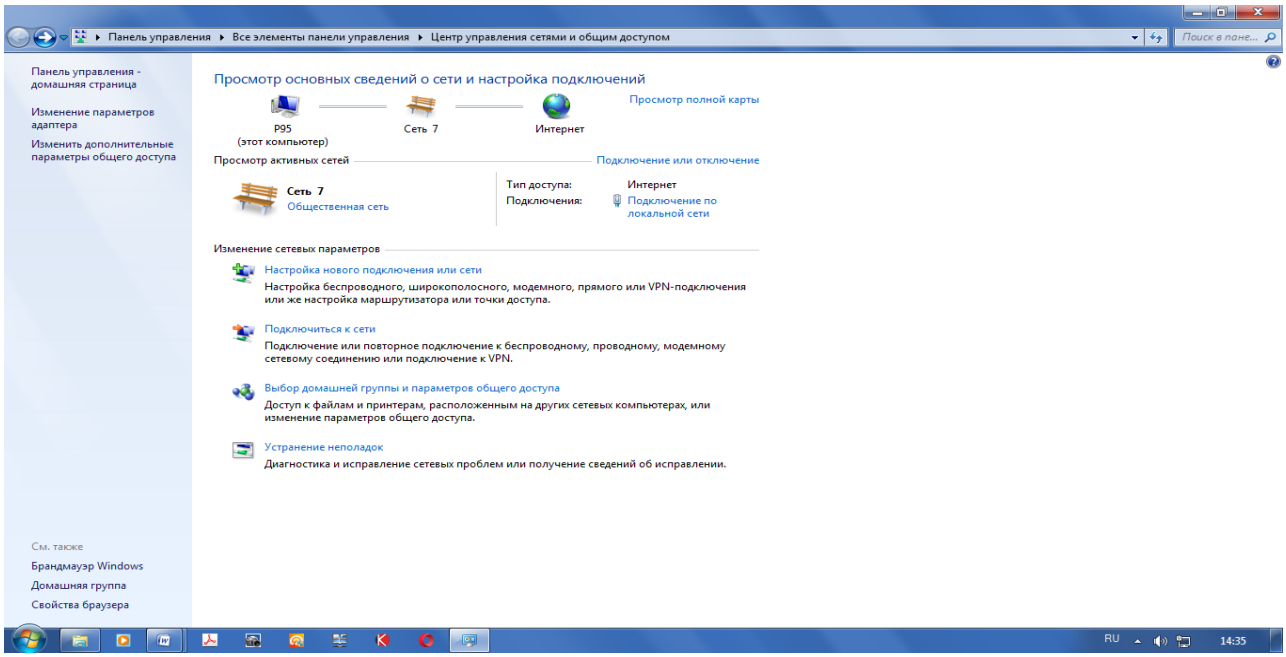


Рис. 5. Центр управління мережами та налаштування доступу

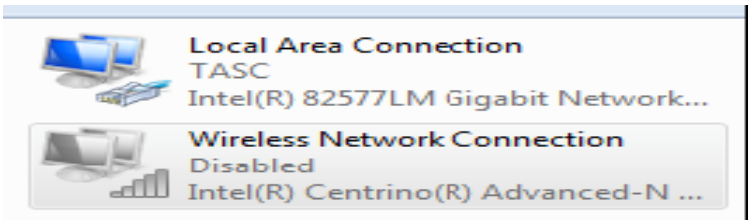


Рис. 6. Список мережевих адаптерів

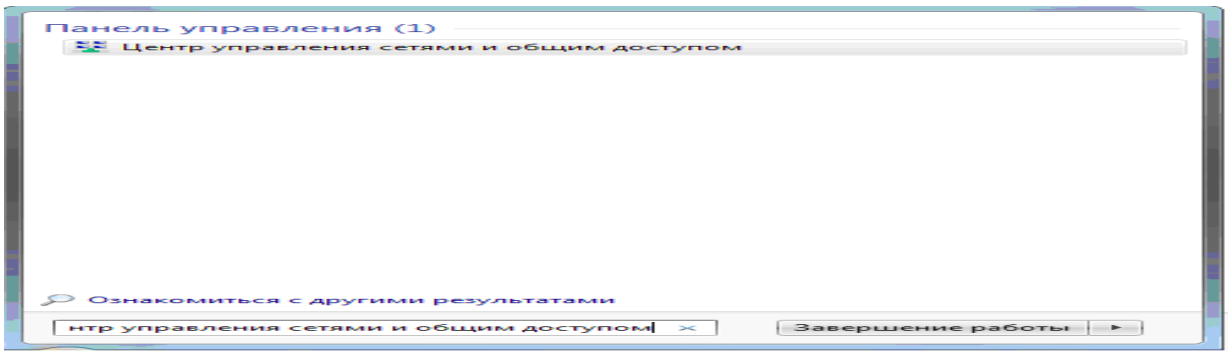


Рис. 7. Область пошуку

Мережа підприємства. Таке розташування в Інтернеті використовується в мережі малого офісу (SOHO). Для цього мережевого розташування також включено виявлення мережі, але ви не можете ні створювати, ні приєднувати комп'ютер до домашньої групи.

Громадська мережа. Це мережеве розташування призначено для використання комп'ютера в таких громадських місцях, як кафе або аеропорти. Це найбільш суворе розміщення, у якого за замовчуванням відключені можливості приєднуватися до домашньої групи та мережеве виявлення.

Доменна мережа. Якщо комп'ютер приєднаний до домену Active Directory, то мережі буде автоматично призначений тип мережевого розміщення «Домен». Доменний тип мережевого розташування аналогічний робочої мережі, за винятком того, що в домені конфігурація брандмауера Windows, мережевого виявлення, а також мережевої карти (адаптера) визначається груповою політикою.

Мережеві розташування, доступні для вибору користувачем, можна побачити на рис. 8.

1.3. Карта мережі

Карта мережі – це графічне представлення розташування комп'ютерів і пристроїв, яке дозволяє побачити всі пристрої вашої локальної мережі, а також схему їх підключення один до одного. У вікні **Центр управления сетями и общим доступом** відображається тільки локальна частина мережевої карти, компоновка якої залежить від наявних мережевих підключень. Комп'ютер, на якому виконується створення карти, відображається в лівому верхньому кутку. Інші комп'ютери підмережі відображаються зліва. Такі пристрої інфраструктури, як комутатори, концентратори і шлюзи в інші мережі відображаються праворуч. Приклад карти мережі ви можете побачити на рис. 9.

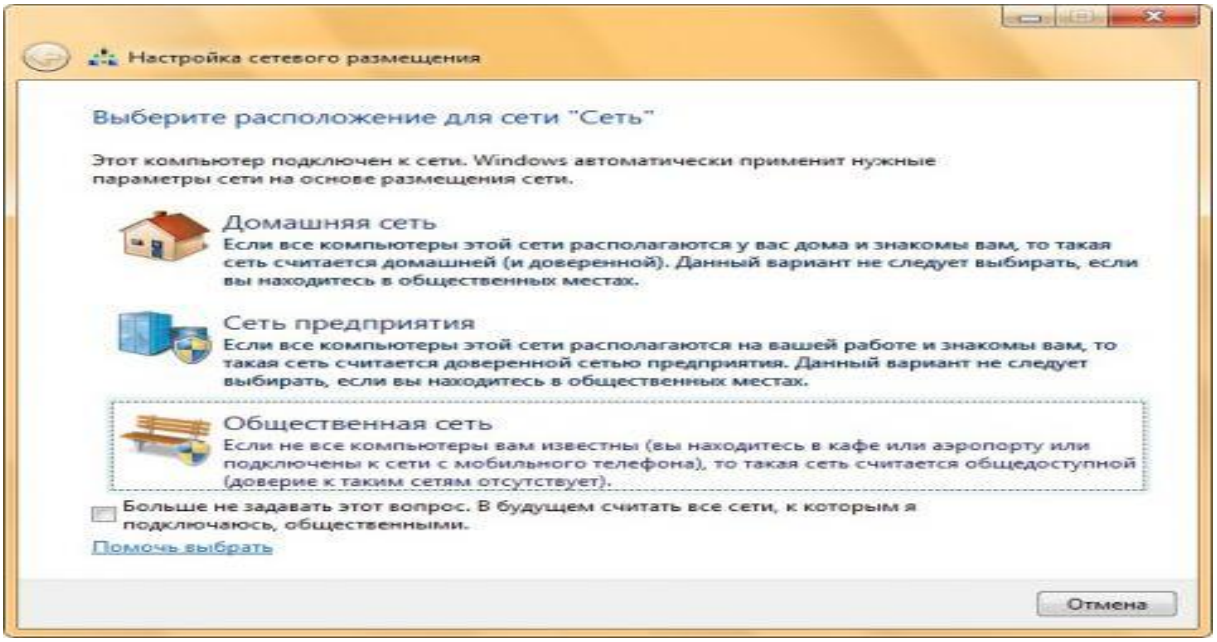


Рис. 8. Вибір мережевого розташування

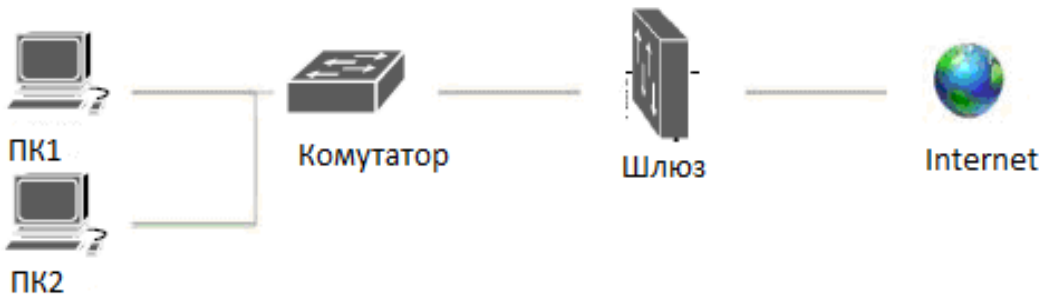


Рис. 9. Приклад карти мережі

За роботу карти мережі в операційних системах відповідають два компоненти:

Виявлення топології зв'язку Link Layer (Link Layer Topology Discover Mapper – LLTD Mapper) – компонент, який запитує в мережі пристрої для включення їх в карту;

Відповідає пристрій LLTD (Link Layer Topology Discover Responder – LLTD Responder) – компонент, який відповідає за запити компонента LLTD Mapper.

За замовчуванням, карту мережі можна переглядати тільки для розташувань «Домашня мережа» або «Мережа підприємства». При спробі перегляду мережевої карти для розташувань «Доменна мережа» або «Громадська мережа» ви побачите наступне повідомлення (рис. 10).

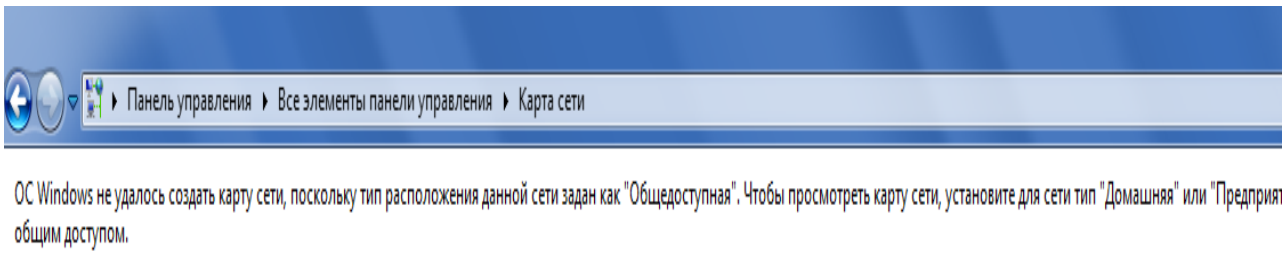


Рис. 10. Спроба перегляду карти мережі для доменної мережі

Для того щоб включити мережеве зіставлення в доменній мережі, вам потрібно на контролері домену виконати наступні дії:

Відкрийте **Управление групповой политикой;**

Виберіть об'єкт групової політики (наприклад, Default Domain Policy, область дії – весь домен), який буде поширюватися на комп'ютер, розташований в доменній мережі, натисніть на ньому правою кнопкою миші і з контекстного меню виберіть команду **Изменить**.

В оснащенні **Редактор управления групповой политикой** розгорніть **Конфигурация компьютера / Политики / Административные шаблоны / Сеть / Выявление топологии связи** (Link Layer) і виберіть політику **Включает драйвер отображение введения / выведения (LLTDIO)»;**

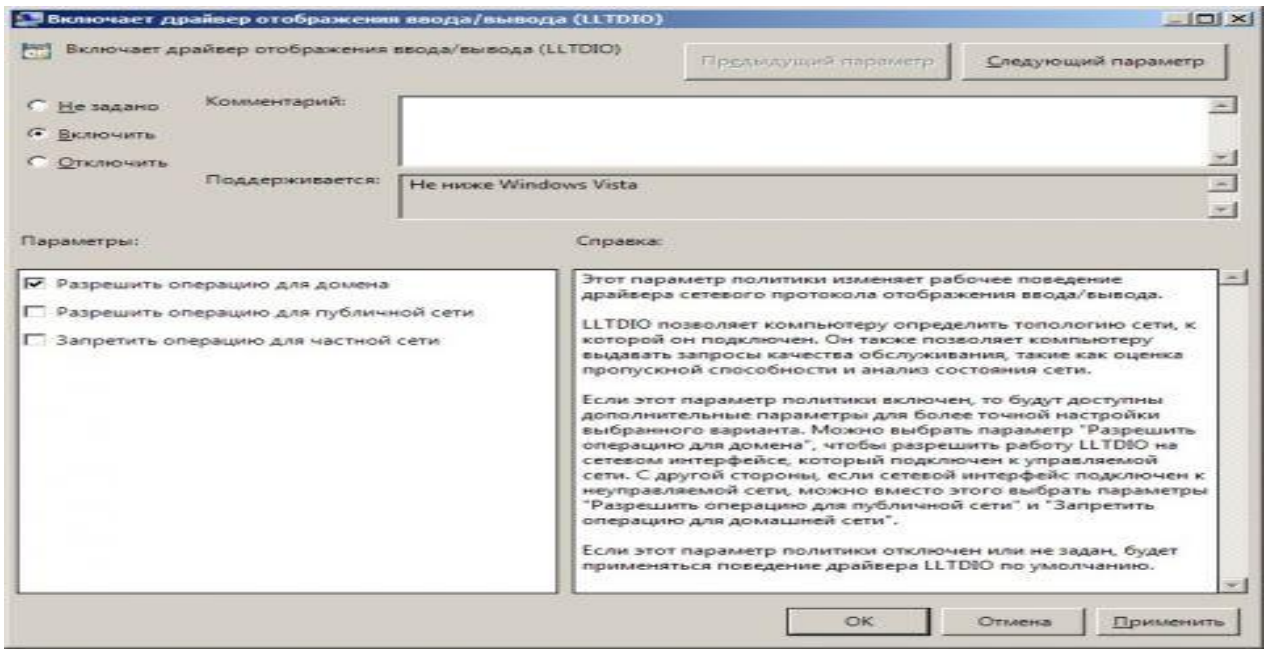


Рис. 11. Зміна групових політик для включення мережевого зіставлення

У властивостях параметра політики встановіть перемикач на опцію **Включить** встановіть прапорець **Разрешить операцию для домену** (рис. 11)

Повторіть аналогічні дії для параметра політики **Включить драйвер ответчика (RSPNDR);**

Оновіть параметри політики на клієнтській машині використовуючи команду **gpupdate / force / boot**;

Оновіть карту мережі (рис. 12).

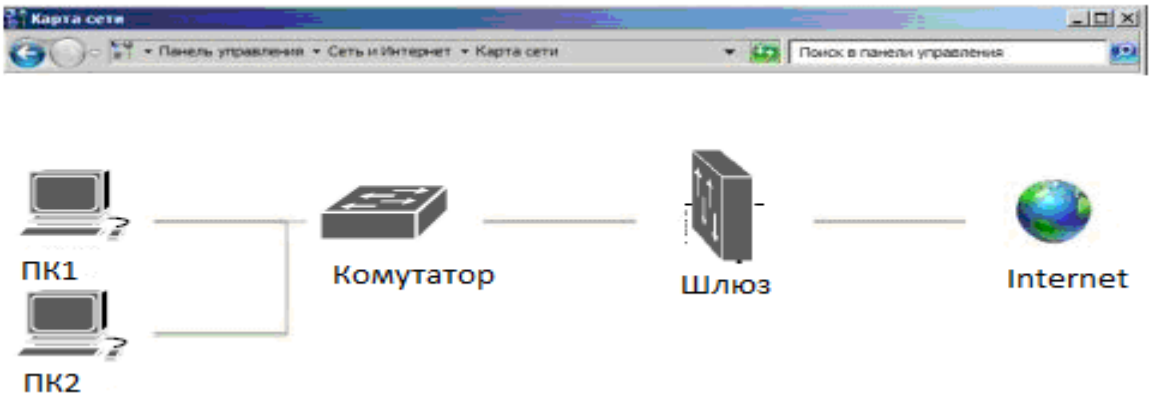


Рис. 12. Карта мережі для доменної мережі

1.4. Мережеві підключення.

Після установлення драйвера для кожного мережевого адаптера, операційна система Windows намагається автоматично налагодити мережеві підключення на локальному комп'ютері. Всі доступні мережеві підключення відображаються у вікні **Сетевые подключения**. Підключення до мережі являє собою набір даних, необхідних для підключення комп'ютера до Інтернету, локальної мережі або будь-якого іншого комп'ютера.

Відкрити вікно **Сетевые подключения** ви можете будь-яким з наступних способів:

1. Відкрийте вікно **Центр управления сетями и общим доступом** і перейдіть за посиланням **Изменение параметров адаптера** (рис. 13).

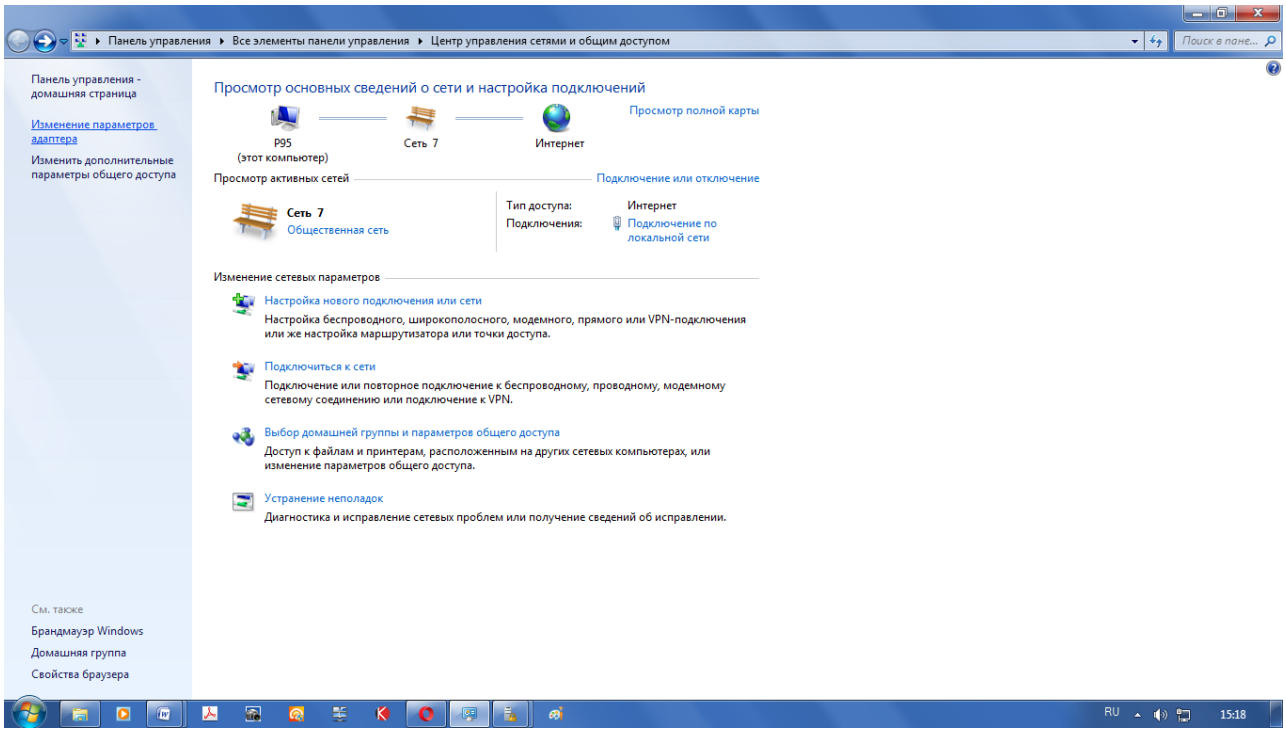


Рис. 13. Зміна параметрів адаптера

2. Натисніть на кнопку **Пуск** для відкриття меню, в поле пошуку введіть **Просмотр сетевых** (рис. 14) і в знайдених результатах відкрийте додаток **Просмотр сетевых подключений.**

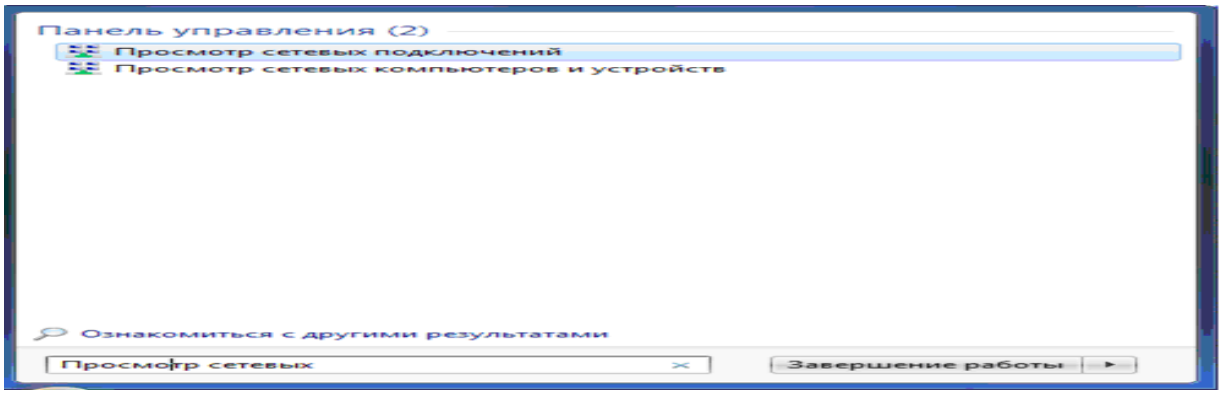


Рис. 14. Перегляд мережевих підключень

Вікно «Мережеві підключення» відображені на рис. 15.

При виборі будь-якого мережевого підключення можна виконати з ним наступні дії:

Перейменування підключення. Операційна система за замовчуванням призначає всім мережевим підключенням імена **Подключение по локальной сети** або **Подключение по безпроводной сети** і номер підключення в тому випадку, якщо у вас існує більше одного мережевого підключення. При бажанні, ви можете перейменувати будь-яке мережеве підключення одним з наступних способів:

1. Натисніть на клавішу **F2**, введіть нове ім'я мережевого підключення, після чого натисніть на клавішу **Enter;**

2. Натисніть правою кнопкою миші на мережевому підключенні яке перейменовується і з контекстного меню виберіть команду **Переименовать**. Введіть нове ім'я мережевого підключення, після чого натисніть на клавішу **Enter;**

Примітка:

- Ім'я підключення не може містити знаків табуляції й будь-яких знаків з наступного набору:

\ / : * ? < > |

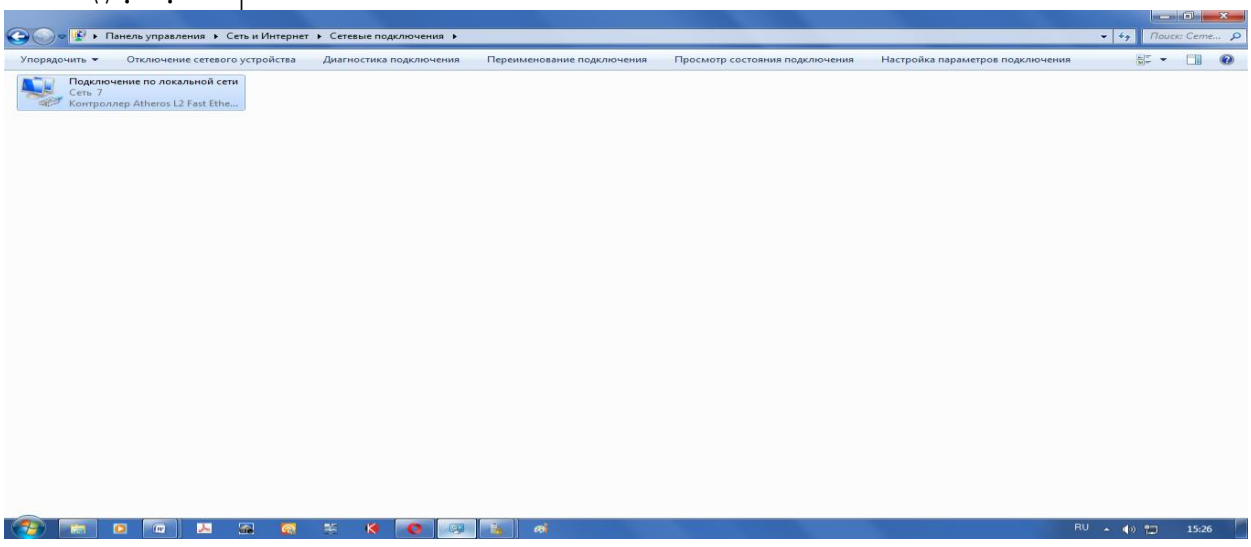


Рис. 15. Вікно Мережеві підключення

Стан мережі. Використовуючи дане вікно, ви можете переглянути будь-які дані про стан мережевого підключення і такі деталі, як IP-адреса, MAC-адреса та інше. Щоб відкрити діалогове вікно відомостей про мережеве підключення, виконайте наступні дії:

Відкрийте діалогове вікно **Состояние** одним із таких способів:

Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Состояние** (рис. 16).

Виберіть підключення до мережі та натисніть на клавішу **Enter**.

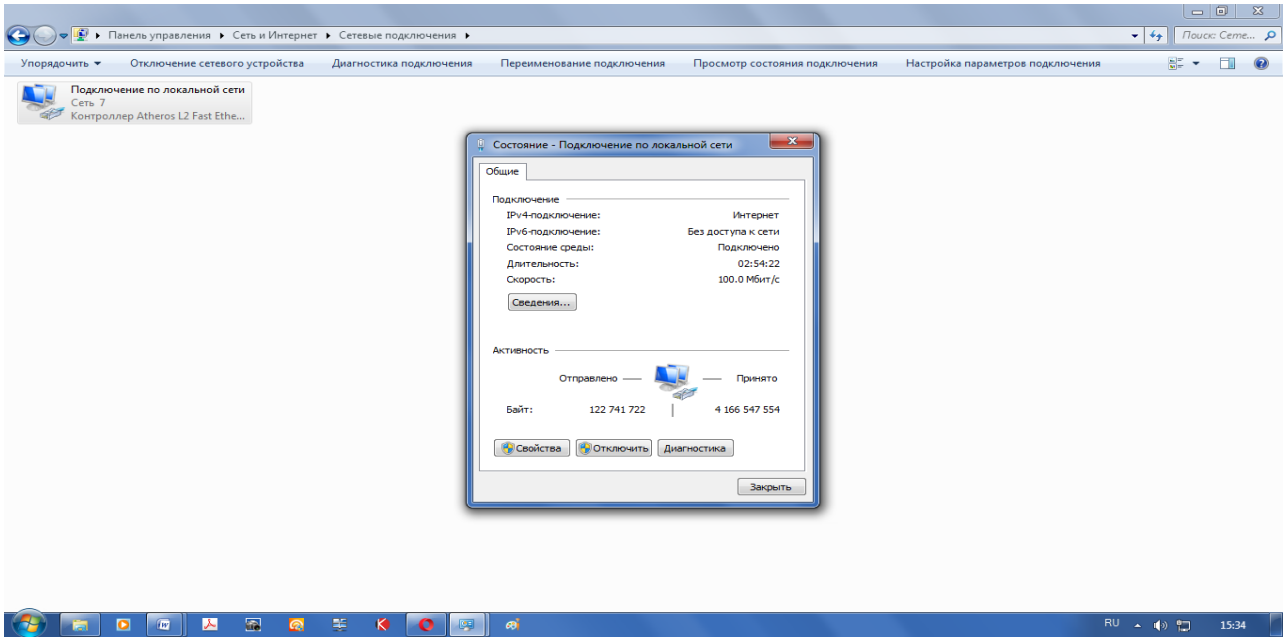


Рис. 16. Вікно стану мережевого з’єднання

Натисніть правою кнопкою миші на мережевому підключенні, яке перейменовується і з контекстного меню виберіть команду **Переименовать**. Введіть нове ім'я мережевого підключення, після чого натисніть на клавішу **Enter**;

Стан мережі. Використовуючи дане вікно, ви можете переглянути будь-які дані про стан мережевого підключення і такі деталі, як IP-адреса, MAC-адреса та інше. Щоб відкрити діалогове вікно відомостей про мережеве підключення, виконайте наступні дії:

Відкрийте діалогове вікно **Состояние** одним із таких способів:

Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Состояние** (рис. 17).

Виберіть підключення до мережі та натисніть на клавішу **Enter**.

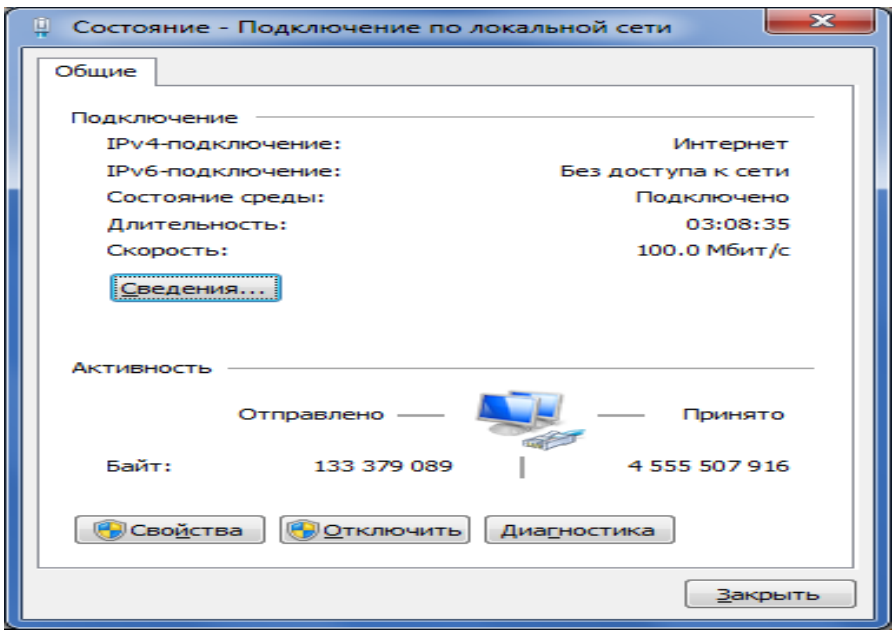


Рис. 17. Діалогове вікно стану підключення по локальній мережі

У вікні **Состояние подключения по локальной сети** натисніть на кнопку **Сведения**. У діалоговому вікні **Сведения о сетевом подключении**, (рис. 18) відображеному нижче, ви можете переглянути докладні відомості про поточний стан мережевого підключення.

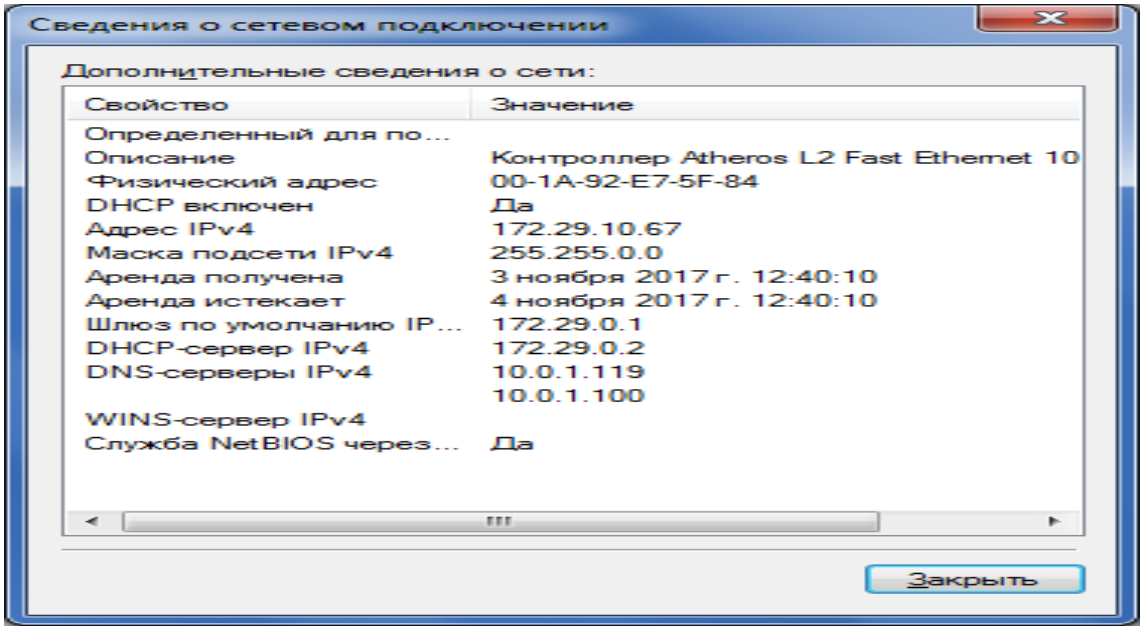


Рис. 18. Відомості про мережеве підключення

Діагностика підключення. У разі виявлення проблем в роботі вашого мережевого підключення, вікно **Сетевые подключения** пропонує засіб діагностики **Устранение неполадок**, яке містить можливість вирішення за допомогою аналізу підключення. Для того щоб скористатися даною засобом виконайте одну з таких дій:

Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Диагностика** (рис. 19).

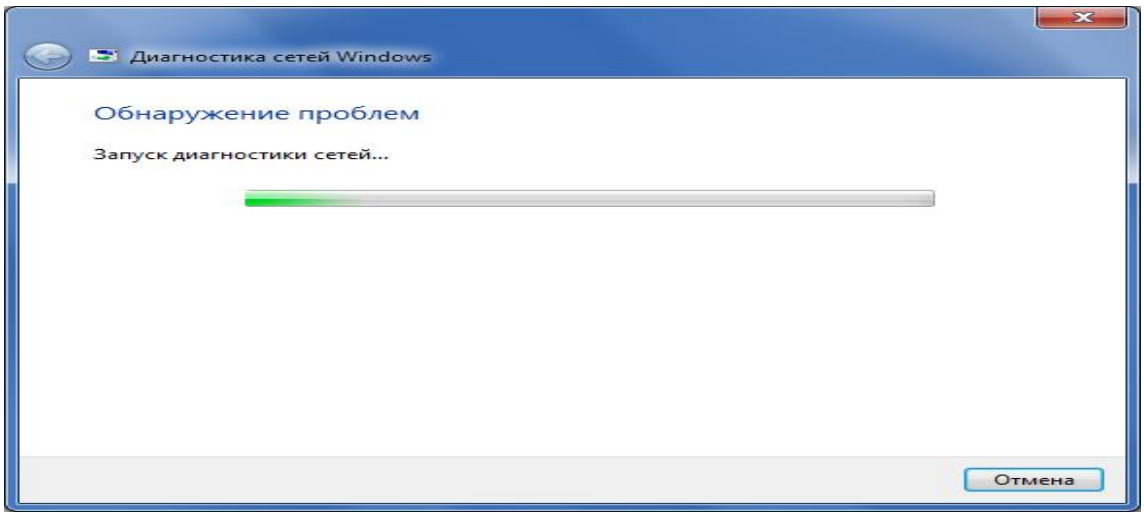


Рис. 19. Відкриття майстра усунення неполадок підключення по локальній мережі

У діалоговому вікні **Диагностика сетей Windows** для усунення неполадок дотримуйтесь дій майстра (рис. 20).

При подачі команди **Просмотреть дополнительные параметры** можна отримати додаткову допомогу (рис. 21).

Відключення мережевого пристрою. Іноді проблеми з мережевими підключеннями вирішуються за допомогою відключення мережевого адаптера комп'ютера від мережі. Для того щоб відключити мережевий адаптер виконайте одну з таких дій:

Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Отключить**.

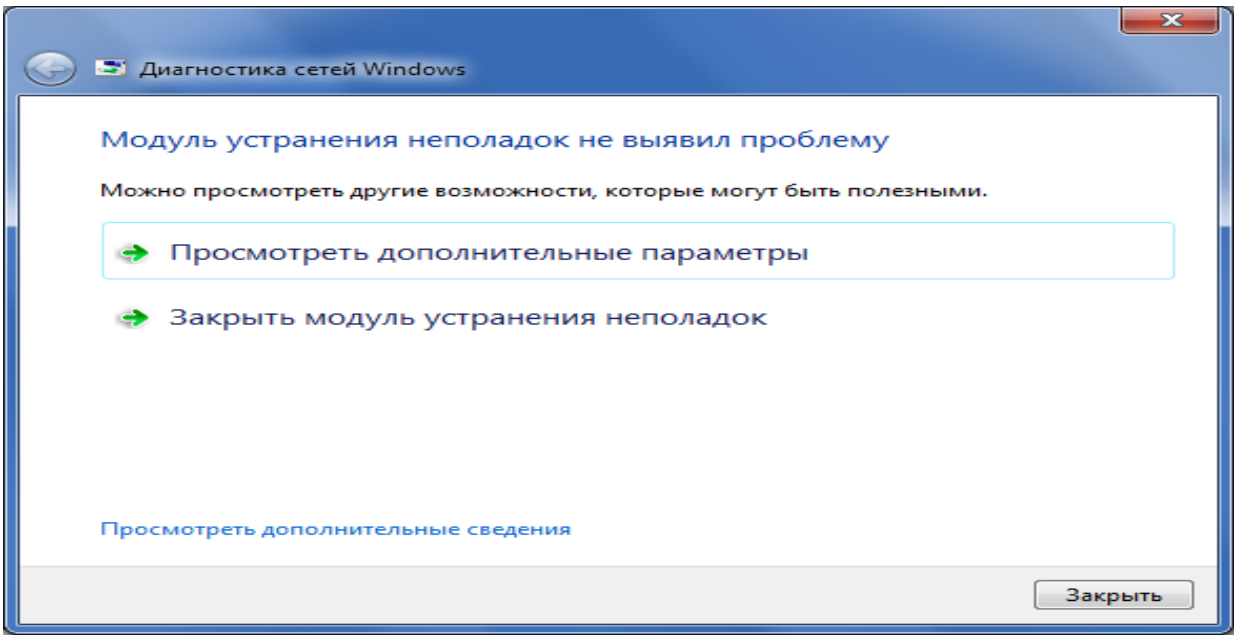


Рис. 20. Вікно майстра усунення неполадок підключення по локальній мережі

Налагодження параметрів підключення. Як такі, мережеві підключення не дозволяють здійснювати комунікації. Здійснення комунікацій забезпечують мережеві клієнти, служби і протоколи, які прив'язані до створених мережевих підключень. Для того щоб змінити налаштування вашого мережевого підключення, ви можете скористатися засобами налагодження параметрів підключення. Для зміни компонентів і налаштувань мережевого підключення, виконайте наступні дії:

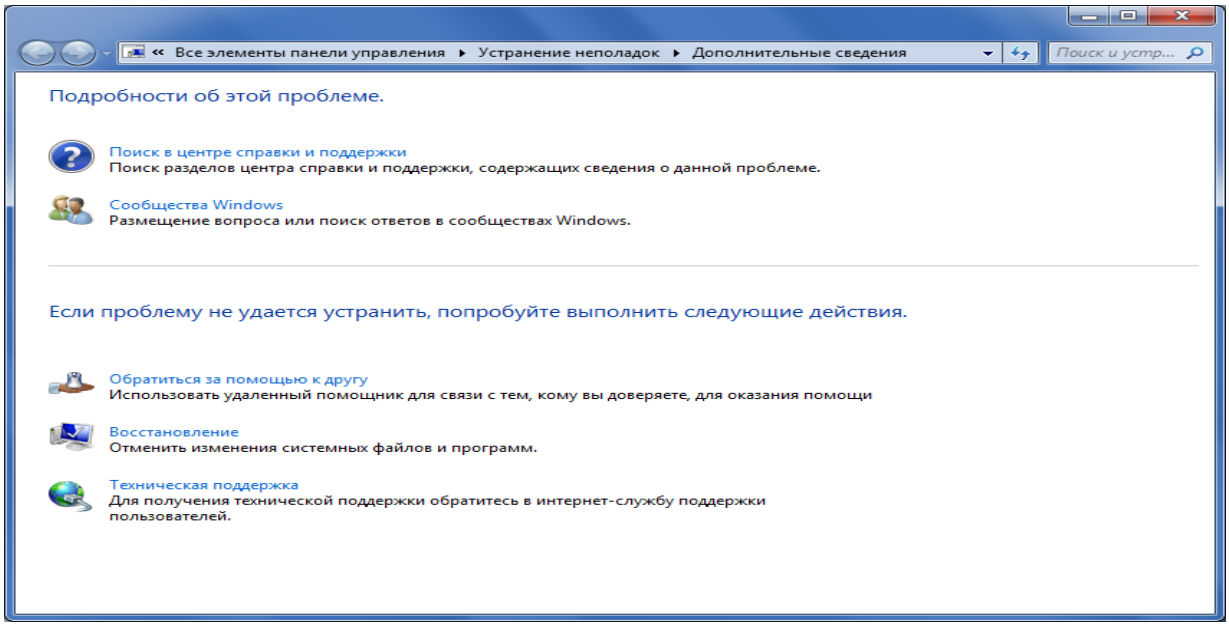


Рис. 21. Вікно додаткової допомоги

Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Свойства.**

Виберіть підключення до мережі та скористайтеся комбінацією клавіш Alt + Enter.

Встановлені біля компонентів прапорці (рис. 22) вказують, що ці компоненти прив'язані до підключення. Діалогове вікно властивостей мережевого підключення відображено нижче:

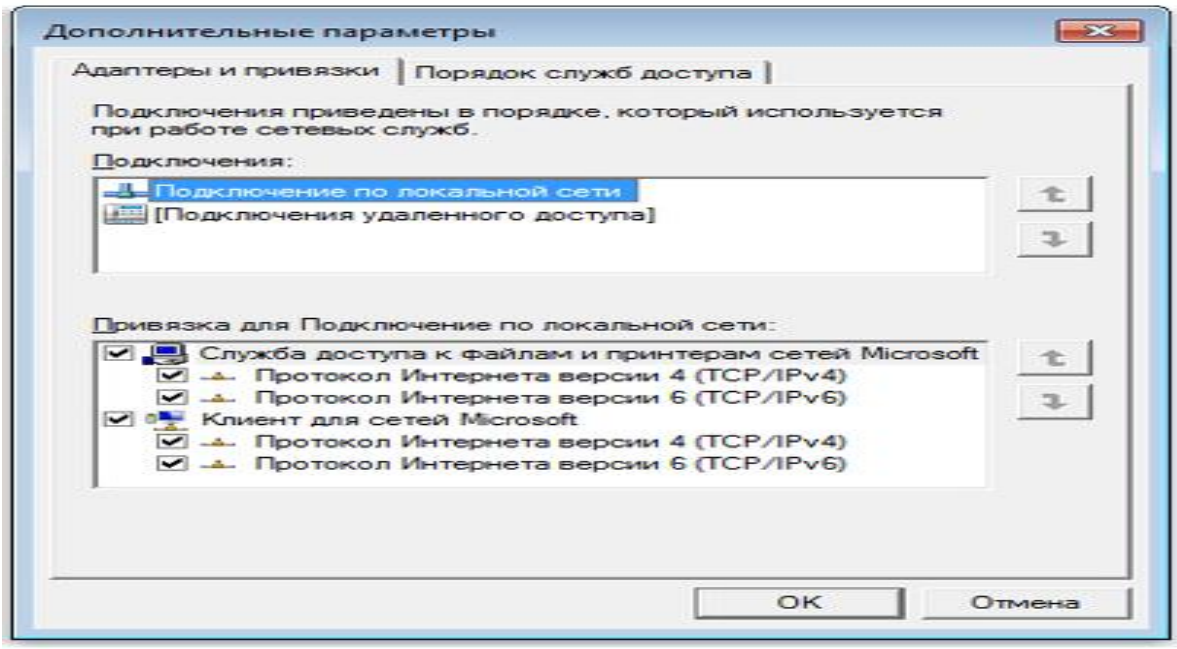


Рис. 22. Діалогове вікно властивостей мережевого підключення

Зміна порядку прив'язки мережевих протоколів

Якщо комп'ютер підключений до мережі, параметри мережевої політики можуть перешкодити виконанню даних дій.

Якщо мережа працює повільно, розгляньте можливість зміни порядку прив'язки мережевих протоколів. Windows намагається зв'язуватися зі службами мережевих протоколів у тому порядку, який зазначений у папці «Мережеві підключення». Для прискорення мережевих підключень можна розташувати протоколи в цьому списку в порядку від найбільш використовуваного до найменш використовуваного. Звичайно найбільш використовуваним є протокол TCP/IP.

Примітка. Якщо використовується тільки протокол TCP/IP, ніяких змін вносити не потрібно.

Натисніть клавішу **ALT** і в меню **Дополнительно** виберіть пункт **Дополнительные параметры** . З появою запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.

Перейдіть на вкладку **Адаптеры и привязки**, а потім у списку **Подключения** виберіть підключення, яке потрібно змінити.

У розділі **Привязка для имя подключения** виберіть протокол, який потрібно перемістити вище або нижче за списком, натисніть кнопку стрілка вгору або стрілка вниз . а потім натисніть кнопку **ОК.**

1.5. Підключення до мережі для Windows 7

Під’єднайте кабель підключення нашої мережі до порту мережевої карти на вашому комп’ютері.

Щоб система видала всі необхідні налаштування для роботи в мережі, мережева карта (рис. 23) вашого комп'ютера повинна бути налаштована в автоматичному режимі отримання мережевих налаштувань.

Рис. 23. Мережеві карти

1. Заходимо в **Пуск Панель управления** (рис. 24).
2. Обираємо Центр управления сетями и общин доступом (рис. 25).
3. Далі у верхньому лівому кутку натискаємо на Изменение параметров адаптера (рис. 5).
4. Вибираємо підключення для мережевого адаптера, до якого під'єднано кабель підключення нашої мережі. Переконайтеся, що з'єднання включено, якщо ні – увімкніть його. За обраним мережевім підключенням натискаємо правою кнопкою миші, вибираємо Свойства (рис. 26).
5. Для подальших налаштувань у відкритому вікні нашого з'єднання потрібно в компонентах, використовуваних ним підключенням, вибрати **Протокол Інтернету версії 4 (TCP/IPv4)** (рис. 27)**.**
6. Далі у властивостях Протоколу Інтернету версії 4 (TCP/IPv4) обираємо **Получить IP-адрес автоматически**. Також натискаємо на **Получить IP-адрес DNS-сервера автоматически** (рис. 28).

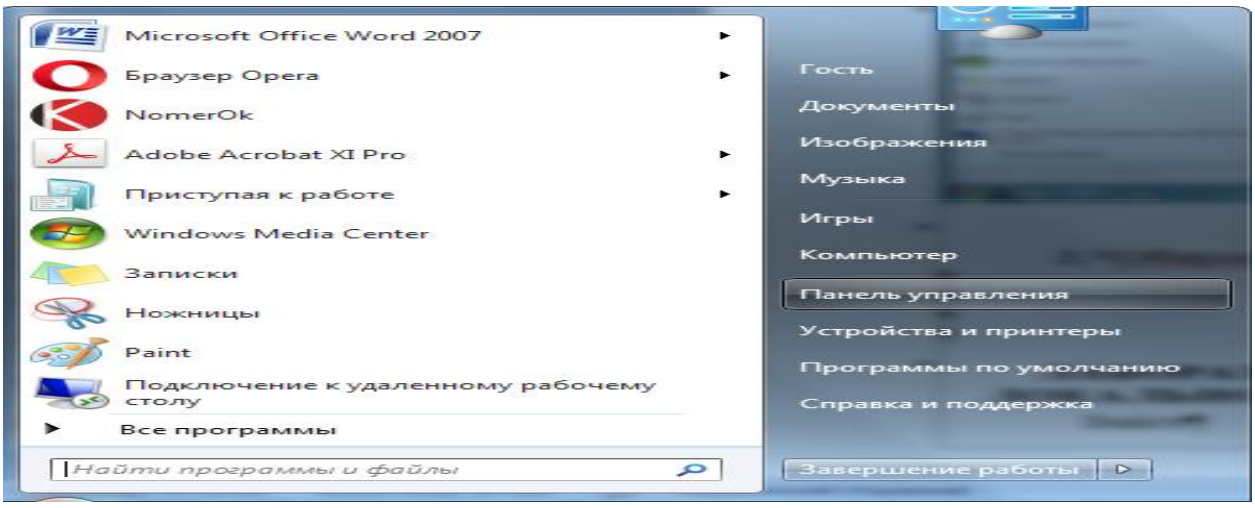


Рис. 24. Вхід в панель управління

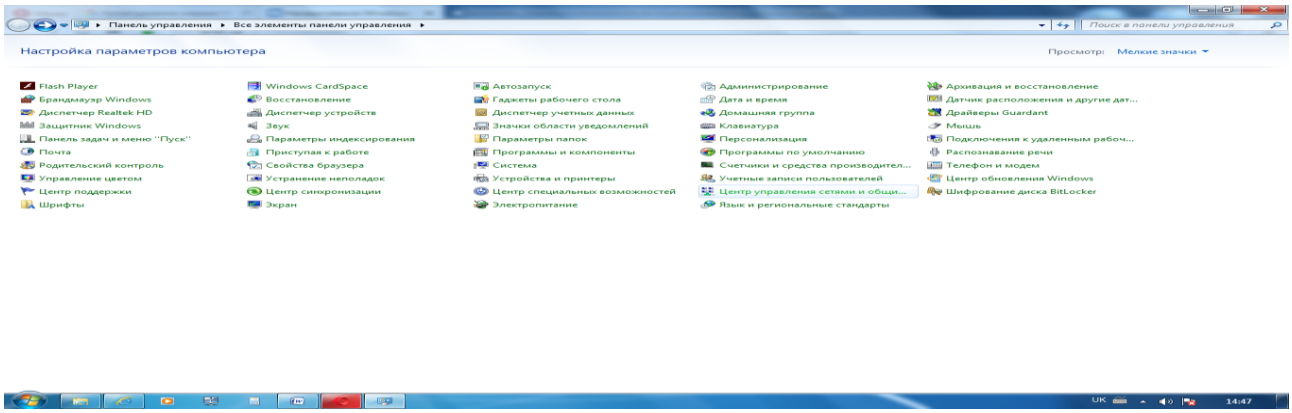


Рис. 25. Центр управління мережами та загальним доступом

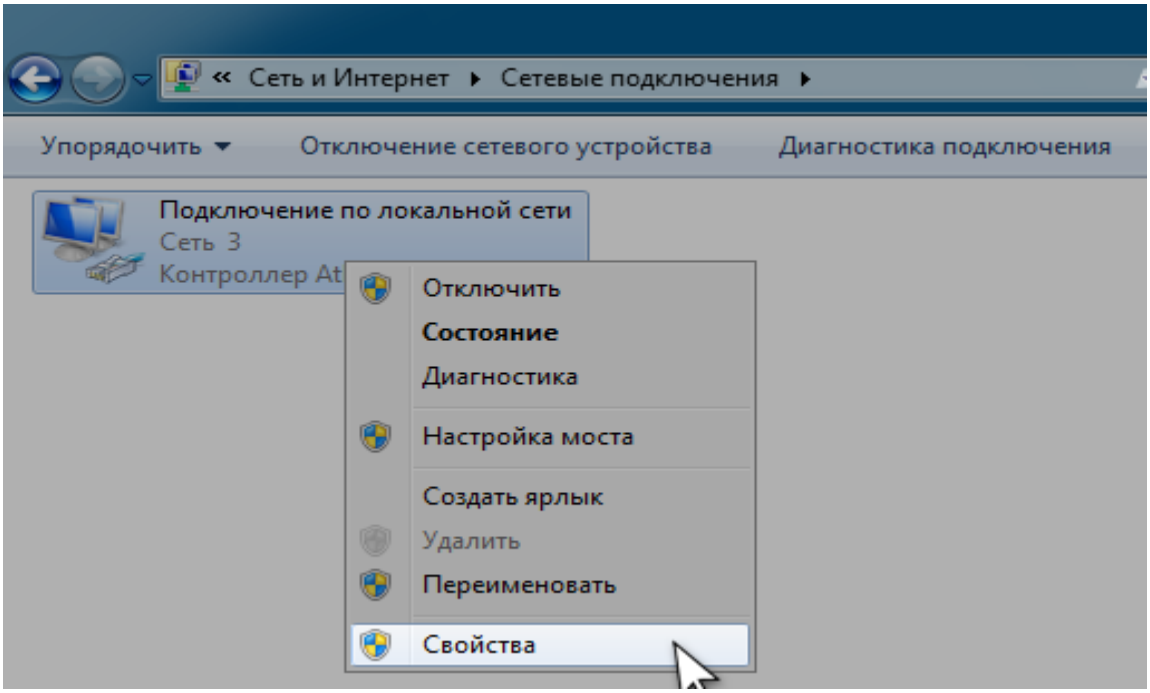


Рис. 26. Відбір властивостей мережі

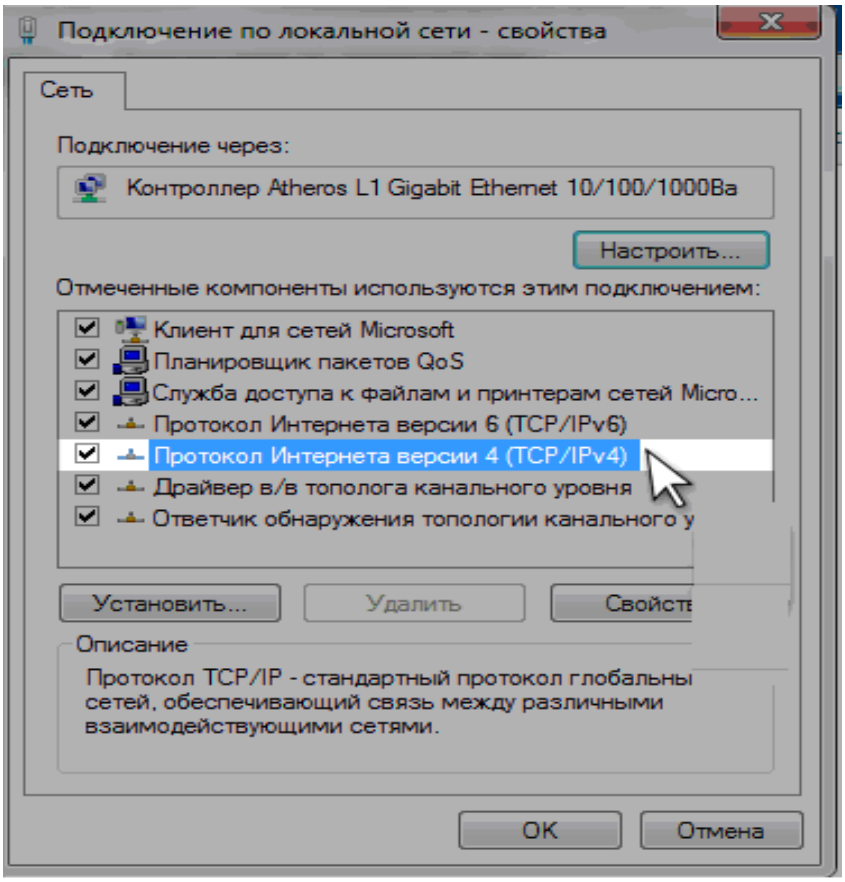


Рис. 27. Відбір протоколу

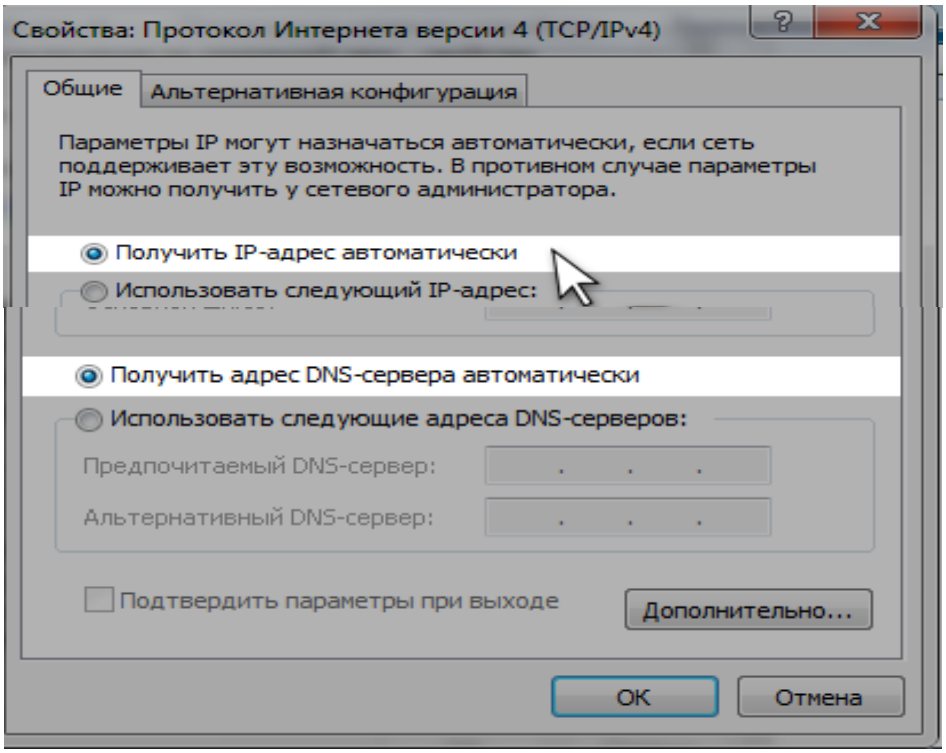


Рис. 28. Видбір параметрів мережі

Після виконання всіх вищеописаних дій, налаштування підключення до мережі можна вважати закінченим.

2. Хід роботи

Виконайте всі дії, що описані в розділі 1 Теорія. Збережіть всі вікна, що використовувалися в роботі у програмі MS Word. При захисті лабораторної роботи представте їх викладачу.

3. Контрольні питання

1. Який компонент операційних систем Windows найчастіше використовується для конфігурування мережевих властивостей та чому?
2. Порядок відкриття вікна «Центр управління мережами і загальним доступом».
3. Які активні профілі підтримує операційна система Windows 7?
4. Розкрийте поняття мережеві розташування.
5. Розкрийте поняття карта мережі.
6. Які компоненти операційної системи Windows 7 відповідають за роботу карти мережі?
7. Як налаштувати компонент **Управление групповой политикой?**
8. Для чого призначений компонент мережеві підключення?
9. Як перейменувати мережеве підключення?
10. Як отримати відомості про стан мережевого підключення?
11. Як усунути проблеми в мережевому підключенні?
12. Як відключити мережевий пристрій?
13. Як провести реальне підключення ПК до мережі?

ЛАБОРАТОРНА РОБОТА 5. НАЛАГОДЖЕННЯ ПАРАМЕТРІВ ЛОКАЛЬНОЇ МЕРЕЖІ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS XP

Мета роботи: навчитись налаштовувати локальну мережу за допомогою операційної системи Windows XP.

Зміст

1. Теорія
1.1 Налагодження параметрів локальної мережі
1.2 Підключення мереженого принтера
2. Хід виконання роботи
3 Контрольні питання

1. Теорія

1.1. Налагодження параметрів локальної мережі

Налагодження параметрів локальної мережі проводиться через **панель задач → Сеть** (рис. 1) команда **Состояние,** або мережеві підключення (рис. 2). З'явиться діалогове вікно із вкладками **Общие** (рис. 3) і **Поддержка** (рис. 4).

Налагодження параметрів служб та протоколу TCP/IP (рис. 5) проводиться введенням команди **Свойства.** При введені команди **Свойства** на вкладці **Общие** можна вибрати служби (рис. 6) та налагодити контролер мережі. При введенні команди **Дополнительно** з'являється можливість додаткового налагодження протоколу TCP/IP (рис.7), DNS сервера – (рис. 8), параметрів підключення – (рис. 9), фільтрацію трафіка мережі – (рис. 10) та налагодження її властивостей (рис. 11).

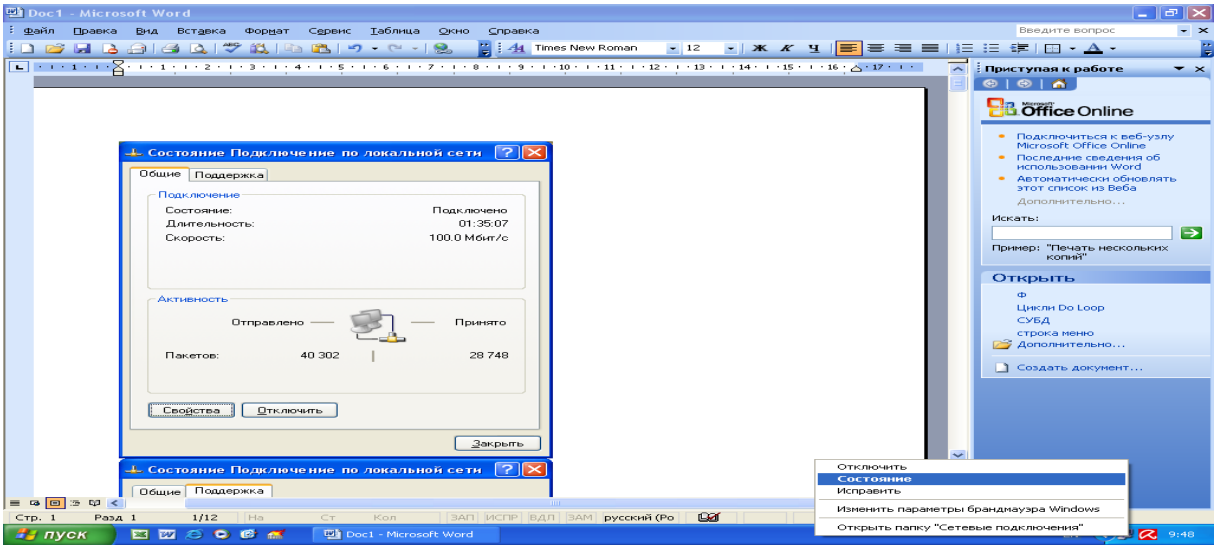


Рис. 1. Початок налагодження параметрів локальної мережі

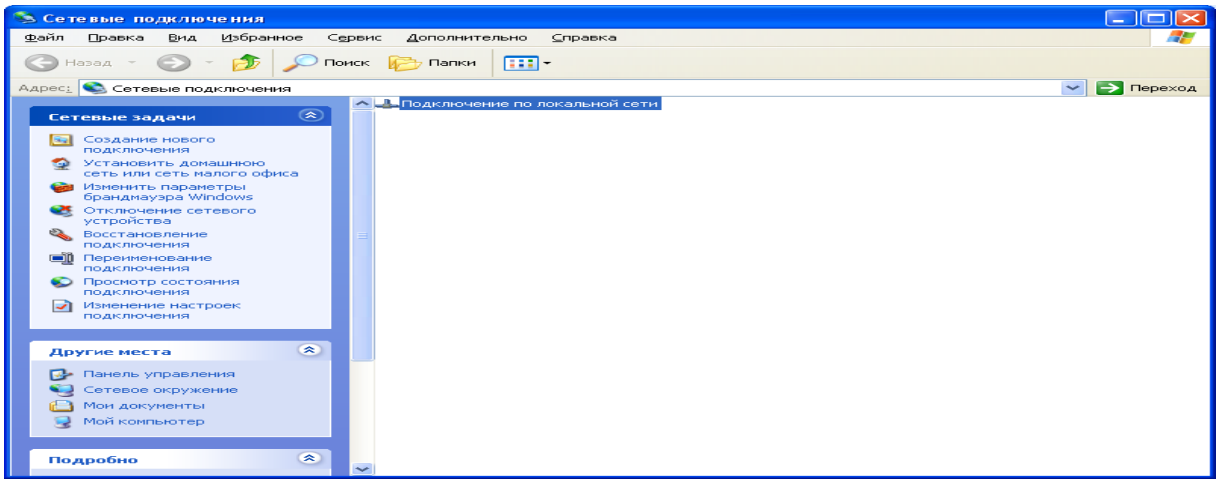


Рис. 2. Мережеві підключення

На вкладці **Проверка подлинности** та **Дополнительно** вибираються параметри захисту комп'ютера в мережі (рис. 12– 20).

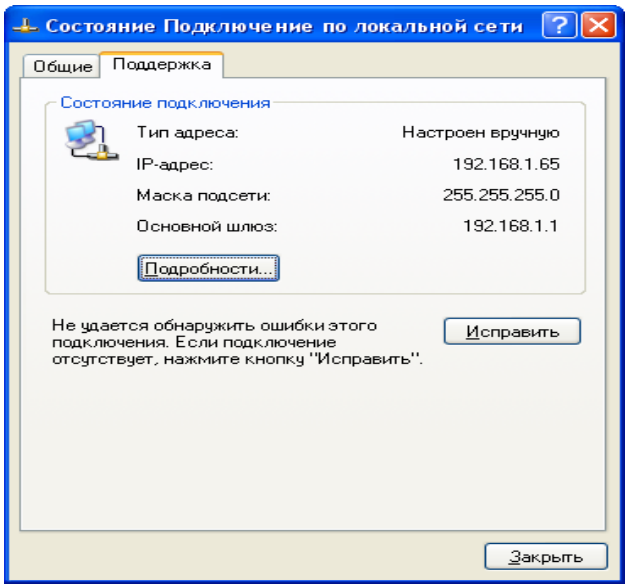


Рис. 3. Стан підключення до мережі вкладка **Поддержка**

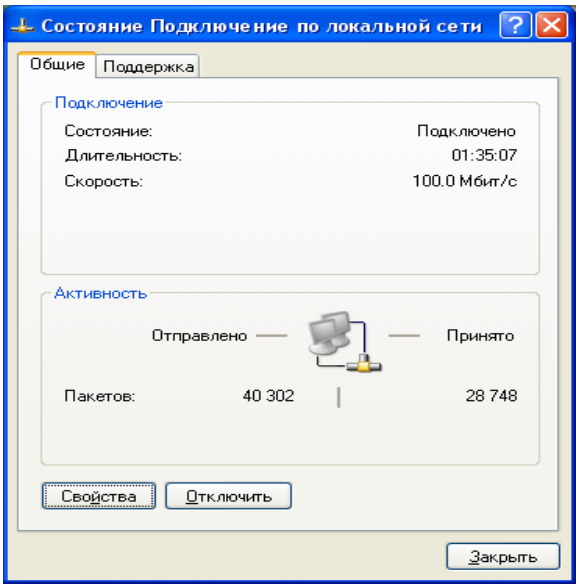


Рис. 4. Вкладка **Общие**

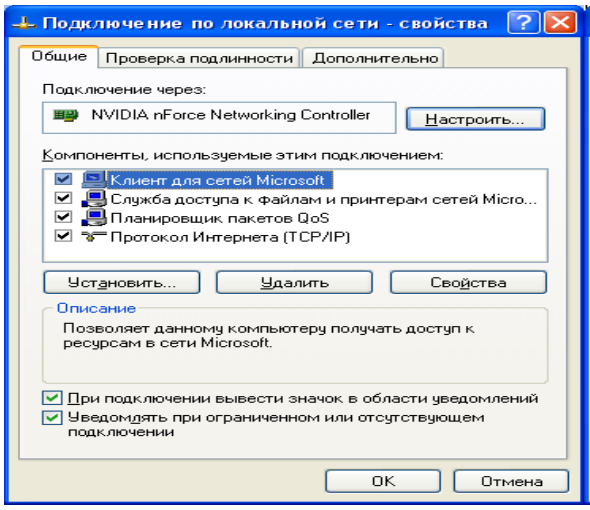


Рис. 5. Вікно **Свойства**

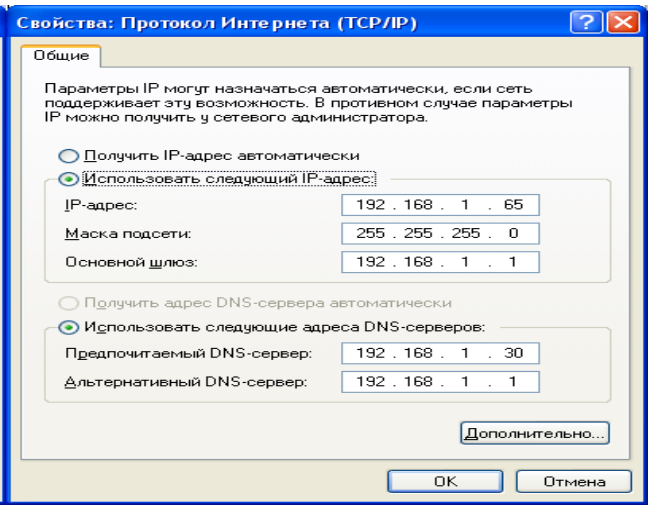


Рис. 6. Параметри протоколу TCP/IP

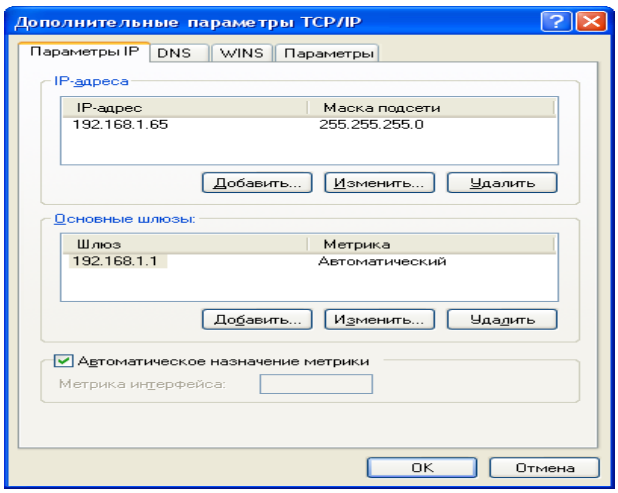


Рис. 7. Додаткові параметри протоколу TCP/IP

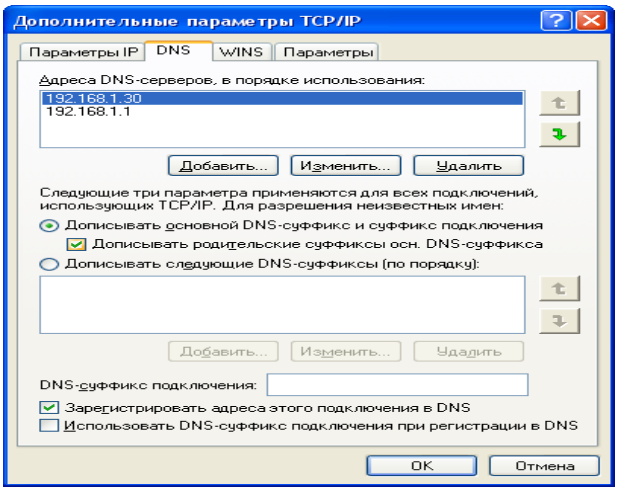


Рис. 8. Параметри DNS сервера

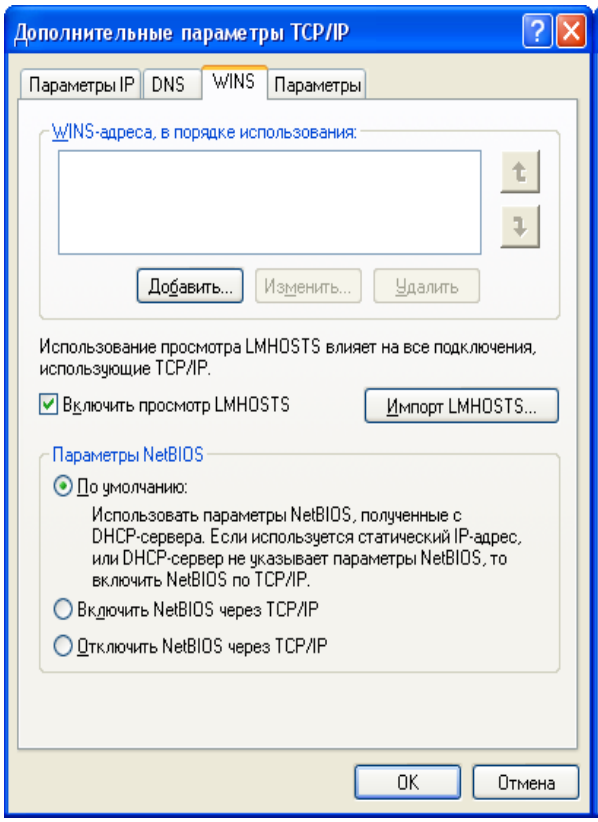


Рис. 9. Параметри підключення

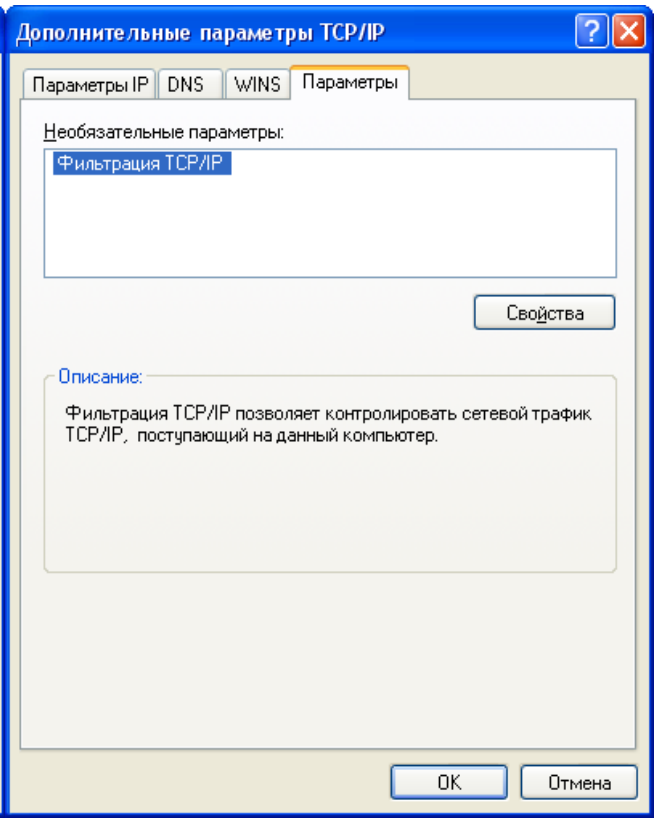


Рис. 10. Фільтрація трафіка

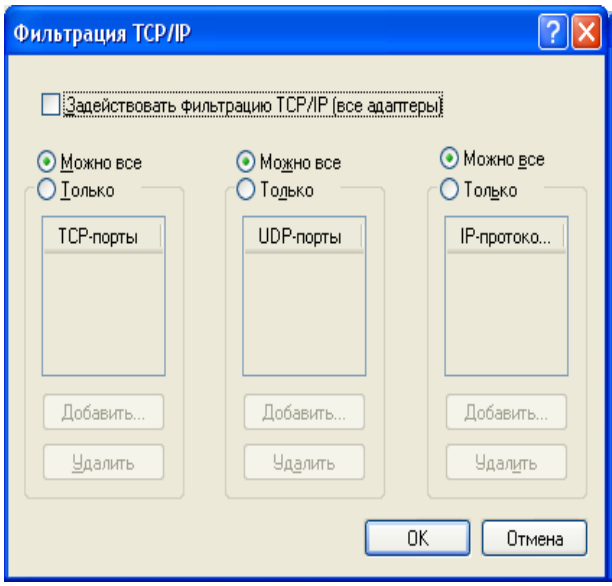


Рис. 11. Відбір параметрів фільтрації

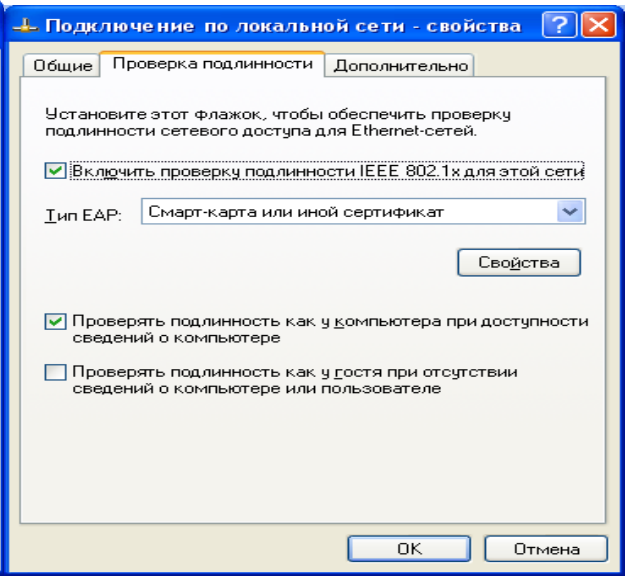


Рис. 12. Параметри захисту комп’ютера

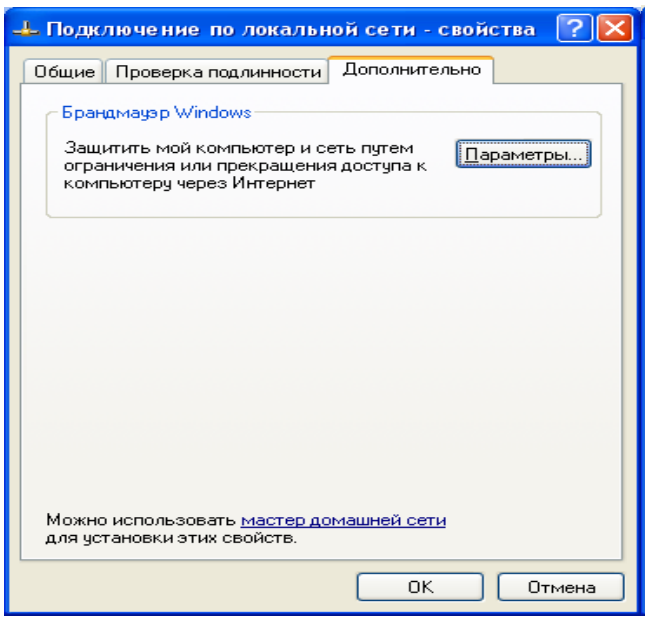


Рис. 13. Запуск брандмауера

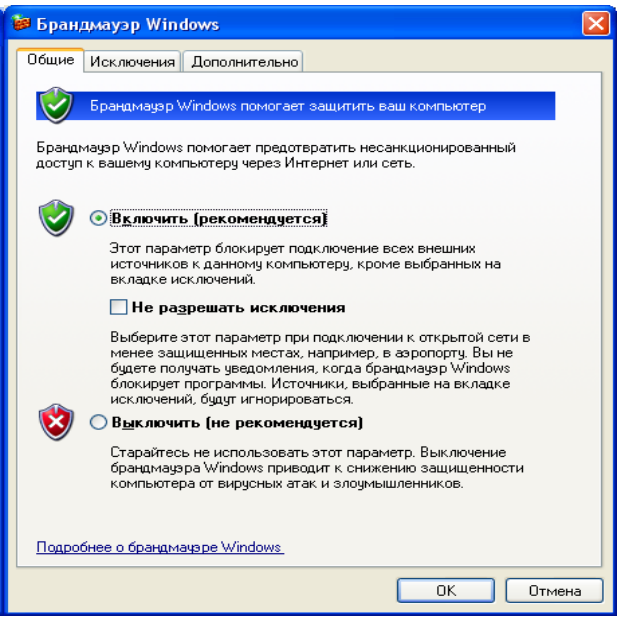


Рис. 14. Відбір параметрів брандмауера

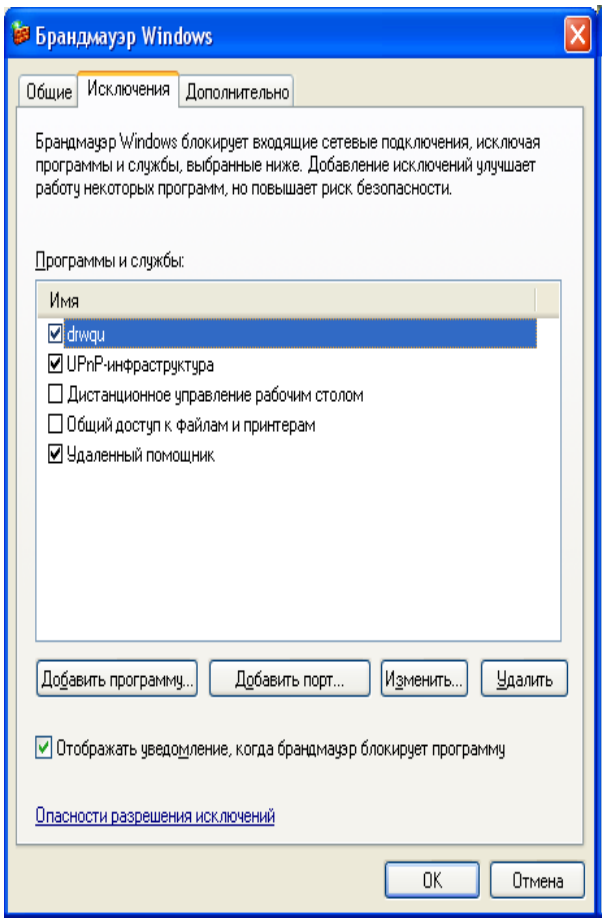


Рис. 15. Дозвіл виключень в захисті

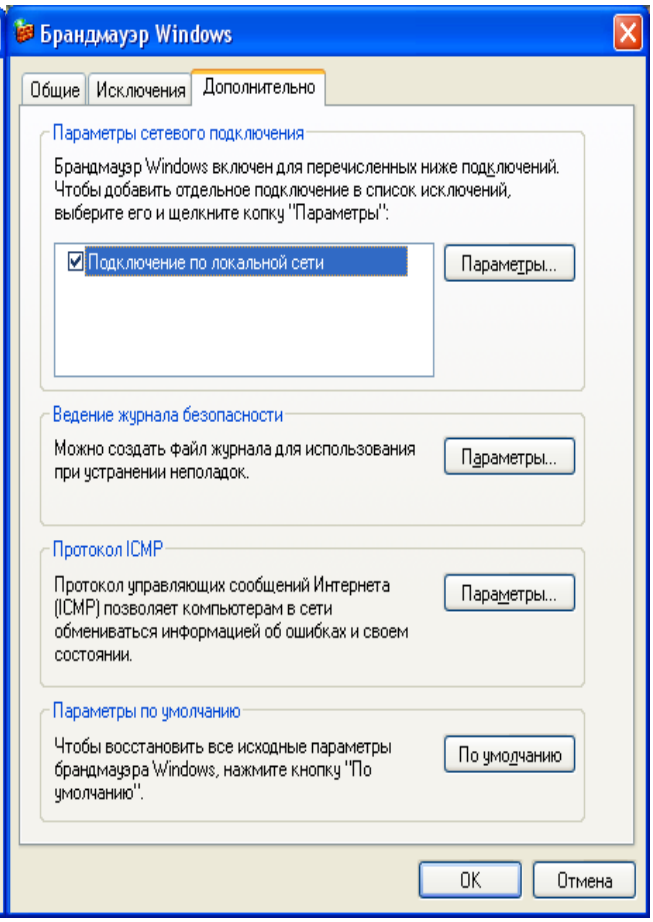


Рис. 16. Вибір параметрів захисту комп’ютера

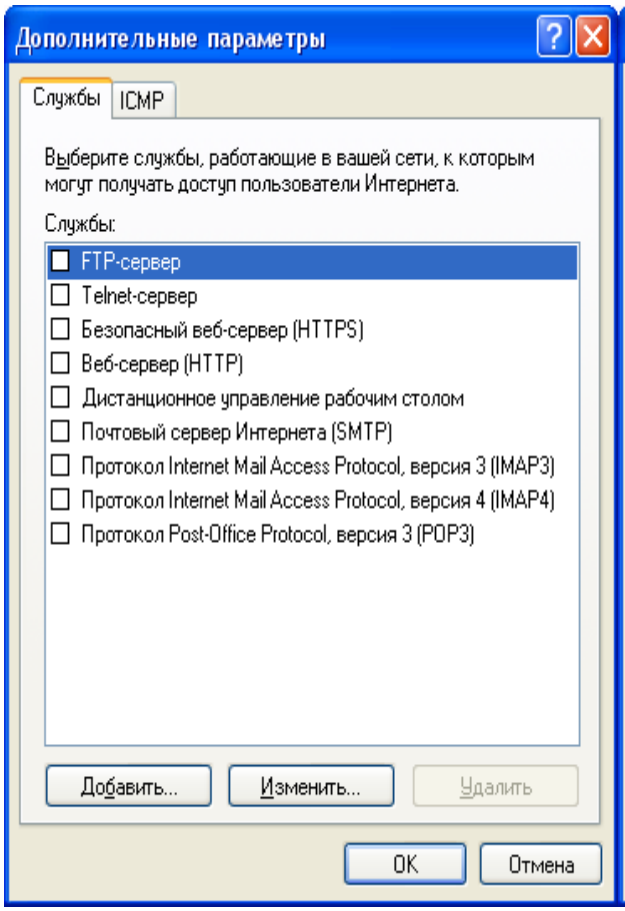


Рис. 17. Служби захисту

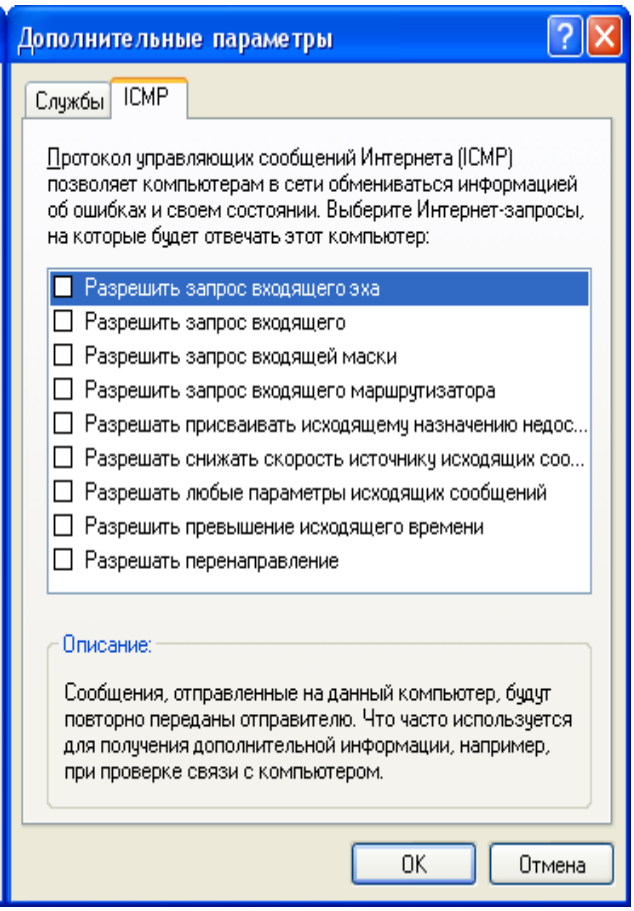


Рис. 18. Параметри відповіді на запити

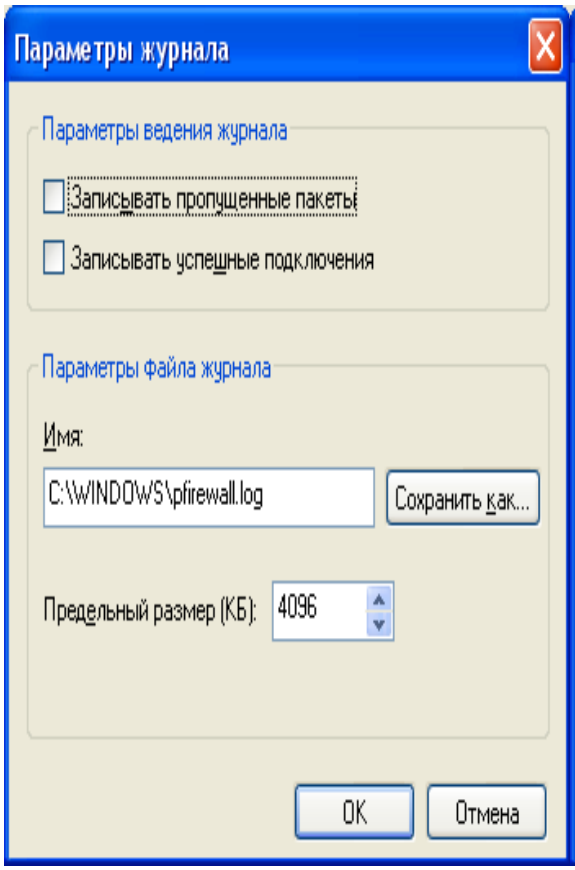


Рис. 19. Параметри журналу безпеки

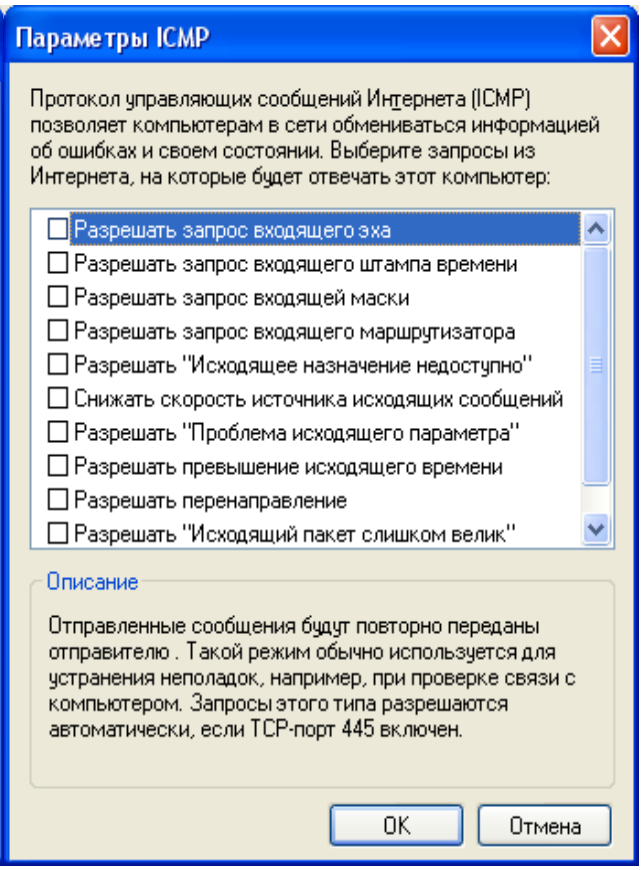


Рис. 20. Параметри відповіді на помилки

1.2. Підключення мереженого принтера

1. Клацнути в панелі завдань на кнопці **Пуск**.
2. Вибрати в головному меню команду **Налагодження → Принтери**.
3. У вікні **Принтери** клацнути на ярличку **Установка принтера** (рис. 21).
4. Далі з'явиться вікно **Майстра установлення** (рис. 22), в якому необхідно клацнути на кнопці **Далі.**
5. У наступному вікні майстра вибрати мережевий принтер і клацнути **Далі**.
6. У наступному вікні клацнути на перемикач **Введіть ім'я принтера** і клацнути подвійним клацанням в полі введення **Ім'я** (рис. 23).
7. Потім вибрати **мережевий** принтер і клацнути **Далі.**
8. У наступному вікні вибрати принтер одного з комп'ютерів мережі й клацнути **Далі,** а в останньому (рис. 24) – **Готово.**

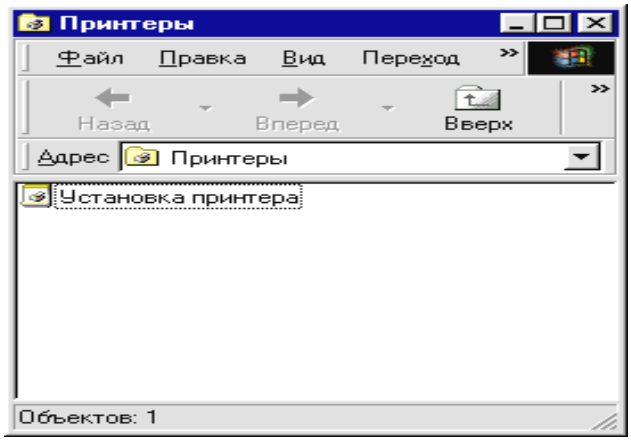


Рис. 21. Вікно установлення принтера

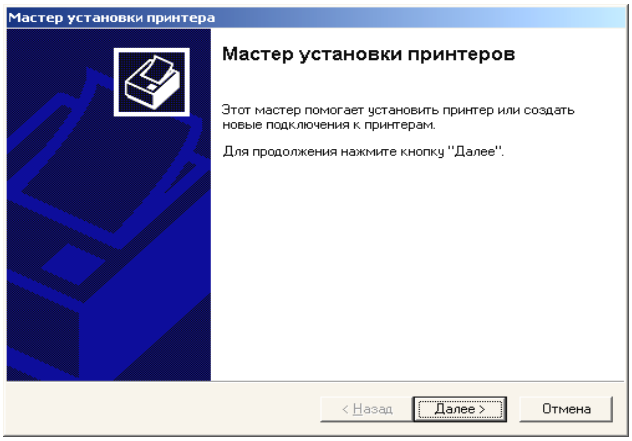


Рис. 22. Вікно майстра установлення принтера

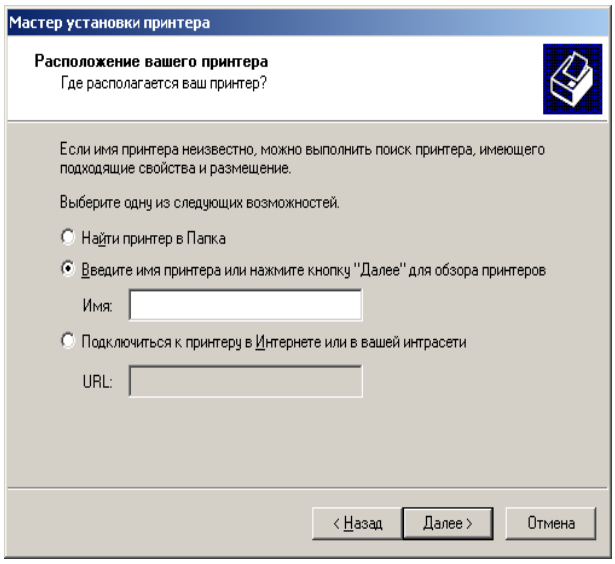


Рис. 23. Вікно введення імені принтера

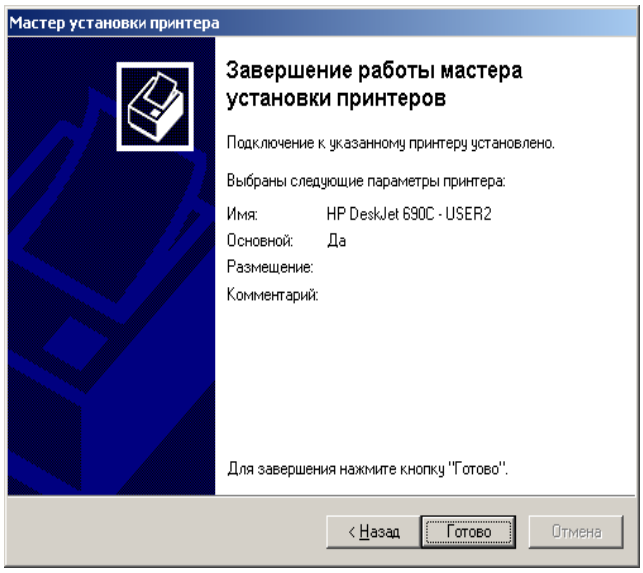


Рис. 24. Вікно завершення роботи майстра

Перевірка підключення мережі

1**.** Клацнути на робочому столі на ярличку **Сетевое окружение** правою кнопкою миші.
2. Вибрати з контекстного меню **Свойства** (рис. 25, 26).

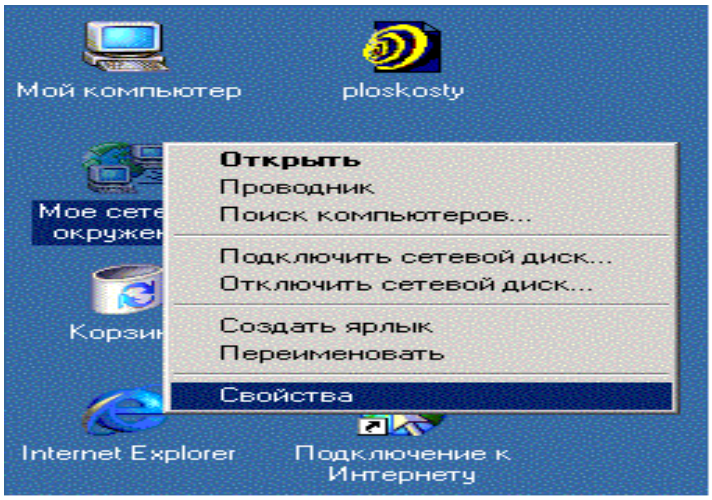


Рис. 25. Вікно контекстного меню

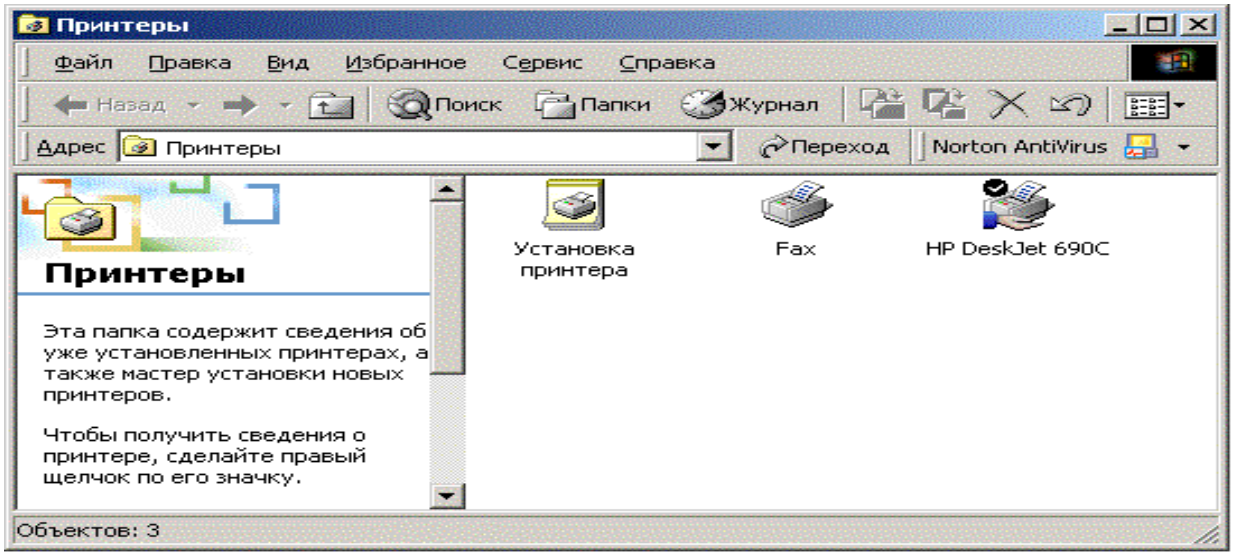


Рис. 26. Вікно властивостей

1. Клацнути у вікні **Мережа і віддалений доступ до мережі** на ярличку **Підключення за локальною мережею** правою кнопкою миші. Вибрати з контекстного меню **Стан** (рис. 27)

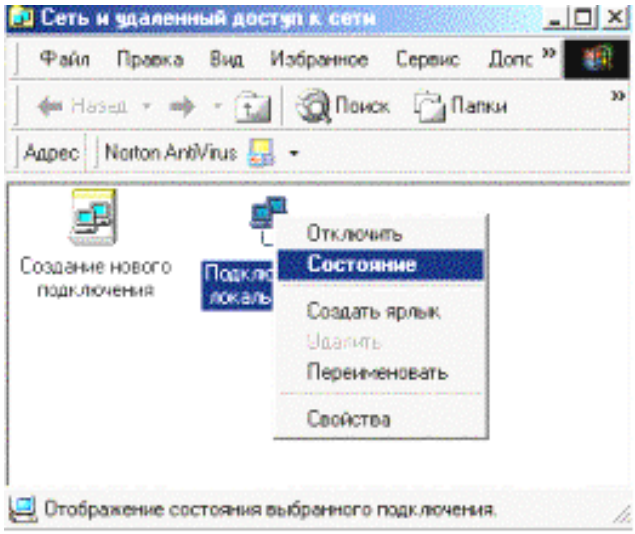


Рис. 27. Вікно вибору стану мережі

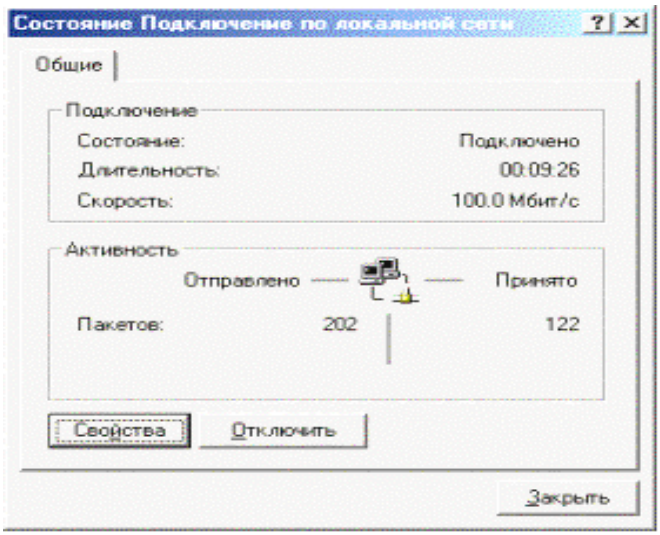


Рис. 28. Вікно перевірки стану мережі

2. Перевірити підключення у вікні, що з’явилося, **Стан підключення за локальною мережею** (рис. 28).
Якщо мережа відключена, то ярличок **Підключення за локальною мережею** буде блідим.

2. Хід виконання роботи

Виконати дії, викладені в розділі 1 Теорія.

3. Контрольні питання

1. З чого почати налагодження параметрів локальної мережі?
2. Як налагодити параметри служб та протоколу TCP/IP?
3. Як налагодити параметри DNS сервера ?
4. Як налагодити параметри захисту комп’ютера в мережі ?

ЛАБОРАТОРНА РОБОТА 6. НАЛАГОДЖЕННЯ БЕЗПРОВОДОВОЇ МЕРЕЖІ

Мета роботи: уміти налагоджувати безпроводову мережу; забезпечувати вхід до мережі комп'ютерів з різними операційними системами.

Зміст

1. Теорія
1.1. Безпроводовий маршрутизатор
1.2. Розміщення безпроводового маршрутизатора
1.3. Безпека безпроводової мережі
2. Хід роботи
2.1. Підключення до безпроводової мережі за допомогою адаптера в ОС Windows 7
2.1.1. Додавання комп'ютерів до мережі
2.1.2. Підключення до мережі за віддаленим з'єднанням.
2.2. Підключення до безпроводової мережі за допомогою модема в ОС Windows XP
3. Контрольні питання

1. Теорія

1.1. Беспроводовий маршрутизатор

Маршрутизатор забезпечує обмін даними між локальною мережею й Інтернетом. Завдяки бездротовому маршрутизатору комп'ютери замість проводів і кабелів з'єднуються з локальною мережею за допомогою радіосигналів. Існує кілька різних типів технологій безпроводових мереж, включаючи стандарти 802.11a, 802.11b і 802.11g. Рекомендується використовувати маршрутизатор, що підтримує стандарт 802.11g, оскільки він забезпечує високу пропускну здатність і потужний радіосигнал.

Рис. 1. Приклад безпроводових роутерів

1.2. Розміщення безпроводового маршрутизатора

Установлювати бездротовий маршрутизатор потрібно у такому місці, де він буде надавати найбільш сильний сигнал при мінімальному рівні перешкод. Для досягнення найкращих результатів виконайте наведені нижче поради.

- Розмістіть безпроводовий маршрутизатор у центрі зони обслуговування. Установіть маршрутизатор якнайближче до центру будинку, щоб забезпечити максимально можливий рівень радіосигналу у всіх приміщеннях будинку.
- Розмістіть бездротовий маршрутизатор вище від підлоги й подалі від стін і металевих предметів, таких як металеві шафи. Чим менше фізичних перешкод між комп'ютером і маршрутизатором, тим більше ймовірність того, що потужність сигналу маршрутизатора буде використовуватися повністю.
- Зменшіть перешкоди. Мережеве встаткування стандарту 802.11g використовує радіочастоти 2,4 Ггц. Цю ж частоту використовують багато мікрохвильових

печей і стільникові телефони. При включенні мікрохвильової печі й виклику за стільниковим телефоном на радіосигнал можуть впливати перешкоди. Уникнути багатьох проблем можна, якщо використовувати стільникові телефон, що працює на більш високій частоті, наприклад 5,8 Ггц.

1.3. Безпека безпроводової мережі

Забезпечення безпеки важливо завжди, але особливо у випадку безпроводової мережі, оскільки сигнал мережі може виходити за межі будинку. Якщо не захищати мережу, то люди, що перебувають поруч, які мають комп'ютер, можуть одержати доступ до інформації, збереженої на мережевих комп'ютерах, і виходити в Інтернет через ваше підключення. Щоб забезпечити безпеку локальної мережі, виконаєте наступні дії.

- Захистіть маршрутизатор, змінивши задані за замовчуванням ім'я користувача й пароль. Багато виробників задають для маршрутизатора ім'я користувача за замовчуванням і пароль, а також ім'я мережі за замовчуванням. Ця інформація може бути використана для одержання несанкціонованого доступу до маршрутизатора. Щоб уникнути цього, необхідно змінити встановлені за замовчуванням ім'я користувача й пароль для маршрутизатора. Звіртеся з документацією обладнання.
- Налаштуйте ключ безпеки мережі. Для налаштування ключа безпеки мережі виконаєте наступні дії.

1. Введіть команду **Пуск/Панель управления/Сеть и Интернет/ Подключение к Интернету.**
2. Клацніть пункт **Создание и настройка новой сети.**
3. Натисніть кнопку **Далее.**

Майстер допоможе створити мережеве ім'я й ключ безпеки. Майстер за замовчуванням запропонує використовувати метод Wi-Fi Protected Access (WPA або WPA2), якщо маршрутизатор підтримує його. За можливістю рекомендується використовувати WPA2, оскільки він забезпечує більш високий рівень безпеки, чому WPA або протокол WEP (Wired Equivalent Privacy). Методи WPA2 або WPA дозволяють також використовувати парольні фрази, що рятує від необхідності запам'ятовувати секретні послідовності букв і цифр.

4. Запишіть ключ безпеки й зберігаєте його в безпечнім місці. Можна також зберегти ключ безпеки на Usb – пристрої дотримуючись вказівок майстра.
5. Використовуйте брандмауера. Брандмауер – це програмне забезпечення або встаткування, що допомагає захистити комп'ютер від зловмисників або шкідливих програм.

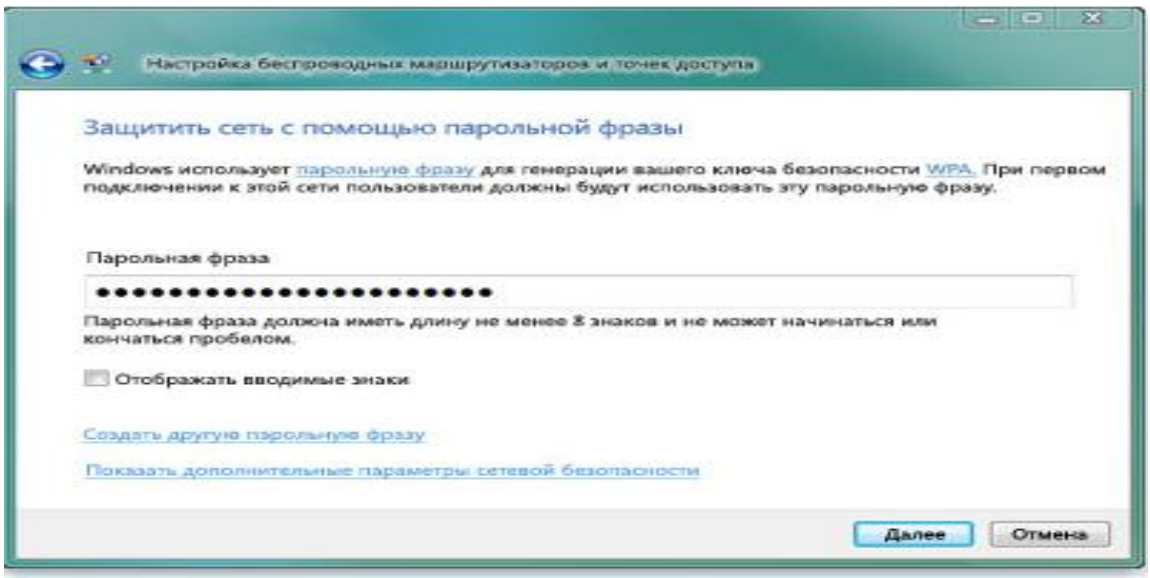


Рис. 2. Створення ключа безпеки мережі

2. Хід роботи

2.1. Підключення до безпроводової мережі за допомогою адаптера в ОС Windows 7

Мережевий адаптер – це обладнання, що з'єднує комп'ютер з локальною мережею. Щоб підключити ноутбук або настільний комп'ютер до безпроводової локальної мережі, необхідний адаптер безпроводової мережі. Багато ноутбуків і настільні комп'ютери оснащені вбудованими адаптерами безпроводової мережі. Щоб перевірити, чи установлений на комп'ютері адаптер безпроводової мережі, виконаєте наступні дії.

1. Введіть команду **Пуск/Панель управления/Система й безпека/Устаткування й звук/Диспетчер обладнань.**
2. З появою запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.
3. Двічі клацніть значок **Сетевые адаптеры** (рис. 3).
4. Знайдіть мережевий адаптер, для роботи в безпроводовій мережі, у нашому випадку це – **Миниплата Dell Wireless 1397 WLAN**

Якщо на комп'ютері не встановлений адаптер безпроводової мережі, його можна купити в магазині, що торгує комп'ютерами або електронною технікою, і встановити самостійно. Рекомендується використовувати адаптери на основі шини USB. Такі адаптери мають малі розміри, їх легко встановлювати й переносити з одного комп'ютера на інший. Перевірте, щоб адаптер того ж типу, що й безпроводовий маршрутизатор. Тип адаптера звичайно зазначений на упаковці.

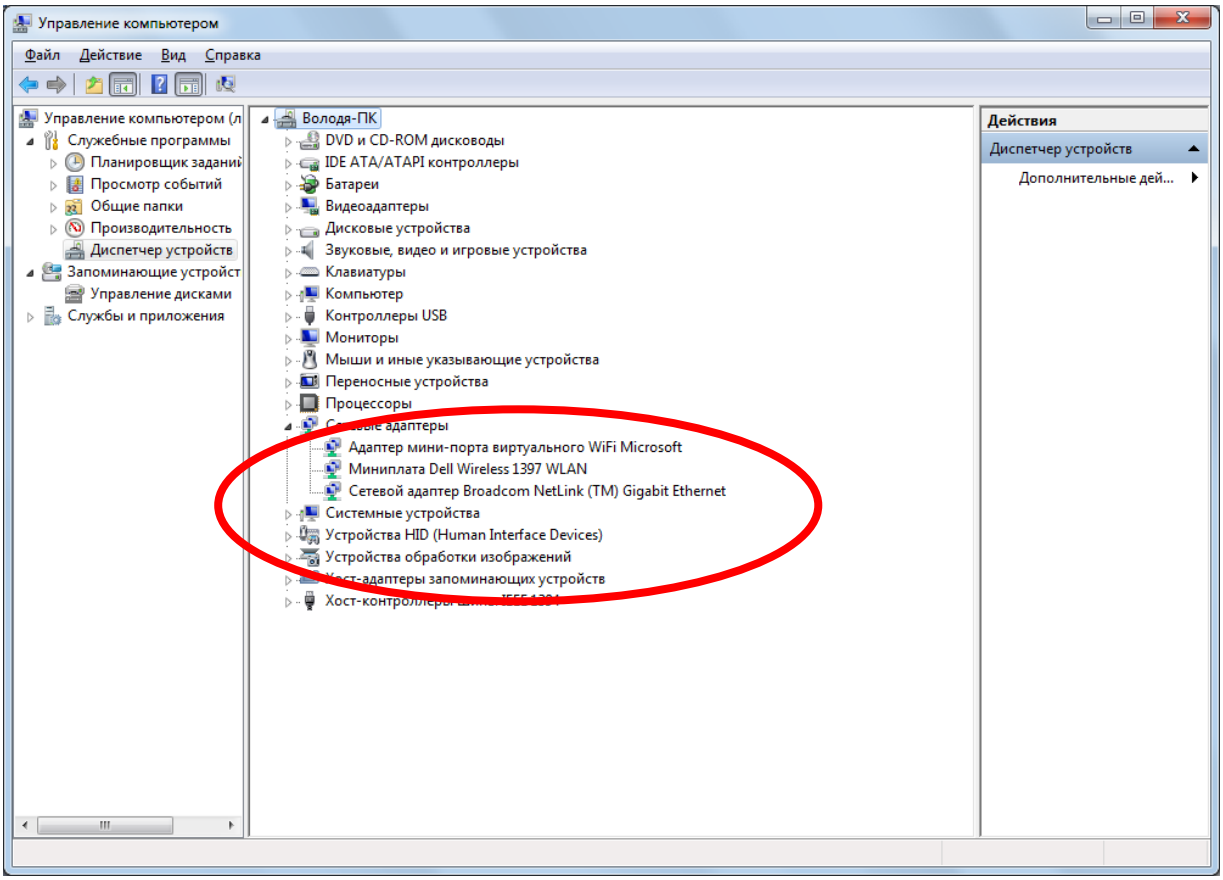


Рис. 3. Мережеві адаптери

2.1.1 Додавання комп'ютерів до мережі

Щоб підключити ноутбук або настільний комп'ютер до безпроводової мережі, необхідно виконати наступні дії.

1. **Пуск/Панель управления/Сеть и Интернет/Подключение к сети** (рис. 4), або натисніть кнопку  **Подключения** на панелі задач.

2. У списку мереж виберіть мережу, до якої потрібно підключитися, і натисніть кнопку **Подключение**.

3. Уведіть ключ безпеки (рис. 5). Можна ввести ключ безпеки вручну або вставити з Usb-Обладнання. Комп'ютер буде автоматично підключено до мережі.

2.1.2. Підключення до мережі за віддаленим з'єднанням.

Для такого з'єднання потрібен модем, який як правило, вставляється в шину USB. Необхідно встановити драйвер модему, який надається при покупці.

Щоб підключити ноутбук або настільний комп'ютер до безпроводової мережі, необхідно виконати наступні дії:

Пуск/Панель управления/Сеть и Интернет/Подключение к Интернету та ввести дані, які отримані від провайдера, за допомогою майстра (рис. 6, 7),

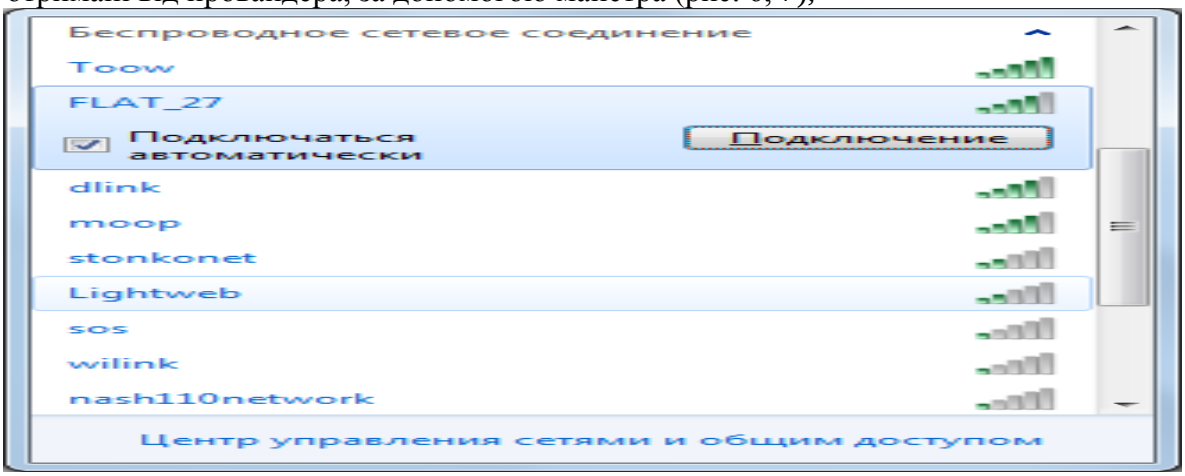


Рис. 4. Список доступних безпроводових мереж

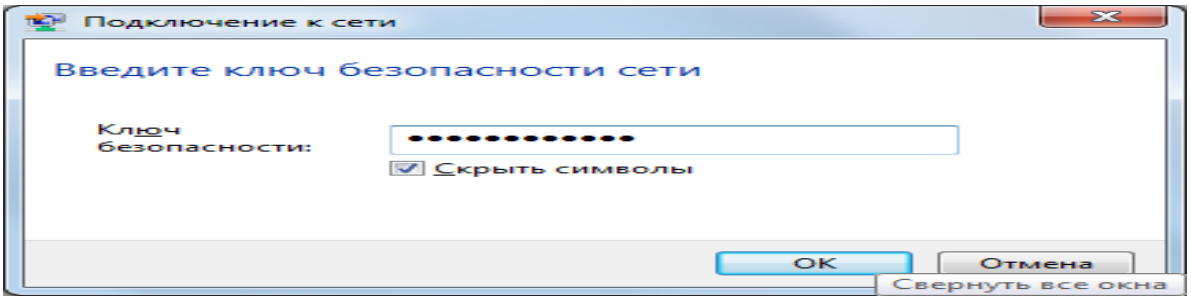


Рис. 5. Ключ мережі

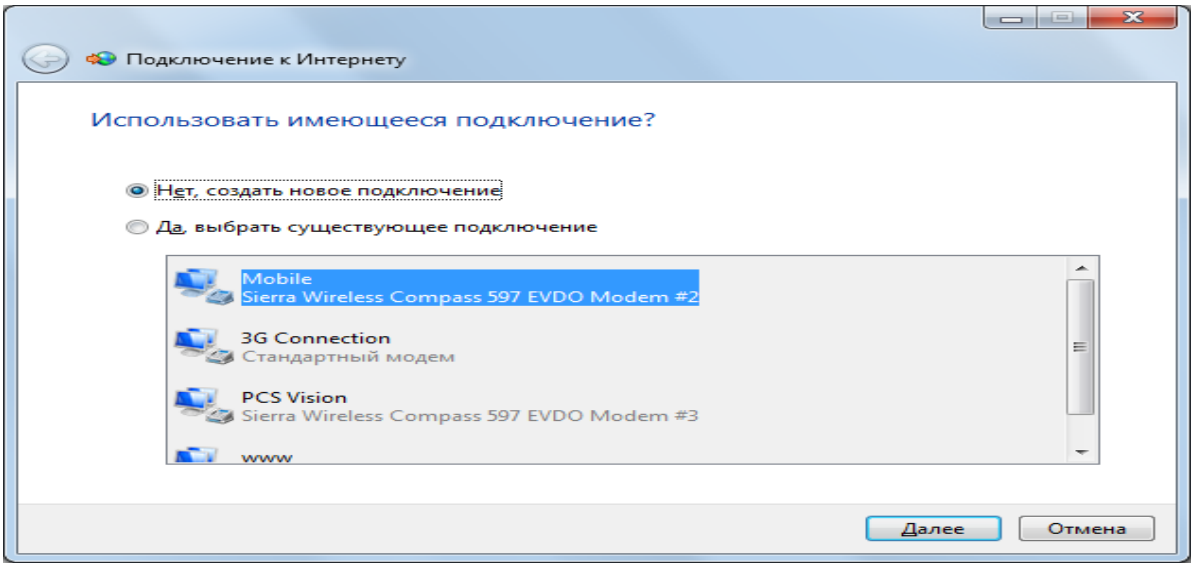


Рис. 6. Вікно майстра підключення

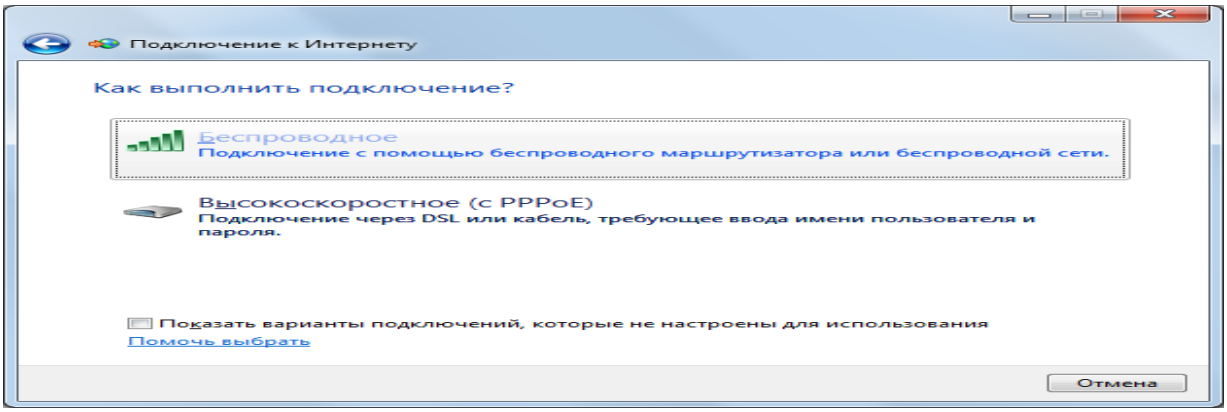


Рис. 7. Вибір безпроводового підключення

(перевірте параметри підключення наведені на рис. 8. встановіть властивості з'єднання).

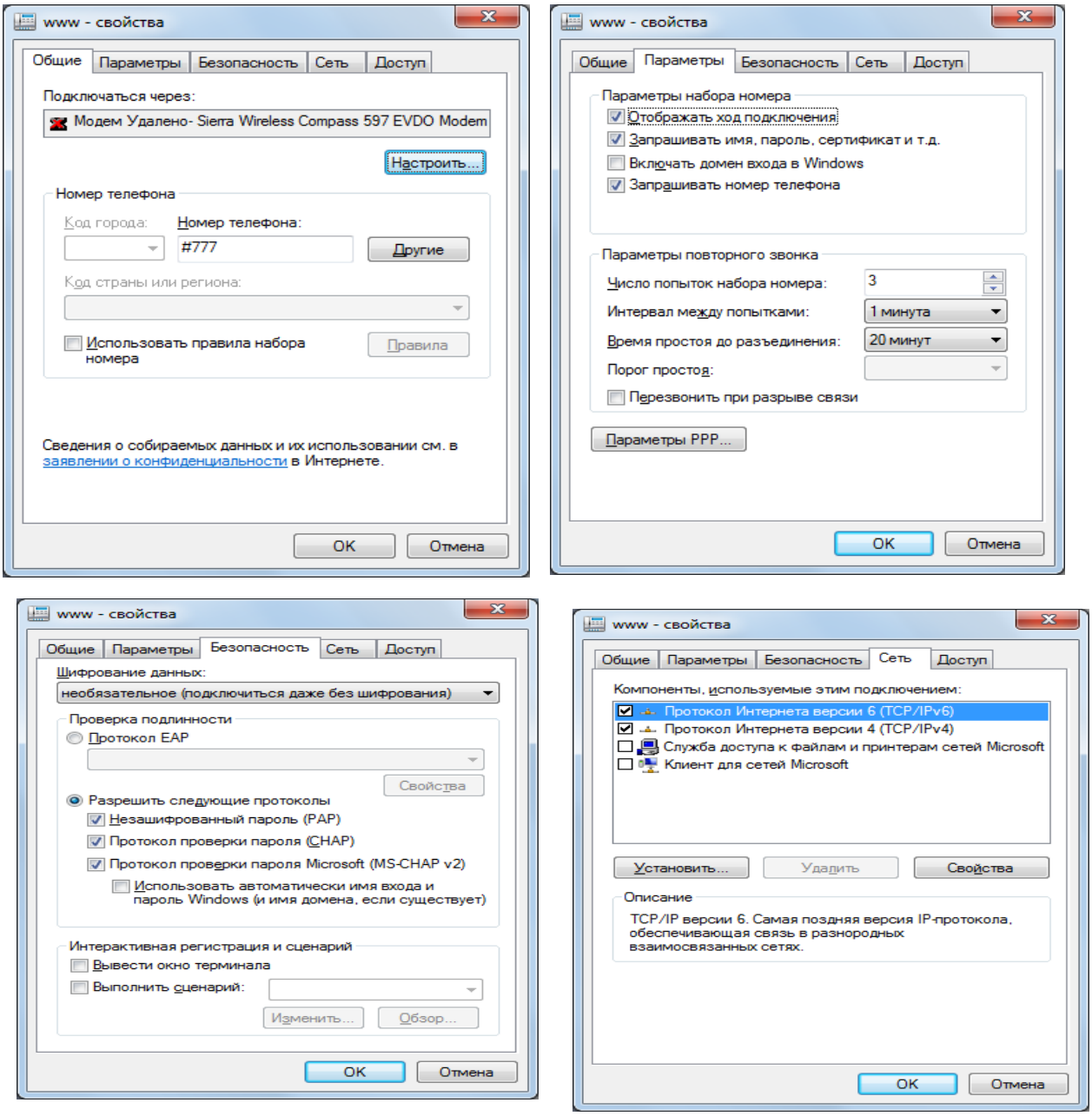


Рис. 8. Параметри підключення

2.2. Підключення до безпроводової мережі за допомогою модему в ОС Windows XP

Для такого з'єднання потрібен модем, який як правило, вставляється в шину USB. Необхідно встановити драйвер модему, який надається при покупці.

Щоб підключити ноутбук або настільний комп'ютер до безпроводової мережі, необхідно виконати наступні дії: **Пуск/Панель управления/Мастер безпроводной сети.** Далі за допомогою майстра (рис. 9) встановити параметри мережі, наприклад, як показано на рис.10.

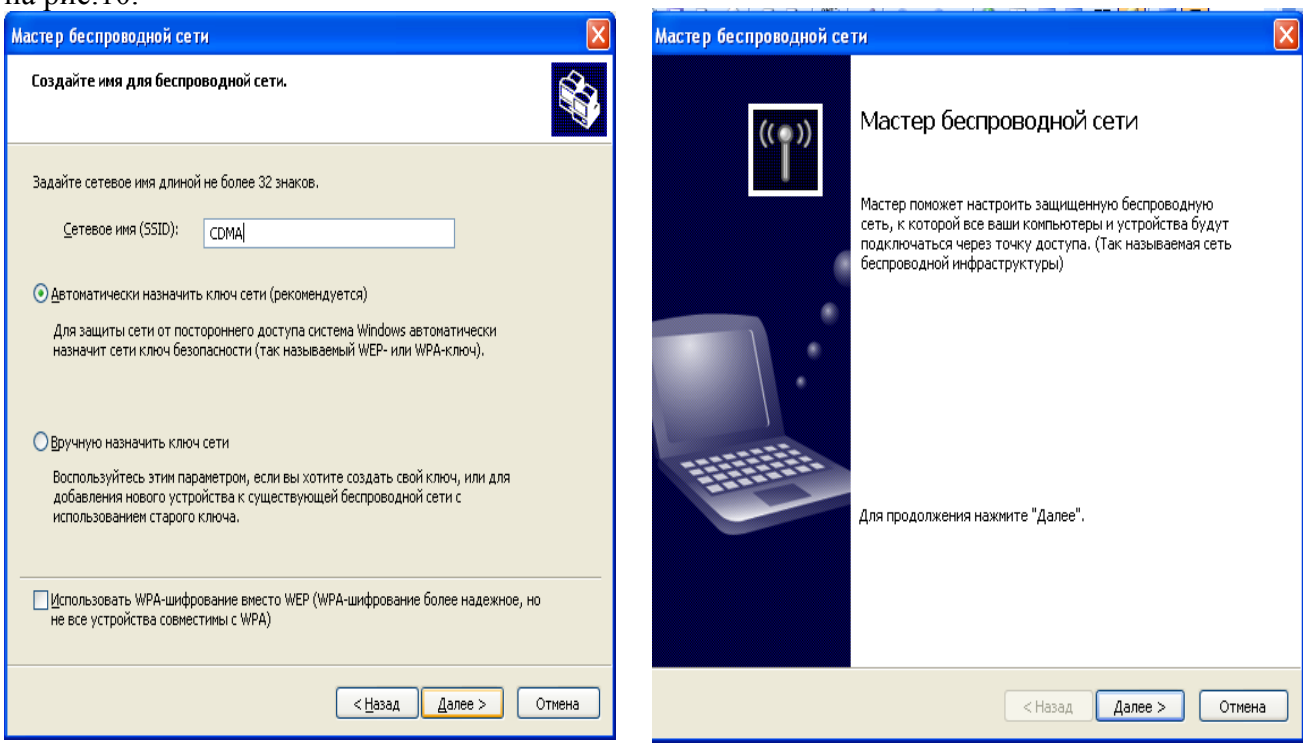
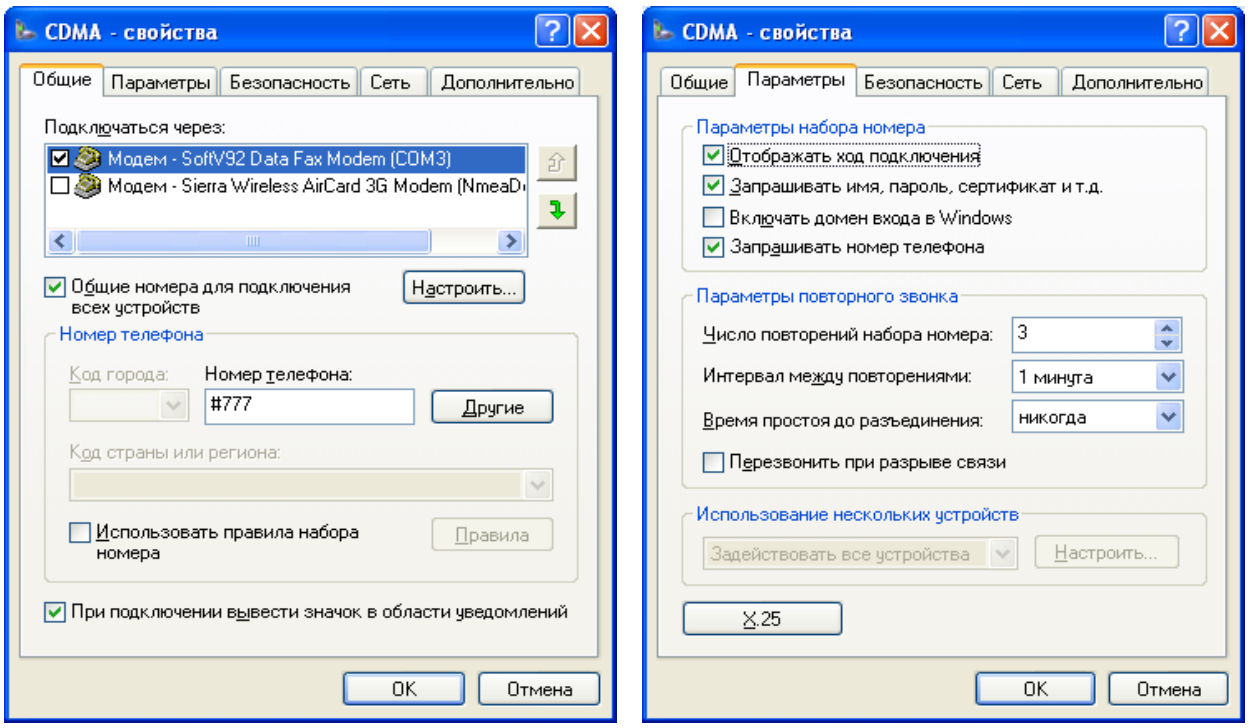


Рис. 9. Майстер встановлення параметрів мережі



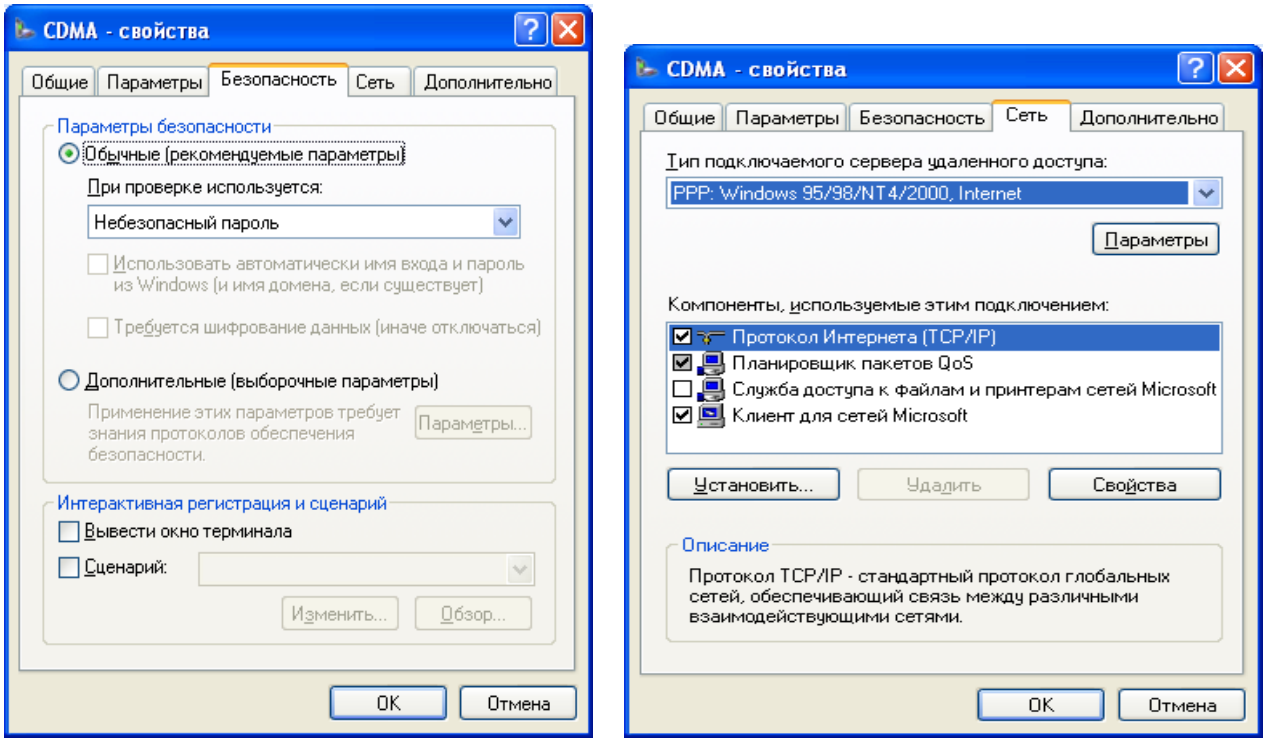


Рис. 10. Параметри підключення

Перевірте параметри підключення, наведені на рис. 10. Встановіть властивості з'єднання.

Вхід до мережі здійснюється командою **Пуск/Доступные подключения/Ім'я мережі.**

4. Контрольні питання

1. Призначення та встановлення безпроводового маршрутизатора.
2. Як забезпечити безпеку безпроводової мережі?
3. Як встановити наявність мережевих адаптерів на комп'ютері?
4. Як підключитися до безпроводової мережі за допомогою адаптера в ОС Windows 7?
5. Як підключитися до мережі за віддаленим з'єднанням в ОС Windows 7?
6. Як підключитися до мережі за віддаленим з'єднанням в ОС Windows XP?

АБОРАТОРНА РОБОТА 7. НАЛАГОДЖЕННЯ В ЛОКАЛЬНІЙ МЕРЕЖІ ТА РОБОТА З РІЗНИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ.

Мета роботи: навчитись налагоджувати параметри локальної мережі; керувати доступом до каталогів та файлів; використовувати інспектора ресурсів; працювати з різним програмним забезпеченням.

Зміст

1. Теорія
1.1. Мережа Windows.
1.2. Об'єднання в мережу домашніх комп'ютерів, що працюють під керуванням різних версій Windows
1.3. Пошук імені та Ір-Адреси комп'ютера
1.4. Призначення загального каталогу
1.5. Підключення принтера.
1.6. Установлення мережевого диска
1.7. Визначення завантаження ресурсів комп'ютера та мережі
1.8. Приклади роботи у локальній мережі Windows за допомогою різноманітного програмного забезпечення
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Домашня мережа Windows

Робота мережі забезпечується програмами операційних систем Windows 3.X, Windows 95, Windows 98, Windows NT, Milenium, Windows 2000, Windows XP, Windows 7, Windows 8, Windows 10. Як правило, відразу при запуску системи машина автоматично запитує Login name (те ж саме, що і user ID) і пароль.

Що потрібно для створення домашньої мережі

Різноманіття встаткування для домашньої мережі може ускладнити вибір при покупці. Перш ніж віришити, яке встаткування придбати, необхідно вибрати тип мережевої технології (способу, яким комп'ютери підключаються й обмінюються один з одним даними в мережі).

Мережеві технології

Найпоширенішими мережевими технологіями є бездротова технологія, Ethernet, HomePNA і Powerline. При виборі мережевої технології враховуються розташування комп'ютерів і бажана швидкість мережі. Вартість цих технологій приблизно однакова. Ці технології розглянуті нижче.

Беспроводова технологія

Для обміну даними між комп'ютерами в бездротовій мережі використовуються радіохвилі. Найпоширенішими стандартами безпроводових мереж є 802.11b, 802.11g і 802.11a. Новий стандарт 802.11n стає усе більш популярним (табл. 1).

Таблиця 1

Короткі характеристики стандартів безпроводових мереж

Швидкість	• 802.11b: максимальна швидкість передачі даних становить 11 мегабіт у секунду (Мбіт/с). Завантаження фотографії розміром 10 мегабайт (МБ) з Інтернету в оптимальних умовах триватиме 7 секунд. • 802.11g: максимальна швидкість передачі даних становить 54 Мбіт/с. Завантаження фотографії розміром 10 мегабайт (МБ) з Інтернету в оптимальних умовах триватиме 1,5 секунди. • 802.11a: максимальна швидкість передачі даних становить 54 Мбіт/с. Завантаження фотографії розміром 10 мегабайт (МБ) з Інтернету в оптимальних умовах триватиме 1,5 секунди.

	• 802.11n: залежно від кількості потоків даних, яке підтримує встаткування, стандарт 802.11n теоретично може передавати дані зі швидкістю 150 Мбіт/з, 300 Мбіт/з, 450 Мбіт/з і 600 Мбіт/с. Примітка. Зазначений час завантаження файлу має на увазі ідеальні умови. Вони не завжди досяжні при звичайних обставинах через відмінність устаткування, веб-серверів, мережі, трафіку і т.д.

Ethernet

Для обміну даними між комп'ютерами в мережі Ethernet використовуються Ethernet-кабелі (табл. 2)

Таблиця 2

Короткі характеристики Ethernet-кабелів

Швидкість	Залежно від типу використовуваного кабелю швидкість передачі даних у мережах Ethernet становить 10, 100 або 1000 Мбіт/с. Найбільш швидким є Gigabit Ethernet, швидкість передачі даних якого становить до 1 гігабіта в секунду (1000 Мбіт/с). Наприклад, завантаження фотографії розміром 10 мегабайт (МБ) може займати при оптимальних умовах зв'язку близько 8 секунд у мережі зі швидкістю 10 Мбіт/з і менш 1 секунди в мережі зі швидкістю 100 Мбіт/с.
Позитивні сторони	• Мережі Ethernet недорогі й швидкі.
Недоліки	• Ethernet-Кабелі повинні бути протягнені між кожним комп'ютером і концентратором, комутатором або маршрутизатором, що може зайняти багато часу. Крім того, можуть виникнути складності при прокладанні кабелю, якщо комп'ютери перебувають у різних кімнатах.

HomePNA

Для обміну даними між комп'ютерами в мережі Homepna використовуються кабелі домашніх телефонних ліній (табл. 3).

Таблиця 3

Короткі характеристики кабелів домашніх телефонних ліній

Швидкість	Homepna 2.0 дозволяє передавати дані зі швидкістю до 10 Мбіт/с. Homepna 3.0 дозволяє передавати дані зі швидкістю до 128 Мбіт/с. Наприклад, завантаження фотографії розміром 10 мегабайт (МБ) займає при оптимальних умовах зв'язку близько 8 секунд у мережі Homepna 2.0 і близько 1 секунди в мережі Homepna 3.0.
Позитивні сторони	• Технологія Homepna використовує існуючі телефонні проведення. • Для з'єднання більш двох комп'ютерів у мережі Homepna не потрібні концентратори або комутатори.
Недоліки	• Телефонні розетки повинні бути в кожній кімнаті, де є комп'ютер, і всі вони повинні бути підключені до одній телефонній лінії.

Powerline

Для обміну даними між комп'ютерами в мережі Powerline використовуються кабелі домашніх електричних ліній (табл. 4).

Таблиця 4

Короткі характеристики кабелів домашніх електричних ліній

Швидкість	Мережа Powerline може передавати дані зі швидкістю до 200 Мбіт/с. Наприклад, у мережі Powerline завантаження фотографії розміром 10 мегабайт (МБ) з Інтернету в оптимальних умовах займає менше секунди.
Позитивні сторони	• Технологія Powerline використовує існуючі електричні проведення. • Для з'єднання більш двох комп'ютерів у мережі Powerline не потрібні концентратори або комутатори.
Недоліки	• Необхідна електрична розетка в кожній кімнаті, де буде розташований комп'ютер. • На мережі Powerline можуть впливати перешкоди й «шум» електролінії.

Необхідне встаткування

Існує кілька видів устаткування, використовуваного в домашніх мережах.

- Мережеві адаптери. Ці адаптери (також називані мережевими інтерфейсними платами (NIC)) підключають комп'ютери до мережі, щоб ті могли обмінюватися даними. Мережевий адаптер можна підключити до порту USB або Ethernet на комп'ютері або встановити усередині комп'ютера у вільне гніздо розширення PCI.
- Мережеві концентратори й комутатори. Концентратори й комутатори підключають два або більше число комп'ютерів до мережі Ethernet. Комутатор коштує ледве дорожче концентратора, але він швидше працює.

Концентратор Ethernet

- Маршрутизатори й крапки доступу. Маршрутизатори з'єднують комп'ютери й мережі один з одним (наприклад, за допомогою маршрутизатора можна підключити домашню мережу до Інтернету). Маршрутизатори також дозволяють декільком комп'ютерам використовувати одне підключення до Інтернету. Маршрутизатори можуть бути кабельними або бездротовими. Необхідності у використанні маршрутизатора в провідній мережі немає, але рекомендується його застосовувати при загальнім підключенні до Інтернету. Для спільного підключення до Інтернету через бездротову мережу необхідний бездротовий маршрутизатор. Крапки доступу дозволяють комп'ютерам і обладнанням підключатися до бездротової мережі.
- Модеми. Комп'ютери використовують модеми для передачі й одержання інформації через телефонні або кабельні лінії. Для підключення до Інтернету потрібний модем. Деякі постачальники кабельного телебачення надають кабельний модем – безкоштовно або за гроші – при замовленні кабельного інтернет-підключення. Також доступні обладнання, що поєднують функції модему й маршрутизатора.

Кабельний модем

- Мережеві кабелі (Ethernet, Homepna і Powerline). Мережеві кабелі з'єднують комп'ютери один з одним або з відповідним устаткуванням, таким як концентратори, маршрутизатори й зовнішні мережеві адаптери. Адаптери Homepna і Powerline звичайно зовнішні й підключаються до комп'ютера за допомогою кабелів Ethernet або USB (залежно від типу адаптера).

У наступній таблиці 5 перераховане встаткування, необхідне для кожного типу мережевих технологій.

Таблиця 5

Устаткування, необхідне для кожного типу мережевих технологій

Технологія	Устаткування	Кількість
Бездротовий адаптер	Адаптер бездротової мережі	Один для кожного комп'ютера в мережі (звичайно вони вбудовані в ноутбуки)
	Крапка доступу або бездротовий маршрутизатор (рекомендується)	Один
Ethernet	Мережевий адаптер Ethernet	Один для кожного комп'ютера в мережі (звичайно вони вбудовані в настільні комп'ютери)
	Концентратор або комутатор Ethernet (необхідний тільки при підключенні більш двох комп'ютерів і спільному підключенні до Інтернету)	Один (найкраще використовувати концентратор або комутатор 10/100/1000, що має достатню кількість портів для підключення всіх комп'ютерів до мережі)
	Маршрутизатор Ethernet (необхідний тільки при підключенні більш двох комп'ютерів і спільному підключенні до Інтернету)	Один (може знадобитися додатковий концентратор або комутатор, якщо в маршрутизатора недостатньо портів для всіх комп'ютерів)
	Ethernet-Кабель	Один для кожного комп'ютера, що підключається до мережевого концентратора або комутатора (рекомендуються кабелі 10/100/1000 категорії 6, але їх використання необов'язкове)
	Кросировочний кабель (необхідний тільки при прямім з'єднанні двох комп'ютерів, без допомоги концентратора, комутатора або маршрутизатора)	Один
Homepna	Адаптер Homepna	По одному для кожного комп'ютера в мережі
	Маршрутизатор Ethernet	Один, якщо потрібний загальний доступ до Інтернету
	Телефонні кабелі	По одному для кожного комп'ютера в мережі (використовуйте стандартний телефонний кабель, щоб підключити комп'ютери до телефонних розеток)
Powerline	Мережевий адаптер Powerline	По одному для кожного комп'ютера в мережі
	Маршрутизатор Ethernet	Один, якщо потрібний загальний доступ до Інтернету
	Електрична проводка в будинку	По одній електричній розетці для кожного комп'ютера в мережі

Рекомендується перевірити, які мережеві адаптери встановлені на комп'ютерах (якщо вони встановлені). Можна використовувати технологію, для якої є більша частина встаткування, або обновити встаткування. Комбінація різних технологій може бути кращим

варіантом. Наприклад, багато використовують бездротової маршрутизатор, використовуваний для провідних Ethernet-Підключень настільних комп'ютерів і безпроводових підключень ноутбуків.

Якщо мережа кабельна, підключення буде встановлено відразу після приєднання Ethernet кабелів. Якщо використовується бездротова мережа, запустіть на комп'ютері, підключеному до маршрутизатора, майстер установки маршрутизатора бездротової мережі або крапки доступу до бездротової мережі (див. лаб. роб. 6).

1.2. Об'єднання в мережу домашніх комп'ютерів, що працюють під управлінням різних версій Windows

Які відмінності між Windows XP і Windows Vista Windows 7 (табл. 6).

Таблиця 6

Основні відмінності в технології мереж між Windows XP, Windows Vista і Windows 7

Елемент	Windows XP	Windows Vista	Windows 7
Ім'я робочої групи за замовчуванням	Mshome в Windows XP Home Edition, WORKGROUP - у всіх інших версіях	WORKGROUP	WORKGROUP
Ім'я загальної папки	Загальні документи	Загальна папка	Публічні документи, загальна музика, загальні малюнки, загальні відео
Простий загальний доступ до файлів	Дозволений за замовчуванням	За замовчуванням не дозволений; для доступу до загальних папок, (якщо загальний доступ наданий), потрібне ім'я користувача й пароль	За замовчуванням не дозволений; для доступу до загальних папок, (якщо загальний доступ наданий), потрібне ім'я користувача й пароль
Виявлення комп'ютерів у мережі й доступ до них	Тільки для комп'ютерів з тієї ж робочої групи	Для всіх комп'ютерів у мережі незалежно від установленої на них операційної системи й приналежності до робочої групи	Для всіх комп'ютерів у мережі незалежно від установленої на них операційної системи й приналежності до робочої групи
Homegroup	Недоступна	Недоступна	Доступно в домашніх мережах. Компонент «Домашня група» доступний у всіх випусках Windows 7. У випусках Windows 7 Starter і Windows 7 Home Basic можна приєднатися до домашньої групи, але не можна її створити.

Елемент	Windows XP	Windows Vista	Windows 7
Місце, де можна змінити параметри й властивості	Мережеве оточення	Центр керування мережами й загальним доступом	Центр керування мережами й загальним доступом
Елементи керування мережею	У різних місцях у межах операційної системи	Переважно в Центрі керування мережами й загальним доступом	Усі елементи розташовані в Центрі керування мережами й загальним доступом

Якщо мережа містить комп'ютери під керуванням різних версій Windows, помістіть всі комп'ютери в одну робочу групу.

Наступним кроком після установки мережі є її більш точне налаштування, щоб усі комп'ютери могли виявляти один одного; це необхідно, якщо планується надання загального доступу до файлів і принтерів.

Якщо в мережі є комп'ютери під керуванням Windows XP, важливо використовувати одне ім'я робочої групи для всіх комп'ютерів у мережі. Це дозволить комп'ютерам під керуванням різних версій Windows виявляти один одного й надавати взаємний доступ. Пам'ятайте, що ім'я робочої групи за замовчуванням – не те саме у всіх версіях Windows.

Щоб визначити або змінити ім'я робочої групи комп'ютера під керуванням Windows XP, виконаєте наступні дії.

1. Натисніть **Пуск**, клацніть правою кнопкою миші **Мой компьютер** і виберіть **Свойства**.
2. У вікні **Свойства** системи перейдіть на вкладку **Имя компьютера**, де відображається ім'я робочої групи. Щоб змінити ім'я, клацніть **Изменить**, у поле **Имя компьютера** введіть нове ім'я, а потім клацніть **ОК**.

Щоб визначити ім'я робочої групи комп'ютера під керуванням Windows Vista або Windows 7, виконаєте наступні дії.

Щоб змінити ім'я робочої групи комп'ютера під керуванням Windows Vista або Windows 7, виконаєте наступні дії.

1. Введіть команду **Пуск/Панель управления/Система и безопасность/Система** (рис. 1)
2. У групі **Имя компьютера**, **Имя домену и параметры робочей группы** натисніть кнопку **Изменить параметры**.
3. У вікні **Свойства** системи на вкладці **Имя компьютера** клацніть **Изменить**.
4. У діалоговім вікні Зміна імені комп'ютера або домену в поле робоча група введіть нове ім'я робочої групи й клацніть **ОК**. Буде запропоновано перезавантажити комп'ютер.

Установіть тип мережевого розміщення. Потім перевірте мережеве розміщення всіх комп'ютерів під керуванням Windows Vista або Windows 7. Мережеве розміщення – це параметр, який дозволяє системі Windows автоматично набудовувати безпеку й інші параметри з урахуванням типу мережі, до якої підключений комп'ютер.

Типи мережевого розміщення

Існує чотири типи мережевого розміщення.

- Домашній. Комп'ютер підключений до мережі, що забезпечує деякий рівень захисту від Інтернету (наприклад, маршрутизатор і брандмауер) що складається з відомих або довірених комп'ютерів. Більшість домашніх мереж відноситься до цієї категорії. Домашня група доступна в мережах з домашнім мережевим розміщенням.
- Робочий. Комп'ютер підключений до мережі, що забезпечує деякий рівень захисту від Інтернету (наприклад, маршрутизатор і брандмауер), що складається з відомих або довірених комп'ютерів. До цієї категорії відноситься більшість невеликих мереж підприємств.
- Загальний. Комп'ютер підключений до мережі, доступної для загального використання. Прикладом загальнодоступних мереж є публічні мережі для доступу в Інтернет, наприклад в аеропортах, бібліотеках і кафе.
- Домен. Комп'ютер підключений до мережі, до складу якої входить контролер домену Active Directory. Прикладом доменної мережі є мережа на робочому місці. Це мережеве розміщення недоступне як варіант вибору й повинне налаштовуватися адміністратором домену.

Переконаєтеся, що в домашній мережі для типу мережевого розміщення встановлене значення «Домашній». Це можна зробити в такий спосіб.

Тип мережевого розміщення відображається в Центрі керування мережами й загальним доступом.

Якщо встановлений загальний тип мережевого розміщення, клацніть Публічна мережа й виберіть необхідний тип розміщення мережі.

Попередження

- Типи «Домашній» і «Робітник» слід використовувати тільки для відомих і довірених мереж, таких як домашня мережа або невелика мережа підприємства. Установка значення «Домашній» або «Робітник» для мережі в громадському місці може являти загрозу безпеки, оскільки дозволяє іншим користувачам мережі бачити ваш комп'ютер.

Переконаєтеся, що брандмауер надає загальний доступ до файлів і принтерів

Якщо використовується брандмауер Windows, цей розділ можна пропустити, оскільки брандмауер Windows автоматично відкриває порти, необхідні для надання загального доступу до файлів і принтерам при використанні спільного доступу або після включення виявлення мережі.

Для виявлення комп'ютерів під керуванням Windows Vista або Windows 7 відкрийте наступні порти:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Для виявлення комп'ютерів під керуванням більш ранніх версій Windows і використання загального доступу до файлів і принтерам з будь-якою версією Windows відкрийте наступні порти:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

Для виявлення мережевих обладнань відкрийте наступні порти:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355

- TCP 5357
- TCP 5358

Щоб домашня група правильно функціонувала між комп'ютерами під керуванням Windows 7, відкрийте наступні порти:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 1900
- TCP 2869
- TCP 3587
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Включення додаткових параметрів загального доступу до файлів і принтерів

При зміні типу мережевого розміщення на «Домашній» або «Робітник» виявлення мережі включається автоматично. Крім того, що випливають параметри загального доступу можна включити окремо:

- Виявлення мережі
- Загальний доступ до файлів (в Windows 7 включається автоматично при наданні загального доступу до файлу або папки)

Після включення цих параметрів на комп'ютері будуть доступні наступні можливості.

- Виявлення інших комп'ютерів і обладнань у домашній мережі й доступність для виявлення іншими комп'ютерами
- Загальний доступ до файлів і папкам
- Надання загального доступу до загальних папок

1.3. Пошук імені та Ір-Адреси комп'ютера

Увівши команду **Свойства** на піктограмі комп'ютер на робочому столі або провіднику можна визначити ім’я, параметри: комп'ютера, операційної системи, та робочу групу куди він входить (рис. 1).

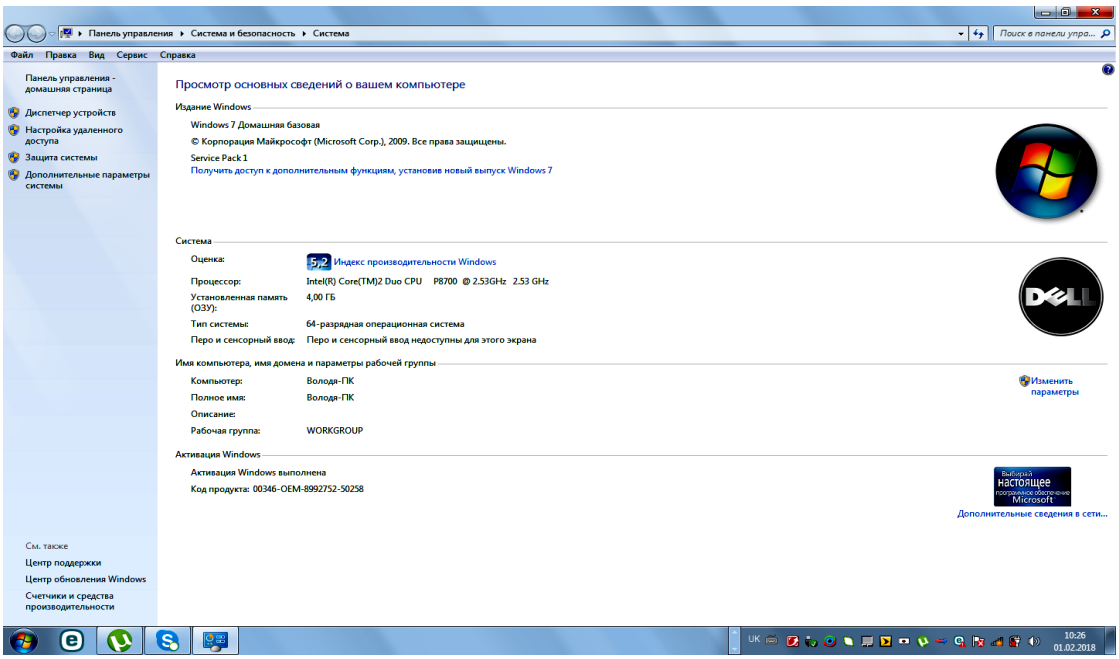


Рис. 1. Параметри комп'ютера

Для одержання доступу до мережі двічі клацніть піктограму **Сетевое окружение** на робочому столі, а потім двічі клацніть значок комп'ютера. Якщо потрібного комп'ютера немає в списку, двічі клацніть піктограму **Вся сеть**.

Натисніть кнопку **Пуск**, виберіть команду **Найти**, а потім виберіть **Компьютер**. Якщо відомо ім'я комп'ютера, запишіть його в поле Ім'я. Наприклад, marketing.

1. Виберіть активне мережеве підключення й у панелі інструментів клацніть **Просмотр состояния подключения.** (Можливо, знадобиться клацнути значок подвійних лапок, щоб знайти цю команду.)
2. Клацніть Таблиця.Ip-Адреса комп'ютера відобразиться в стовпці значень напроти Ipv 4-адреси (рис. 2).

Інша можливість: Натисніть правою кнопкою миші на мережевому підключенні і з контекстного меню виберіть команду **Состояние** (див лаб. 4). Виберіть підключення до мережі та натисніть на клавішу **Enter**.

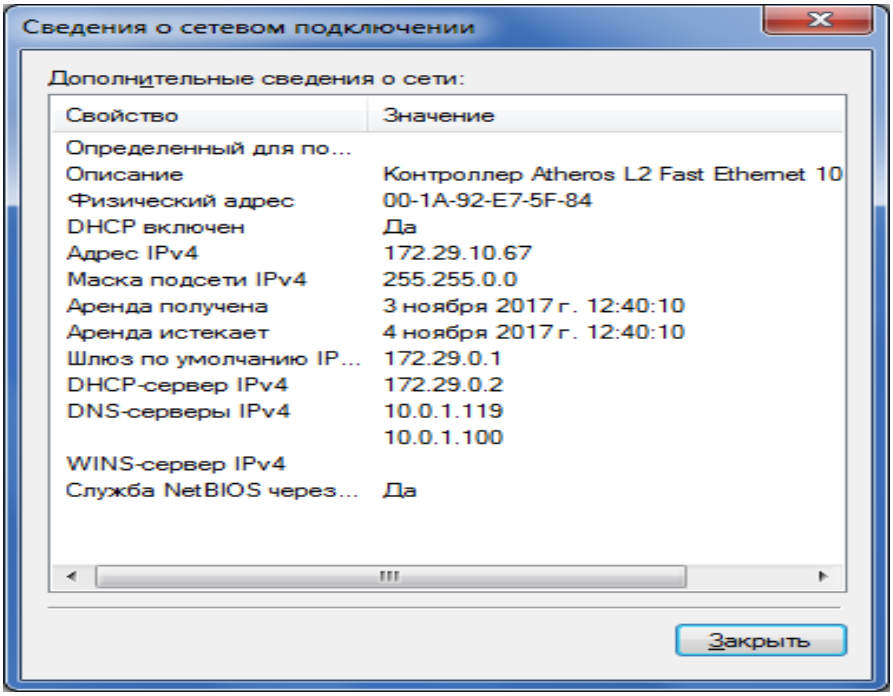


Рис. 2. Таблиця Ip-Адреса комп'ютера

Використання засобів командного рядка для одержання відомостей про мережу

Для швидкого одержання інформації про комп'ютер і мережу, а також для діагностики неполадок у мережі можна скористатися засобами командного рядка.

Для визначення імені комп'ютера у командному рядку введіть hostname і натисніть клавішу Enter.

Для визначення IP-адреси комп'ютера у командному рядку введіть ipconfig і натисніть клавішу Enter.

Для визначення фізичної адреси у командному рядку введіть ipconfig /all і натисніть клавішу Enter.

Якщо на комп'ютері встановлене більше одного мережного адаптера, будуть виведені фізичні імена окремо для кожного адаптера.

Для отримання нової IP-адреси якщо в мережі використовується протокол Dynamic Host Configuration Protocol (DHCP) необхідно:

1. У командному рядку введіть **ipconfig /release** і натисніть клавішу **Enter**.

Це звільняє поточну Ip-Адресу.

2. Для одержання нової Ip-Адреси введіть у командному рядку **ipconfig /renew** і натисніть клавішу **Enter**.

Конфігурація DHCP буде оновлена для всіх адаптерів. Для відновлення Ip-Адреси конкретного адаптера введіть його ім'я, яке можна довідатися, написавши ipconfig у командному рядку. Це може знадобитися, якщо виникли проблеми з підключенням.

1.4. Призначення загального каталогу

У вікні **Мой компьютер** або в провіднику Windows виберіть каталог, що потрібно зробити загальним. У контексно-залежному меню виберіть команду **Свойства та вкладку доступ** (рис. 3).

Виберіть параметр **Общий ресурс**. Виберіть тип доступу в групі **Тип доступа** і, при необхідності, уведіть пароль.

Домашні групи забезпечують швидкий і зручний спосіб автоматичного надання загального доступу до музики, зображень і чимало іншого. Як щодо файлів і папок, загальний доступ до яких не надається автоматично?

Саме для цього створене нове меню **Общий доступ** (рис. 4).

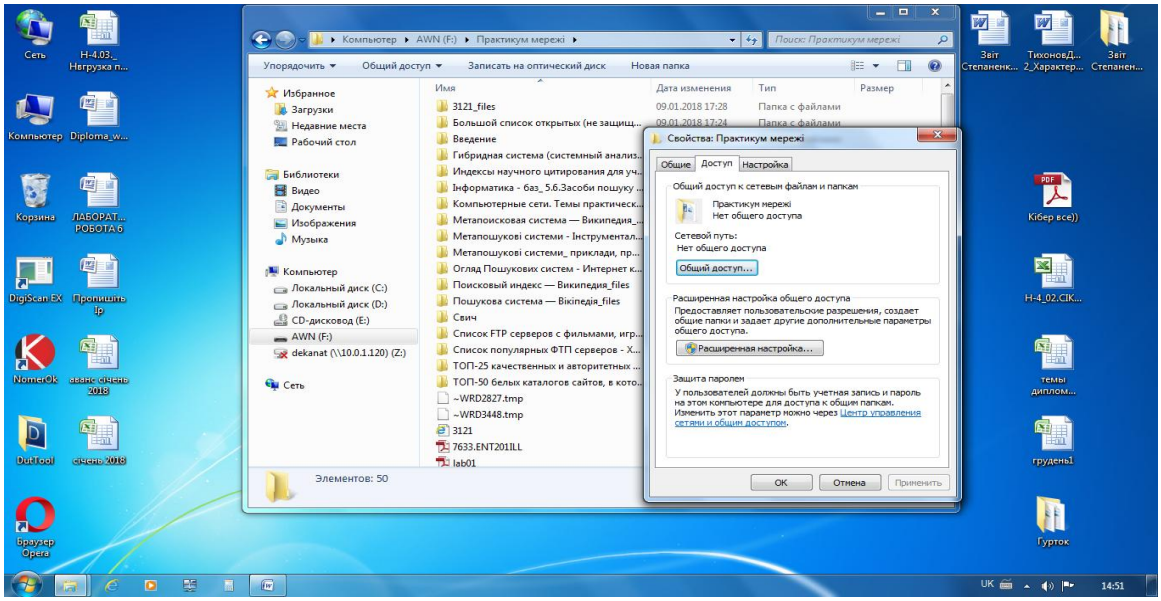


Рис. 3. Вкладка доступ

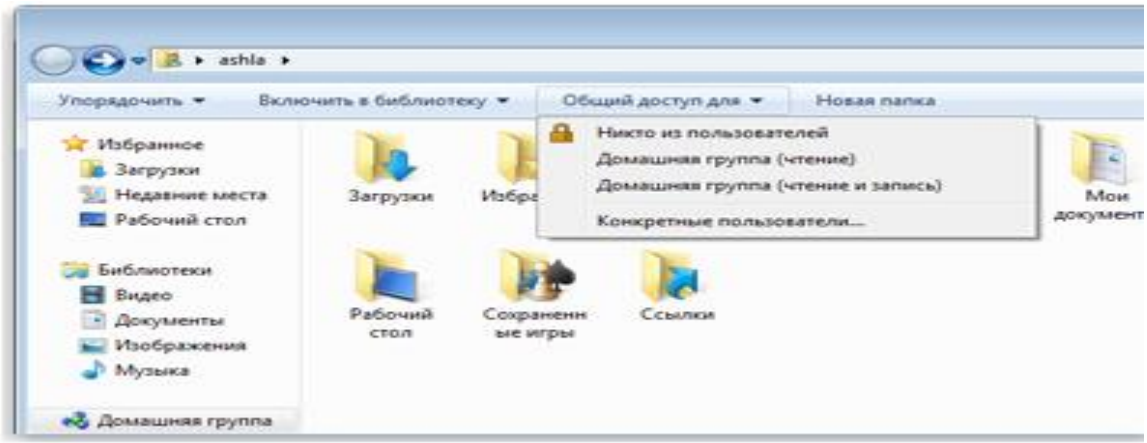


Рис. 4. Меню загальний доступ

За допомогою меню «Загальний доступ» можна вибрати окремі файли й папки й надати загальний доступ до них. Набір пунктів, представлених у цьому меню, залежить від типу обраного елемента й типу мережі, до якої підключений комп'ютер.

1.5. Установка принтера в мережі

Виявлення безпроводових і мережевих обладнань для підключення до комп'ютера

До комп'ютера можна підключати бездротової телефон, клавіатуру, мишу або інше обладнання. Сюди входять обладнання Bluetooth і безпроводові (Wi-Fi) обладнання. Можна також додати до комп'ютера мережеві обладнання, наприклад принтер, запам'ятовувальний пристрій або медіаприставку з підтримкою роботи в мережі.

Для пошуку непідключеного устрою до комп'ютера введіть команду **Пуск/Устройства и принтеры/Добавление устройства** з'явиться вікно пошуку устроїв, які не підключені до комп'ютера.

Немає необхідності додавати обладнання, уже підключені до комп'ютера за допомогою Usb-кабелю або іншого мережевого підключення. Windows буде автоматично виявляти й відображати їх.

Якщо Windows не може виявити бездротове обладнання, яке потрібно додати до комп'ютера, далі приводиться ряд порад, які можуть допомогти.

- Переконайтеся, що обладнання, з яким необхідно створити з'єднання, включене, заряджене й не перебуває в сплячому режимі.
- Переконайтеся, що це обладнання не було додано до даного комп'ютера раніше. Додані обладнання не відображаються майстром додавання обладнань у списку обладнань, які можна підключити.
- Переконайтеся, що обладнання перебуває в зоні дії бездротової мережі, звичайно в межах 2-3 метрів для більшості обладнань Bluetooth або 30 метрів для Wi- Fi. Якщо немає гарантії того, що обладнання перебуває в зоні дії бездротової мережі, спробуйте перемістити його ближче до комп'ютера. Якщо між обладнанням і комп'ютером перебуває стіна, спробуйте перенести обладнання в одне приміщення з комп'ютером.
- Переконайтеся, що відсутні інші обладнання, що створюють перешкоди для даного бездротового обладнання, наприклад мікрохвильові печі, безпроводові телефони й інші безпроводові обладнання.
- Якщо до комп'ютера підключений зовнішній адаптер Bluetooth або Wi-Fi, перевірте правильність його підключення, установки й роботи.
- Якщо можливість використання Bluetooth на комп'ютері є вбудована, переконаєтеся, що радіопередавач Bluetooth включений. Включити або виключити приймач бездротової мережі. Багато ноутбуків обладнані зовнішніми перемикачами для включення або вимикання цього передавача. Якщо невідомо, як його включити, зверніться до документації, що поставляється разом з комп'ютером, або відвідаєте веб-сайт виготовлювача.
- Якщо необхідно додати на комп'ютер бездротове мережне обладнання, його слід спочатку налагодити на роботу у використовуваній бездротовій мережі. Якщо невідомо, як це зробити, зверніться до документації, що поставляється разом з обладнанням, або відвідаєте веб-сайт виготовлювача обладнання.

Є два основні способи підключити принтер до комп'ютерів у домашній мережі:

- підключити його прямо до одного комп'ютеру й зробити його загальним для інших комп'ютерів у мережі;
- підключити принтер до мережі як автономне обладнання.

Налаштування загального принтера

Найпростіший спосіб підключення принтера до домашньої мережі – підключити його до одному з комп'ютерів і зробити його загальним в Windows. Такий принтер називається загальним принтером.

Перевага загального принтера в тому, що в такий спосіб можна підключити будь-який USB-Принтер. Недолік: комп'ютер, до якого підключений принтер, повинен бути завжди включений, а якщо ні, то інші комп'ютери не зможуть одержати доступ до принтера.

У попередніх версіях Windows налаштування загального принтера могло викликати деякі проблеми. Але нова можливість Windows 7, набагато спрощує цей процес.

Якщо мережа налаштовується як домашня група, принтери й деякі файли стають загальними автоматично.

Якщо домашня група вже налаштована й іншому комп'ютеру потрібен доступ до загального принтера, виконаєте наступні дії.

Підключення вручну до принтера домашньої групи

Примітка: після установки принтера доступ до нього можна одержати в діалоговім вікні **Печать** будь-якої програми, як і до звичайного принтера, прямо підключеного до комп'ютера. Для використання принтера комп'ютер, до якого він підключений, повинен бути включений.

Налаштування мережевого принтера

Мережеві принтери – обладнання, розроблені для підключення прямо до мережі в якості автономних обладнань, раніше використовувалися в основному у великих офісах. Але зараз часи змінилися.

Виробники принтерів виготовляють усе більше різних принтерів, призначених для роботи в домашніх мережах. У мережевих принтерів є одна велика перевага над загальними принтерами: вони завжди доступні.

Є два основні способи підключення мережевих принтерів: кабельний і бездротовий.

- У кабельних принтерів є порт Ethernet, через який вони підключаються до маршрутизатору або концентратору за допомогою кабелю Ethernet.
- Безпроводові принтери звичайно підключаються до домашньої мережі за допомогою технологій Wi-Fi або Bluetooth.

Деякі принтери підтримують обоє методи підключення. В інструкціях, що поставляються із принтером, описується точний метод його установки.

Установка мережевого, беспроводового принтера або принтера Bluetooth

1. Введіть команду **Пуск/Устройства и принтеры** (рис. 6).
2. Натисніть кнопку **Установка принтера**.
3. У майстру установки принтерів виберіть **Добавить сетевой, безпроводной или Bluetooth-Принтер.**
4. Виберіть необхідний принтер зі списку доступних і натисніть кнопку **Далее**.
5. При необхідності встановіть на комп'ютері драйвер принтера, клацнувши **Установить драйвер**. З появою запиту пароля адміністратора або підтвердження введіть пароль або надайте підтвердження.
6. Виконаєте інші вказівки майстра й натисніть кнопку **Готово.**

Примітка: В разі необхідності можна задати параметри доступу до принтера ввівши команду **Свойства принтера** (рис. 7). Також можливо дозволяти або забороняти друк різним групам користувачів (рис. 8), відбирати порти (рис. 9).

1.6. Установлення мережевого диска

1. Введіть команду **Пуск/Панель управления/Система и безопасность** (рис. 10). **Администрирование Управление компьютером** (рис. 11). **Запоминающие устройства/Управление дисками** (рис. 12). Клацніть правою кнопкою миші диск, який потрібно підключити, і виберіть команду **Изменить букву диска или путь к диску** (рис. 13).

2. Натисніть кнопку **Добавить**, клацніть **Подключить том как порожнюю NTFS-Папку** й уведіть шлях до порожньої папки на NTFS – Диску (рис. 14) або натисніть кнопку **Обзор**, щоб знайти папку. Натисніть кнопку **ОК**; потім натисніть кнопку **ОК** ще раз.

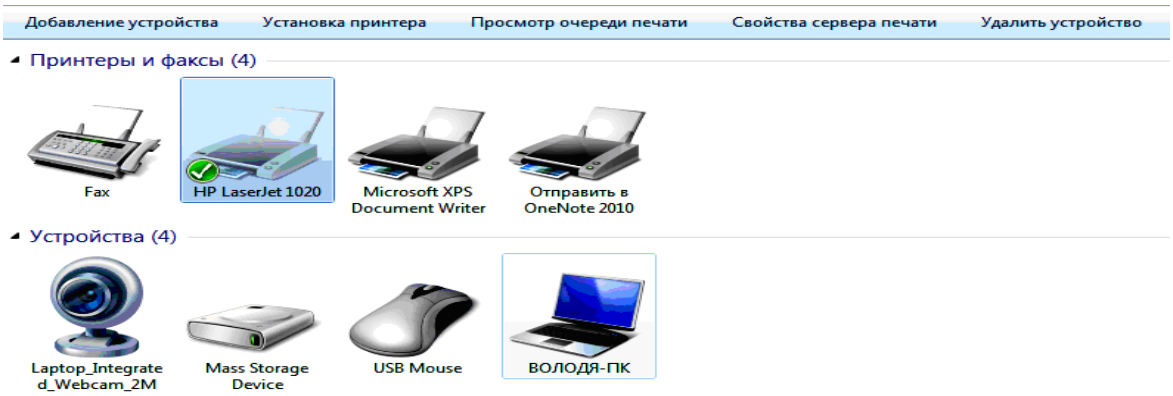


Рис. 6. Вікно «Принтери»

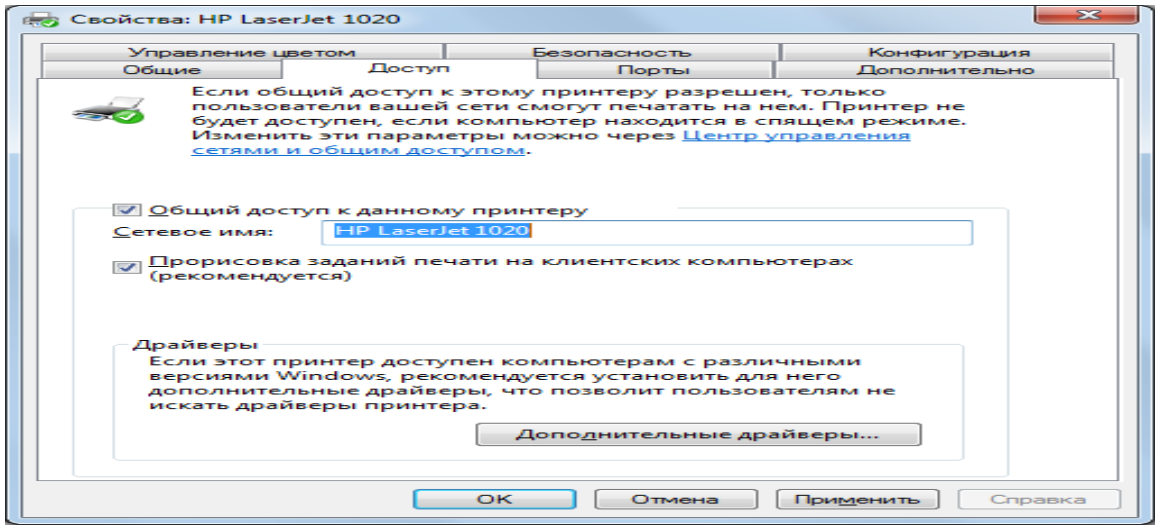


Рис. 7. Доступ до принтера

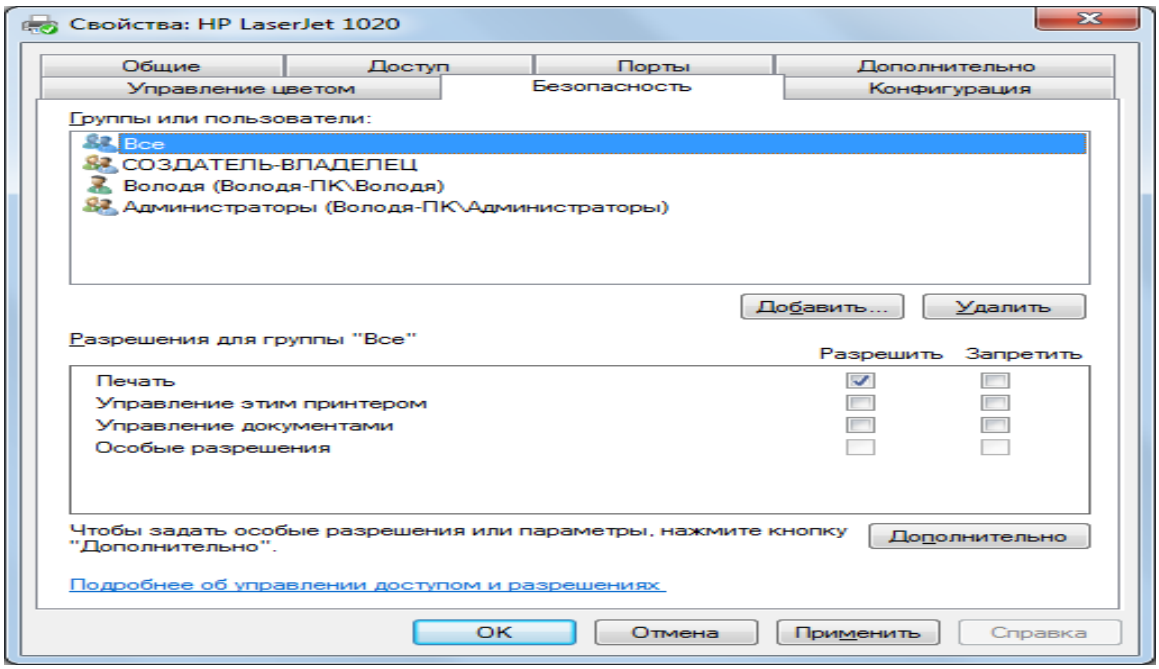


Рис. 8. Вікно дозволу друку різним користувачам

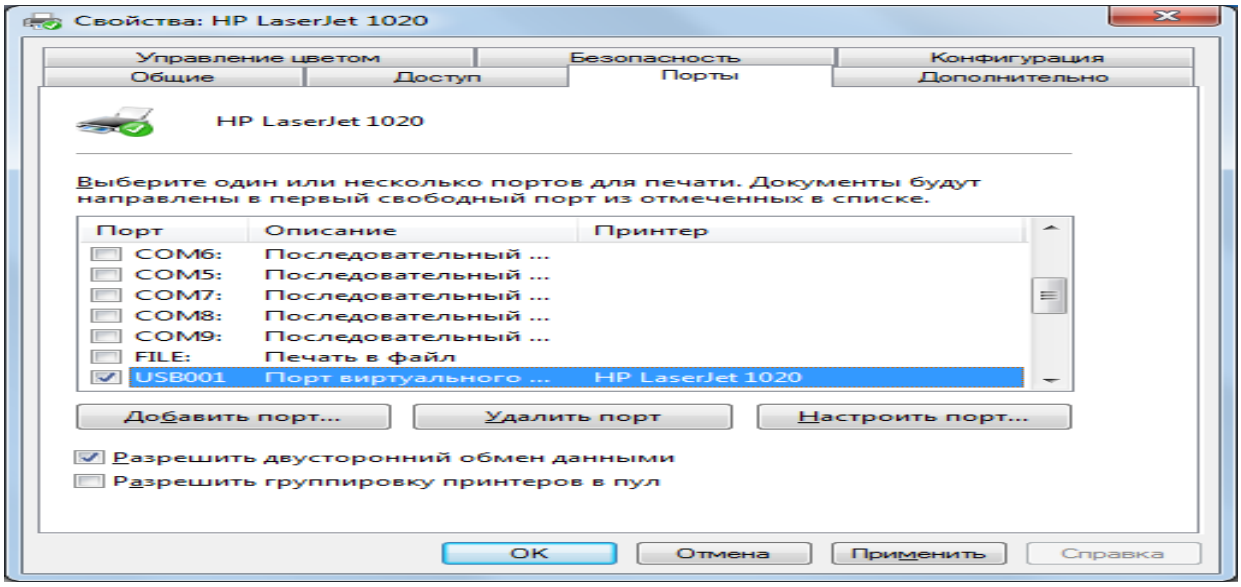


Рис. 9. Вікно портів принтера

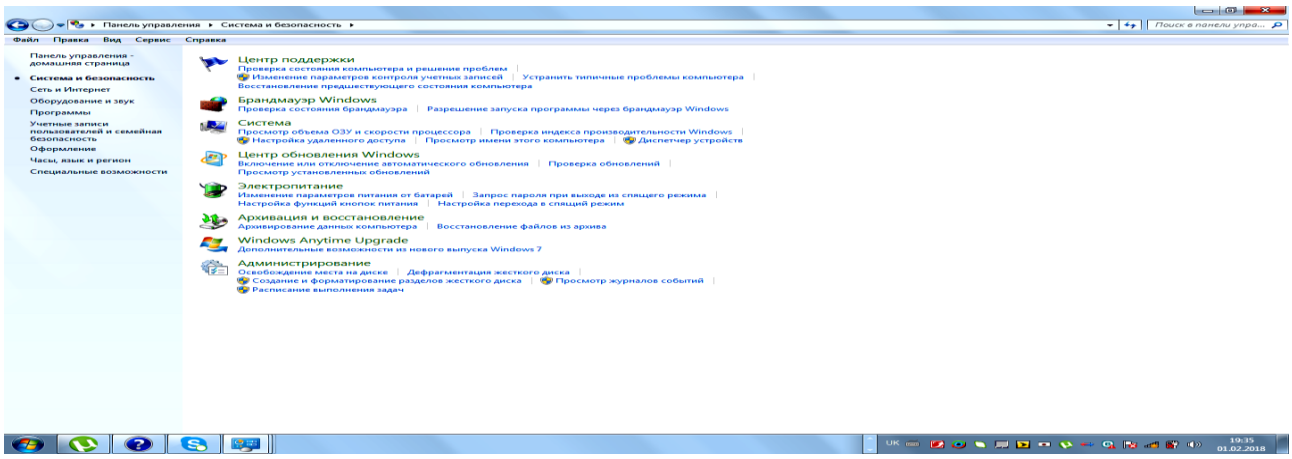


Рис. 10. Вікно «Система і безпека»

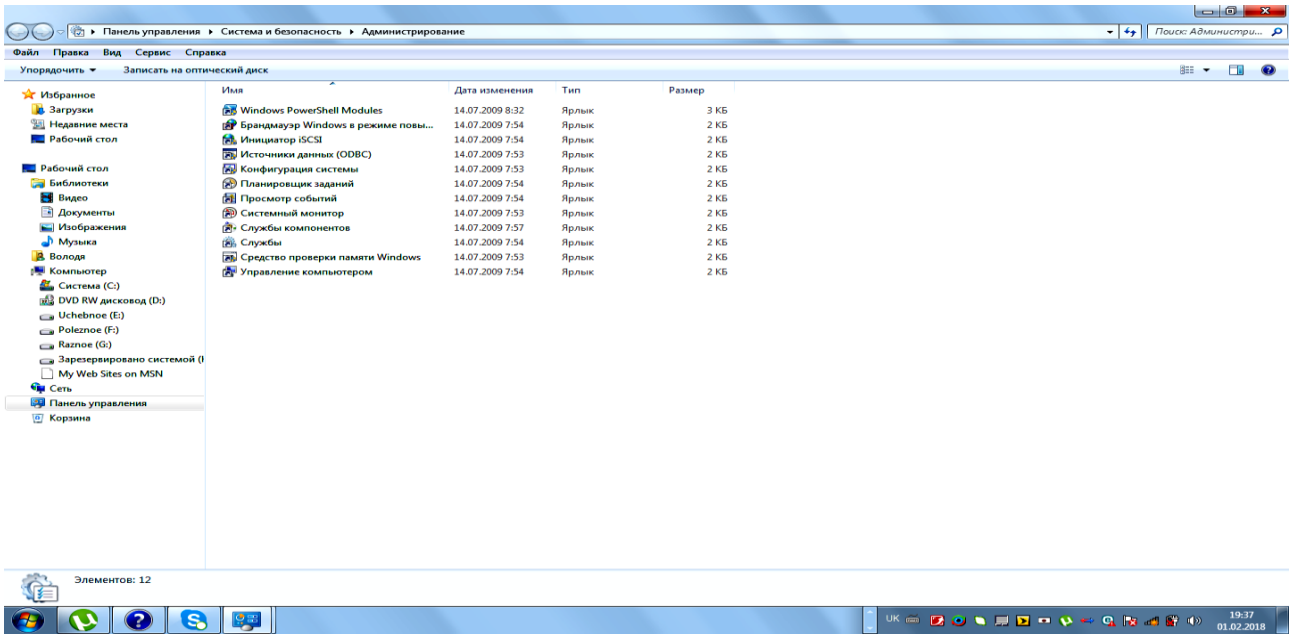


Рис. 11. Вікно «Адміністрування»

Видалення мережевого диска

1. Введіть команду **Пуск/Панель управления/Система и безопасность/ Администрирование** (рис. 2). **Управление компьютером** (рис. 3). **Запоминающие устройства /Управление дисками** (рис. 13). Клацніть правою кнопкою миші диск, який потрібно підключити, і виберіть **Изменить букву диска или путь к диску** (рис. 14).

2. Натисніть кнопку **Удалить**, потім кнопку **ОК**.

Примітка: Кошик не розпізнає підключені диски, тому спроба вилучити файл, що зберігається на підключеному диску, може викликати помилку. Щоб остаточно вилучити файл із комп'ютера, не відправляючи його в кошик, клацніть файл і натисніть комбінацію клавіш SHIFT+DELETE. При остаточнім видаленні файлу його не можна відновити, якщо немає резервної копії файлу.

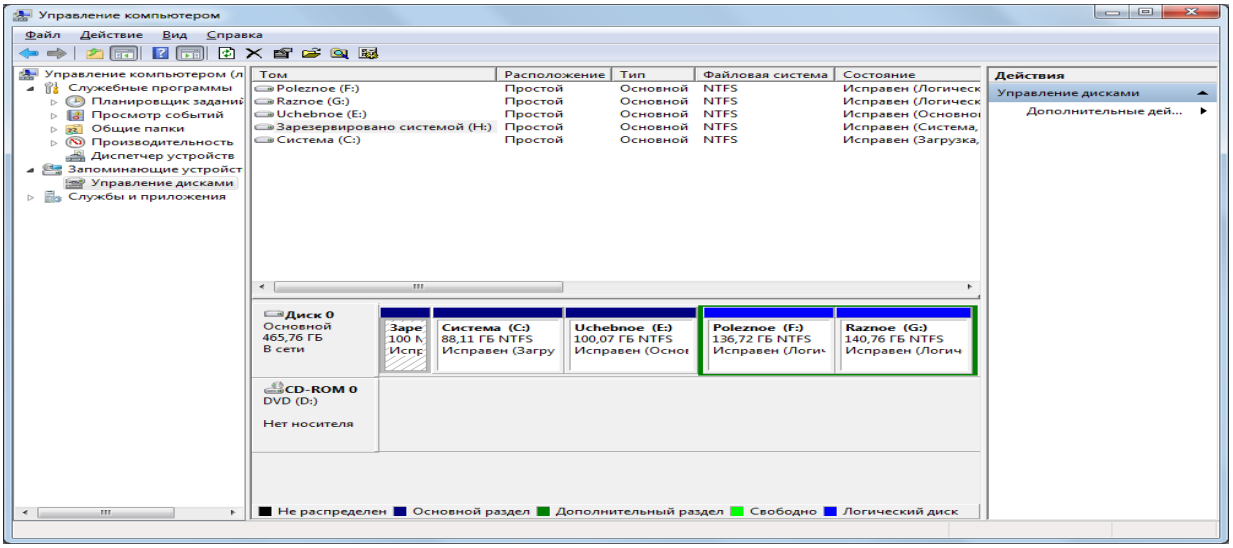


Рис. 12. Вікно «Управління дисками»

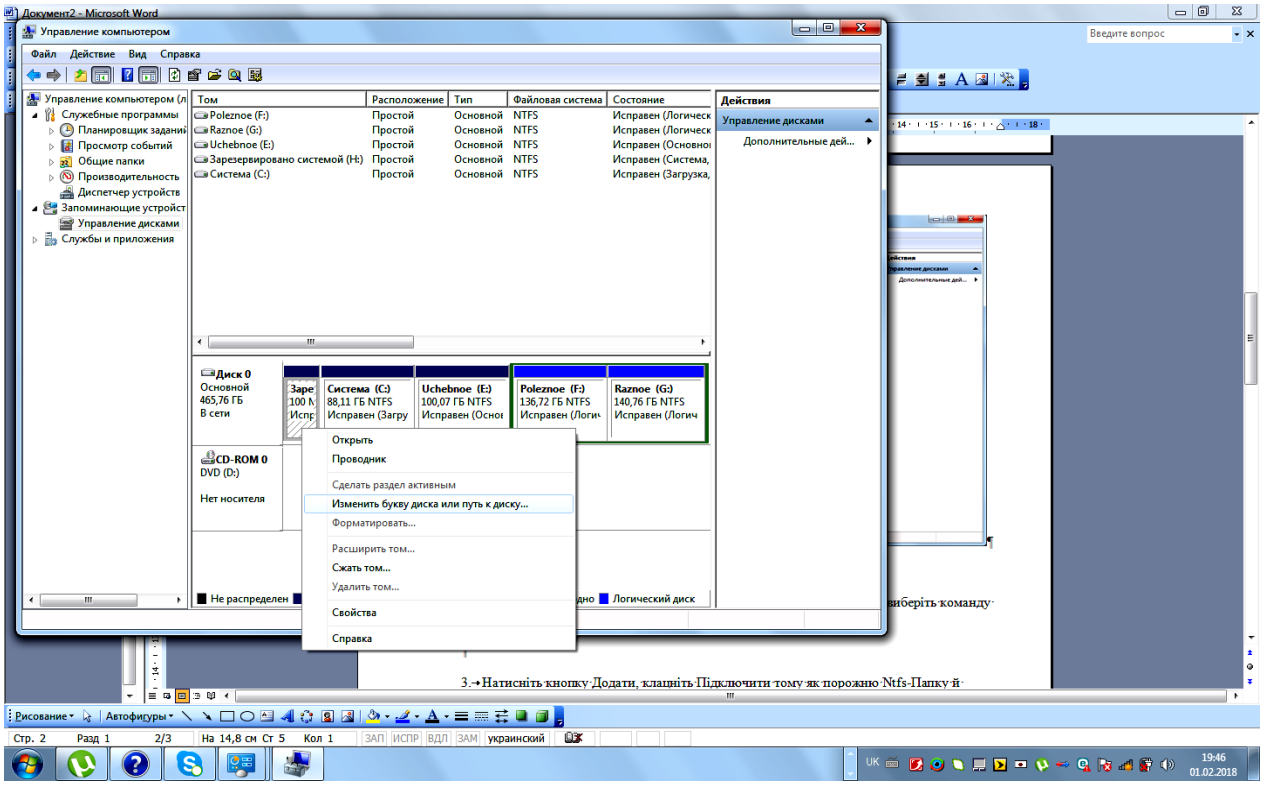


Рис. 13. Відбір команди **Изменить букву диска или путь к диску**

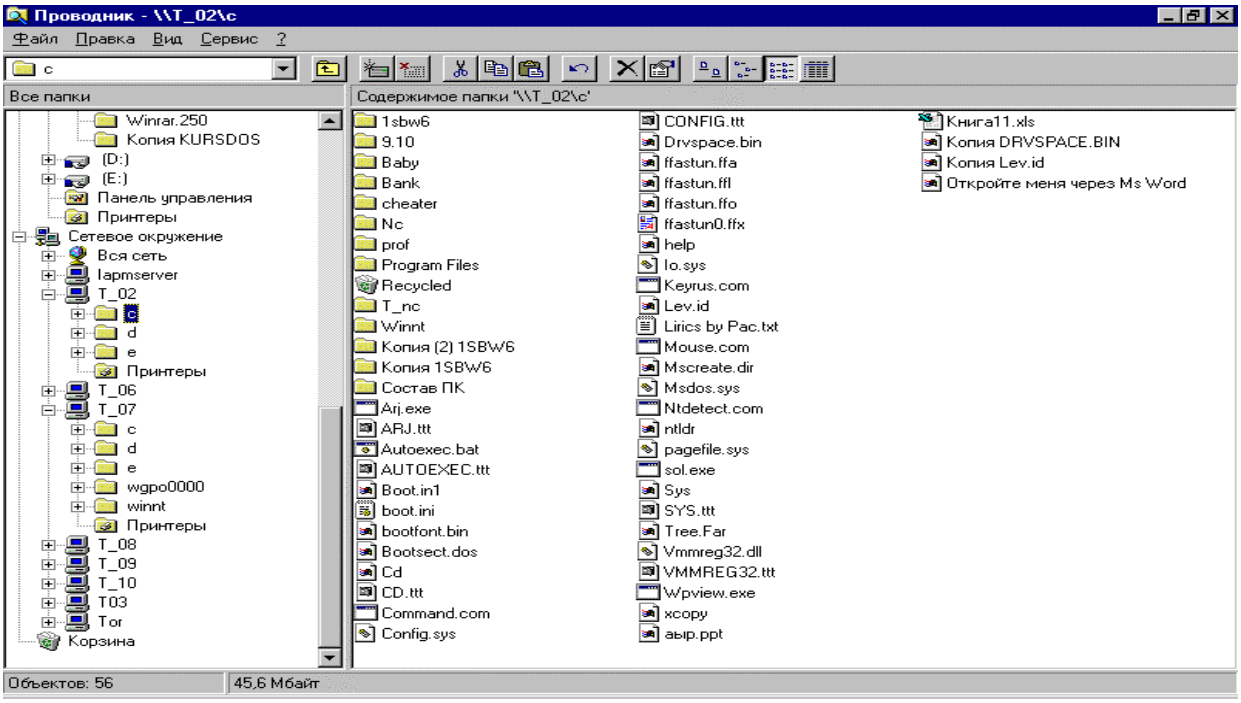
1.7. Визначення завантаження ресурсів комп'ютера та мережі

- Натисніть кнопку **Пуск** у поле пошуку введіть **монитор ресурсов** і в списку результатів клацніть **Монитор ресурсов.** Відкриється вікно монітора ресурсів (рис. 15) на вкладках якого можна відслідкувати завантаження компонентів в режимі реального часу.

1.8. Приклади роботи у локальній мережі Windows за допомогою різноманітного програмного забезпечення

В операційних системах Windows існує убудована можливість роботи в локальній мережі за допомогою різноманітних програм, наприклад, провідника. При відкритті мережевого оточення (рис. 16) доступними є комп'ютери, наприклад, T_02… T_10, а також їхні логічні диски (C, D, E і т.д.) із каталогами й файлами. Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій. Для забезпечення доступу до логічних дисків із мережі необхідно на робочому столі Windows відкрити піктограму

Мой компьютер і з контекстно-залежному меню командою **доступ** установити загальний доступ до потрібних дисків. Програма-оболонка Far-manager при введенні команди "Drive" із підміню Left або Right із наступним вибором команди "network" (рис. 17) дозволяє одержати доступ до комп'ютерів, наприклад, T_02… T_10, а також їхнім логічним дискам (C, D, E і т.д.) із каталогами й файлами (рис 18). Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій.



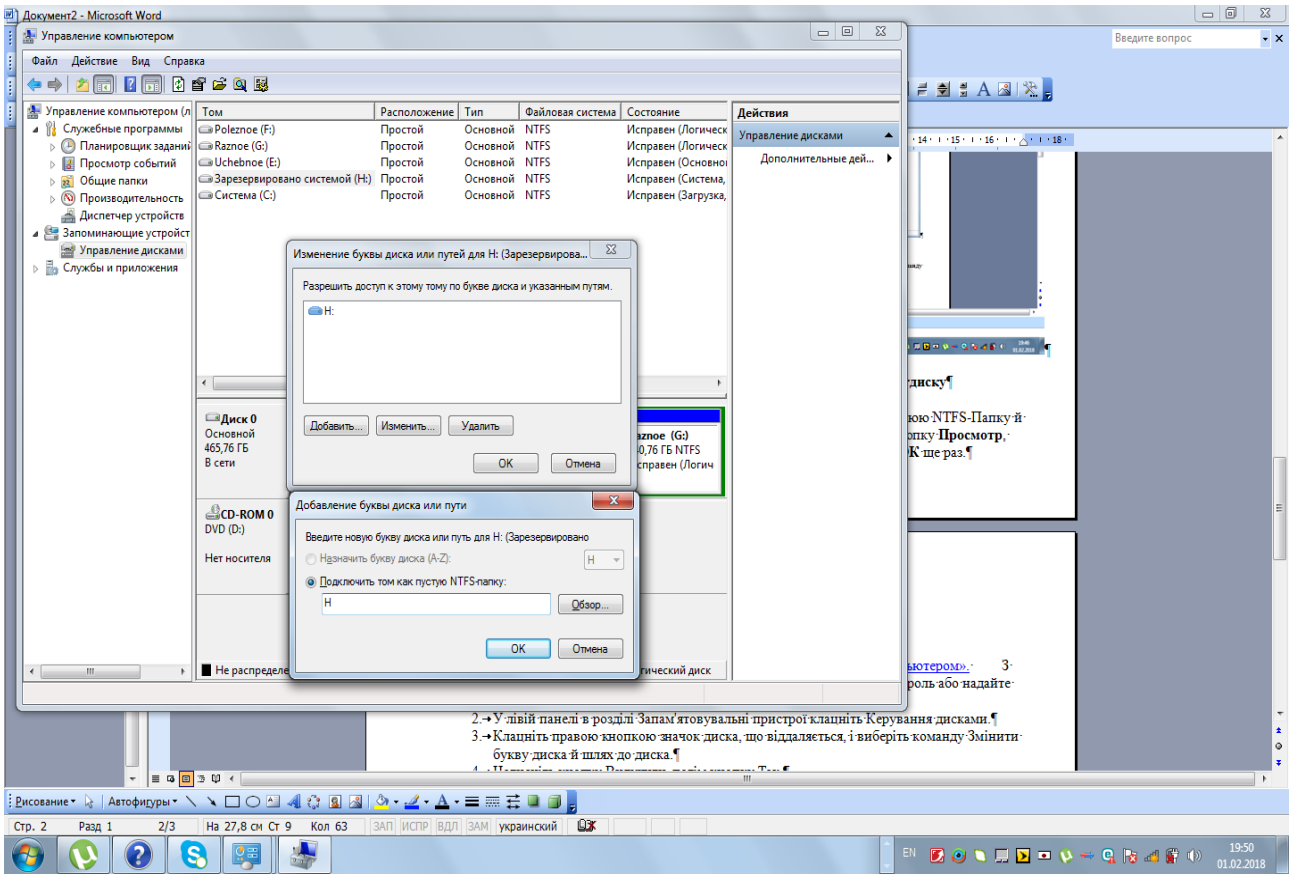
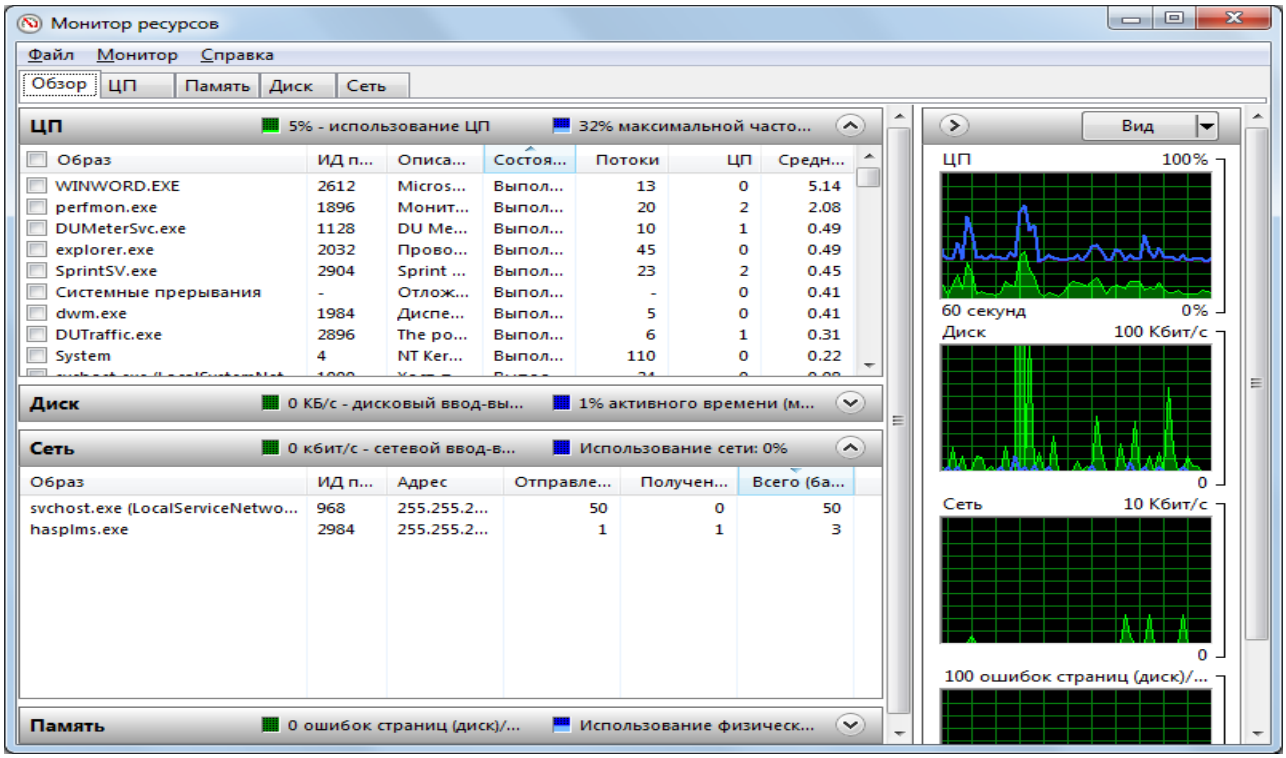


Рис. 14. Вибір та призначення параметрів мережевому диску



- Рис. 15. Вікно монітора ресурсів

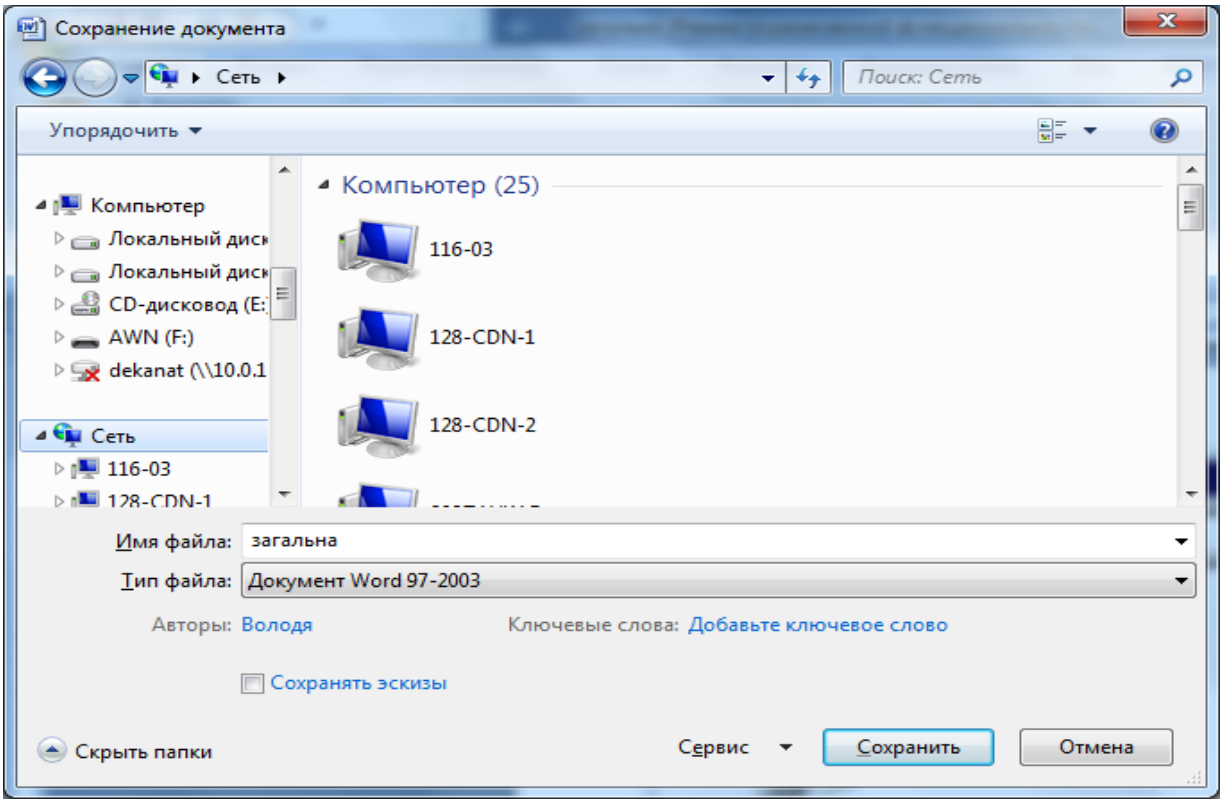


Рис. 16. Приклад роботи в локальній мережі за допомогою провідника.

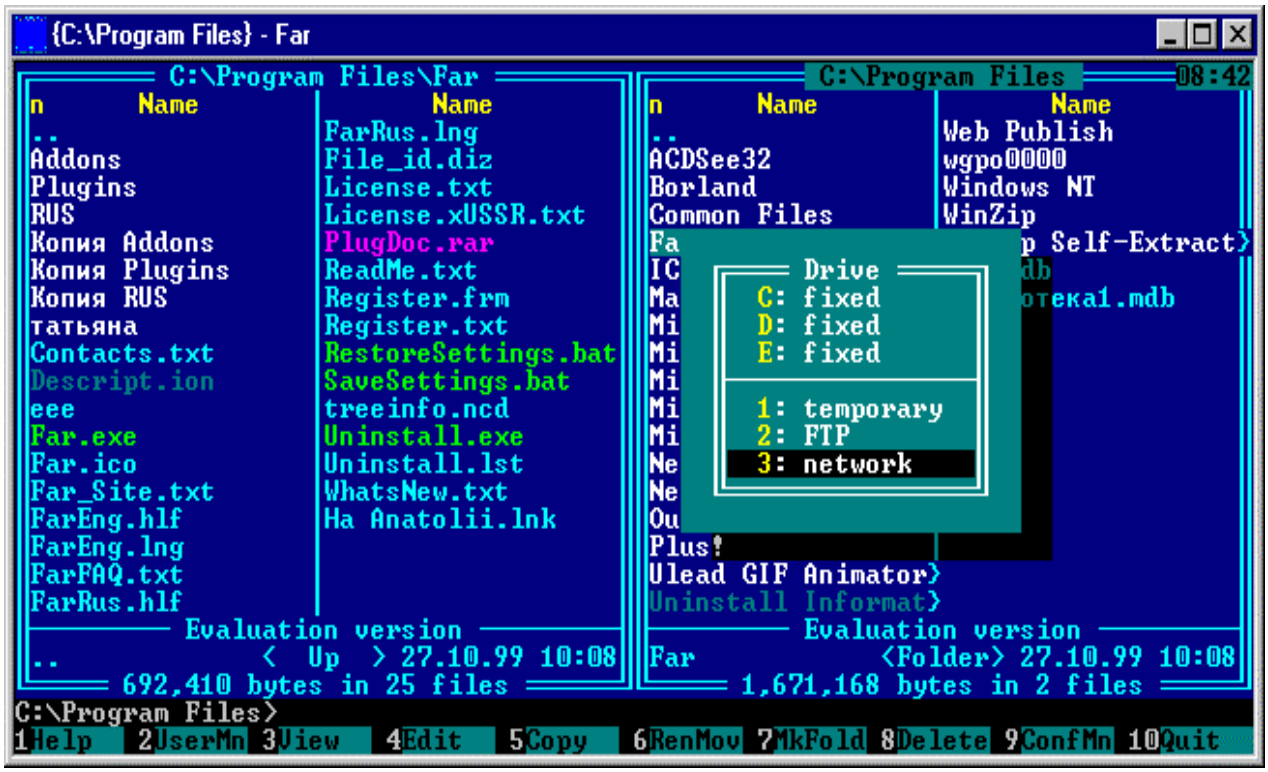


Рис. 17. Вибір локальної мережі

Аналогічна робота в мережі з Total Commander (рис. 18). Подальша робота з каталогами й файлами нічим не відрізняється від звичайних операцій.

Аналогічна робота з локальною мережею програм із пакета Microsoft Office які дозволяють зберігати і відкривати файли на комп'ютерах локальної мережі при введенні команд **Сохранить, сохранить как, открыть** із підміню **Файл** із наступним вибором мережевого оточення (рис 19).

Аналогічна робота в мережі з Norton Commander під Windows де подається команда **Disconnect Network Drive** із підменю **Disk** для входу в локальну мережу, або **Map Network Drive** для створення мережевого диска.

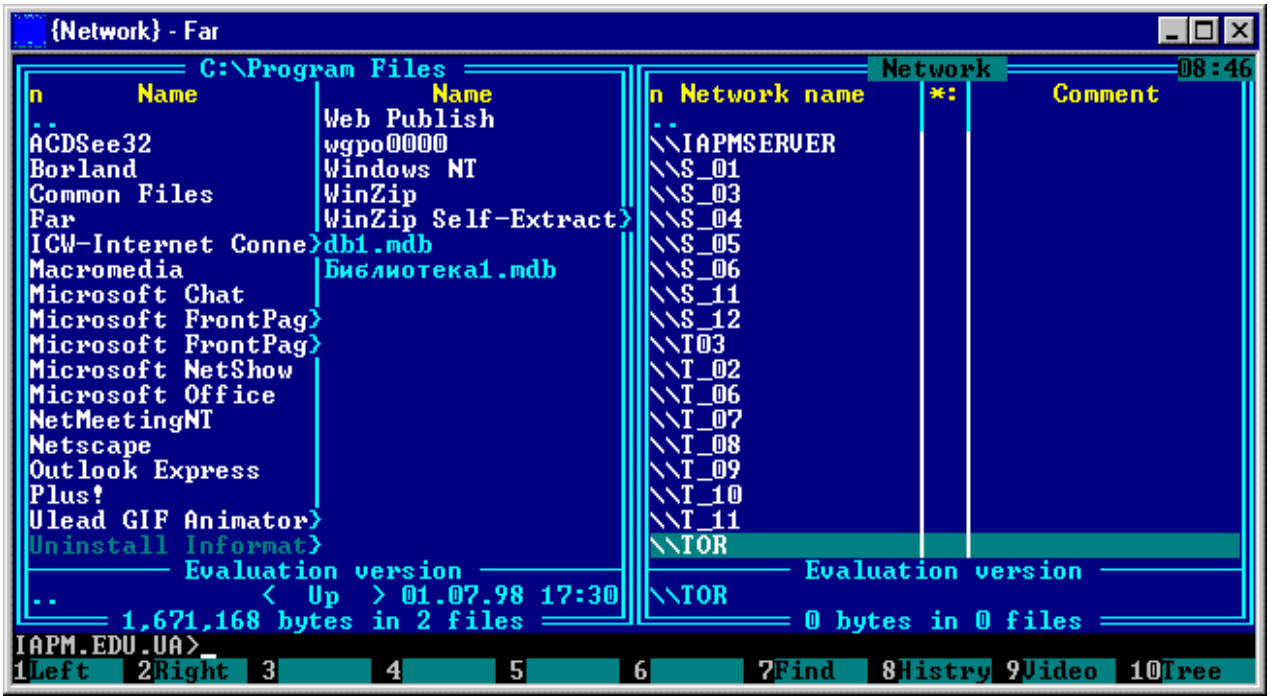


Рис. 18. Список комп'ютерів локальної мережі

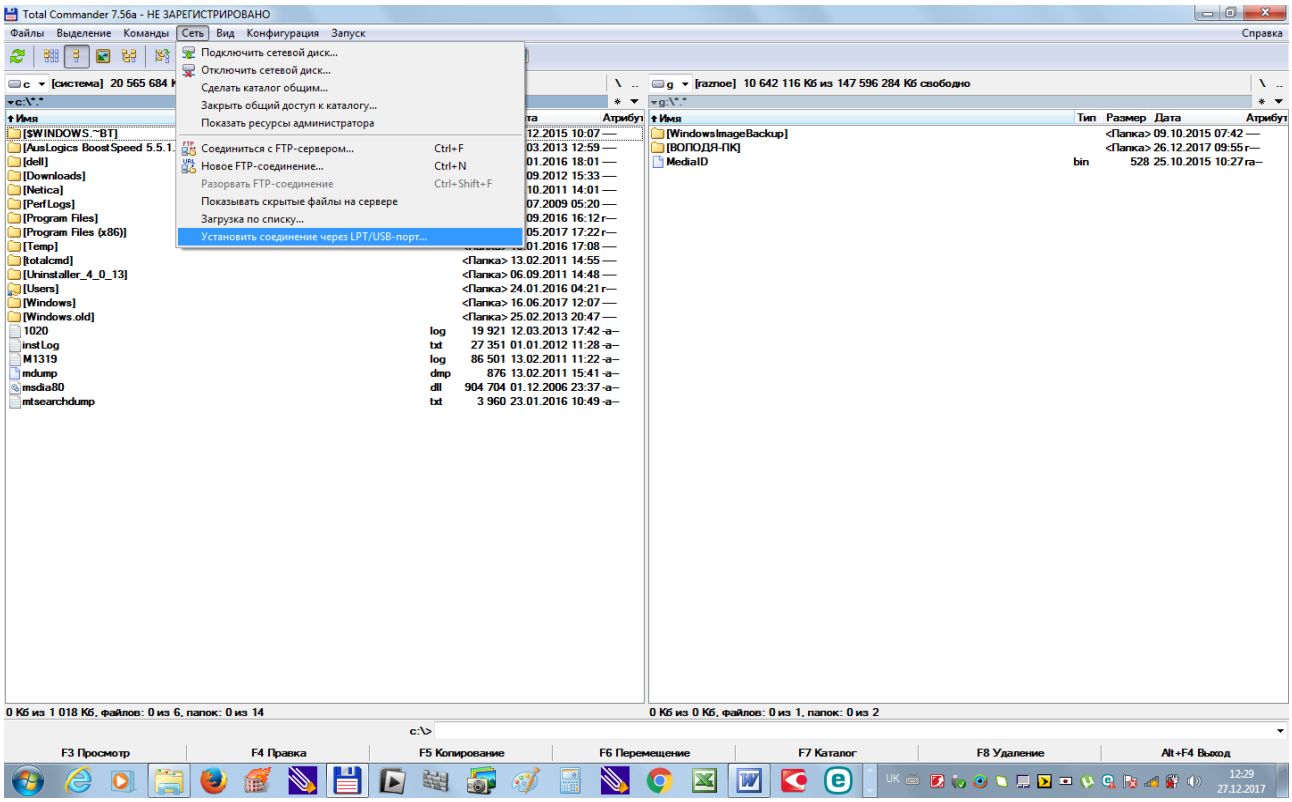


Рис. 19. Вибір мережевої команди в Total Commander

2. Хід роботи

1. Проведіть налагоджування параметрів мережі через панель керування.
2. Проведіть пошук комп'ютера в мережі за вказівкою викладача.
3. Проведіть об'єднання в мережу домашніх комп'ютерів, що працюють під керуванням однакових версій Windows.
4. Проведіть об'єднання в мережу домашніх комп'ютерів, що працюють під керуванням різних версій Windows.
5. Забезпечте повний доступ користувачів мережі до довільного каталогу вашого комп'ютера.
6. Обмежте доступ до вказаного каталогу однієї групи користувачів.
7. Змініть ім'я свого комп'ютера в мережі.
8. Поверніть ім'я свого комп'ютера в мережі.
9. Запустіть інспектора ресурсів та перевірте, хто найбільш інтенсивно використовує ресурси вашого комп'ютера.
10. Проведіть копіювання, переміщення, перейменування, створення каталогу на комп'ютері N+1 (диск D) за допомогою провідника.
11. Проведіть копіювання, переміщення, перейменування, створення каталогу на комп'ютері N+1 (диск D) за допомогою оболонки Far-manager або Norton Commander.
12. Створіть файл у програмі Microsoft Word та збережіть його на диску D на комп'ютері N+1.
13. Відкрийте довільний файл з комп'ютера N-1 у програмі Microsoft Word на своєму комп'ютері.
14. Створіть файл у програмі Microsoft Excel та збережіть його на диску D на комп'ютері N+1.
15. Відкрийте довільний файл з комп'ютера N-1 у програмі Microsoft Excel на своєму комп'ютері.
16. Створіть файл у програмі Microsoft Access та збережіть його на диску D на комп'ютері N+1.
17. Відкрийте довільний файл з комп'ютера N-1 у програмі Microsoft Access на своєму комп'ютері.

3. Контрольні питання

1. Як проводиться налагоджування мережі Windows?
2. Які переваги та недоліки мережевої технології Ethernet?
3. Які переваги та недоліки мережевої технології HomePNA?
4. Які переваги та недоліки мережевої технології Powerline?
5. Які характеристики стандартів безпроводових мереж?
6. Наведіть приклади устаткування, використовуваного в домашніх мережах.
7. Як об'єднати в мережу домашні комп'ютери, що працюють під управлінням різних версій Windows?
8. Які основні відмінності в технології мереж між Windows XP, Windows Vista і Windows 7.
9. Які Типи мережевого розміщення існують?
10. Як знайти ім’я та Ір-Адресу комп'ютера, робочу групу куди він входить?
11. Як отримати доступ до локальної мережі?
12. Як встановити параметри доступу до каталогів та файлів?
13. Як установити мережевий принтер?
14. Як встановити налаштування мережевого принтера
15. Як встановити та видалити мережевий диск?
16. Використання інспектора для контролю за використанням загальних ресурсів.
17. Робота в мережі за допомогою провідника.
18. Робота в мережі за допомогою оболонки Far-manager.
19. Робота в мережі за допомогою програм, які входять до складу Microsoft Office.

ЛАБОРАТОРНА РОБОТА 8.
КОМУНІКАЦІЙНІ УТИЛІТИ ДЛЯ РОБОТИ В МЕРЕЖІ

Мета роботи: уміти користуватися мережевими утилітами; їх параметрами; формувати відповідні команди; аналізувати отримані дані .

Зміст

1. Теорія
1.1 Утиліта IPconfig
1.2 Утиліта Ping
1.3 Утиліта Tracert
1.4 Утиліта Netstat
1.5 Утиліта Pathping
1.6 Утиліта Route
1.7 Команда ivconfig для пристрою «Ноутбук»
1.8 Утиліта ARP
2. Хід роботи
3. Контрольні питання

1. Теорія

До складу операційної системи Windows включений ряд комунікаційних утиліт, які дозволяють визначити значення параметрів IP- конфігурації (**ipconfig**), перевірити працездатність з'єднання з віддаленим вузлом (**ping**), прослідкувати маршрут проходження пакетів до віддаленого вузла (**tracert**).

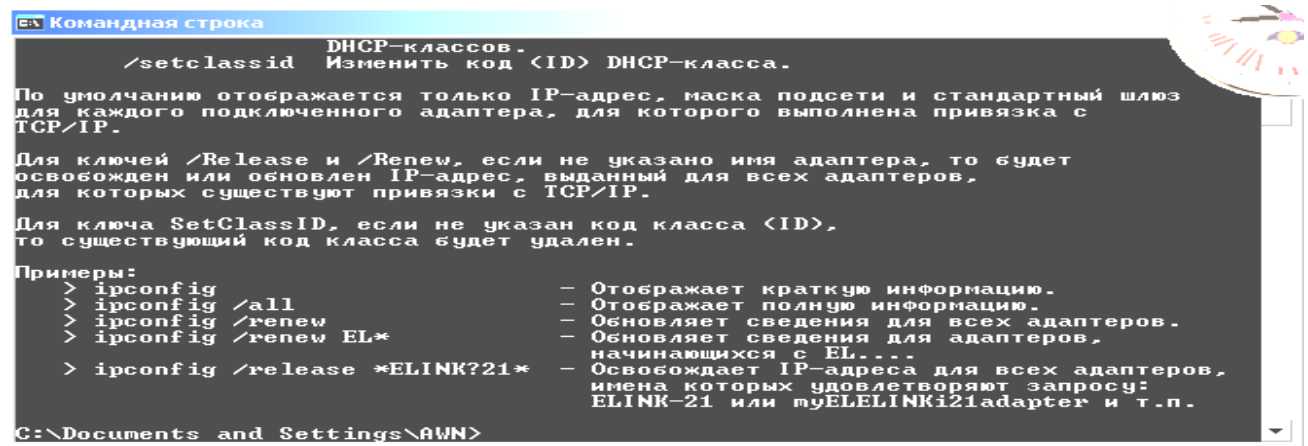
Для їх запуску достатньо перейти в режим командного рядка (**Пуск-Все прораммы-Стандартные-Командная строка**) і ввести з клавіатури у відповідь на запрошення ім'я утиліти з відповідними параметрами.

1.1. Утиліта IPconfig

Утиліта **ipconfig** є одним з основних інструментів користувача, яка показує значення параметрів IP- конфігурації (звідси і її назва). У випадку виклику утиліти без додаткових ключів на екран виводяться:

- IP- адреса локального DNS- сервера (сервера імен);
- IP- адреса самого хосту і маска підмережі;
- IP- адреса сервера-шлюза до Internet.

Є додаткові можливості утиліти, що дозволяють переглянути поточну конфігурацію адрес TCP/IP для всіх установлених на даному комп'ютері мережевих адаптерів, з'єднань що комутуються, з її допомогою можна визначити Ip-Адресу даного комп'ютера. Запущена без параметрів команда ifconfig видає в якості результату поточну конфігурацію адрес TCP/IP для всіх установлених на даному комп'ютері мережевих адаптерів, з'єднань, що комутуються (рис. 1).



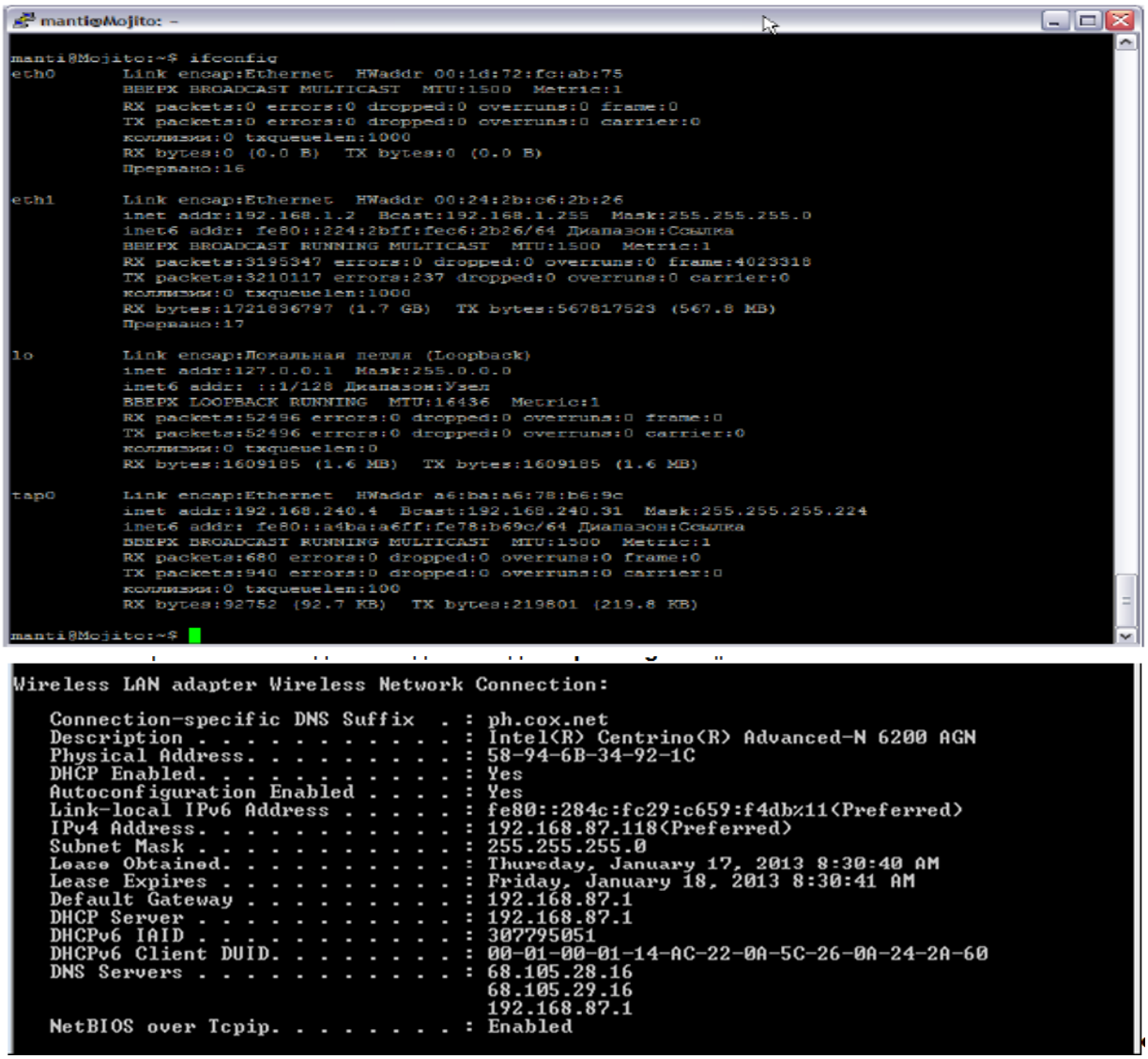


Рис. 1. Додаткові можливості утиліти

До складу операційних систем Windows XP, Windows 2000, Windows 7 поряд з утилітою ipconfig входить також її графічний аналог, який працює у стандартному вікні Windows, - winipcfg.

Windows 2000 та Windows XP не мають такого аналога, але в них для перегляду відомостей про IP-конфігурацію можна скористуватися іншою утилітою – **Сетевые подключения**. Її запуск здійснюється за допомогою команди **Пуск-Все прораммы-Стандартные-Связь-Сетевые подключения**. У вікні, що відкриється, треба клацнути правою кнопкою миші по з'єднанню, вибрати з контекстного меню команду **Состояние** і у вікні стану з'єднання перейти на вкладку **Поддержка**.

IP-адреси використовуються для ідентифікації комп'ютерів в мережі. IP-адреса завжди має довжину 32 біти і складається з чотирьох частин, які називаються октетами (octet). Чотири частини об'єднуються в запис, в якому кожний октет відокремлюється крапкою, наприклад, 198.68.191.10.

За своєю структурою кожна 32-бітова IP-адреса ділиться на дві частини – префікс і суфікс, які складають дворівневу ієрархію. Префікс означає фізичну мережу, до якої підключений комп'ютер, а суфікс – окремий комп'ютер в цій мережі. Яка частина адреси відноситься до префікса, а яка до суфікса, визначається значеннями перших чотирьох бітів і відповідно до цього вони поділяються на три основних класи A, B і C. Для забезпечення максимальної гнучкості IP-адреси виділяються організаціям в залежності від кількості мереж і комп'ютерів в організації у відповідності з цими класами.

Мережі класу A належать найбільшим світовим постачальникам послуг Internet. Їх усього 126, а кожна з них може мати майже 17 мільйонів комп'ютерів.

Мережі класу B – мережі середнього масштабу. Їх може бути трохи більше 16 тисяч, а в кожній з них 65 534 хостів. Такі мережі мають найбільші університети та інші великі організації.

Мережі класу C – мережі дрібних постачальників, кількість яких може перевищувати 2 мільйони, а число комп'ютерів в кожній мережі – до 254. Саме до цього класу мереж відносяться мережі переважної більшості провайдерів Internet.

Якщо довільну IP-адресу символічно позначити як набір октетів w.x.y.z, то в узагальненому вигляді структуру IP-адрес для основних класів A, B і C можна представити у вигляді (табл. 1).

Таблиця 1

Структура IP-адрес в мережах класів A, B і C.

Клас мережі	**Значення першого октанту (w)**	**Октант номеру мережі**	**Октант номеру хосту**	**Кількість мереж**	**Кількість хостів в мережі**
A	1-126	w	x.y.z	126	16 777 214
B	128-191	w.x	y.z	16 384	65 534
C	192-223	w.x.y	z	2 097 151	254

Наведена таблиця дозволяє за відомою IP-адресою комп'ютера швидко визначити клас мережі, її номер та номер комп'ютера в мережі. Наприклад, комп'ютер з IP-адресою 221.132.3.123 знаходиться в мережі класу C з ідентифікатором мережі 221.132.3 і має в цій мережі ідентифікатор 123. Для того, щоб відділити префікс від суфікса в IP-адресі застосовується спеціальне 32-бітне число, яке називається маскою мережі. За своєю структурою маска представляє собою такий же набір з чотирьох октетів, що і звичайна IP-адреса. Нижче (табл. 2) наведені маски підмереж, які використовуються за замовченням для мереж класів A, B і C.

Таблиця 2

Значення масок підмереж (за замовчуванням)

Клас мережі	**Значення маски**
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Маски підмереж застосовується також для логічного поділу великих мереж на підмережі меншого масштабу. Для зручності користувачів у Internet кожному комп'ютеру поряд із IP-адресою присвоюється власне символьне ім'я. Цю функцію в Internet виконує доменна служба імен – DNS (Domain Name System). Вона являє собою розподілену базу даних, в якій підтримується ієрархічна система символьних імен. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним іменем вузла. База даних про відповідність символьних імен і IP-адрес не зберігається на кожному комп'ютері, а розподілена за великою кількостю DNS-серверів, що розташовані на різних вузлах Internet. Кожного разу, коли в прикладній програмі виникає необхідність перетворити ім'я в IP-адресу, вона стає клієнтом служби імен. Клієнт сервера DNS знає IP-адресу сервера DNS свого адміністративного домену і направляє йому запит, у якому повідомляє відоме символьне ім'я і просить повернути відповідну IP-адресу. Якщо дані про запитану відповідність вдається відшукати в базі даного DNS-серверу, то він відразу посилає відповідь клієнту. Якщо ж сервер DNS не може знайти відповіді на запит, він тимчасово стає клієнтом для іншого сервера DNS, а потім – наступного сервера імен і т.д., поки не знайде такий сервер, який зможе дати відповідь на запит.

1.2. Утиліта Ping

Це службова програма, що перевіряє зв'язок з віддаленим комп'ютером. Для цього використовуються пакети відлуння-запиту і відлуння-відповіді спеціального протоколу міжмережевих керуючих повідомлень ICMP (Control Message Protocol).

Формат команди:

ping [-<Sw>] [<ім'я_кінцевого_комп'ютера>],

де -<Sw> - комбінація додаткових параметрів, призначення окремих з яких наведено нижче (рис. 2), <ім'я_кінцевого_комп'ютера> - IP-адреса або доменне ім'я віддаленого хосту.

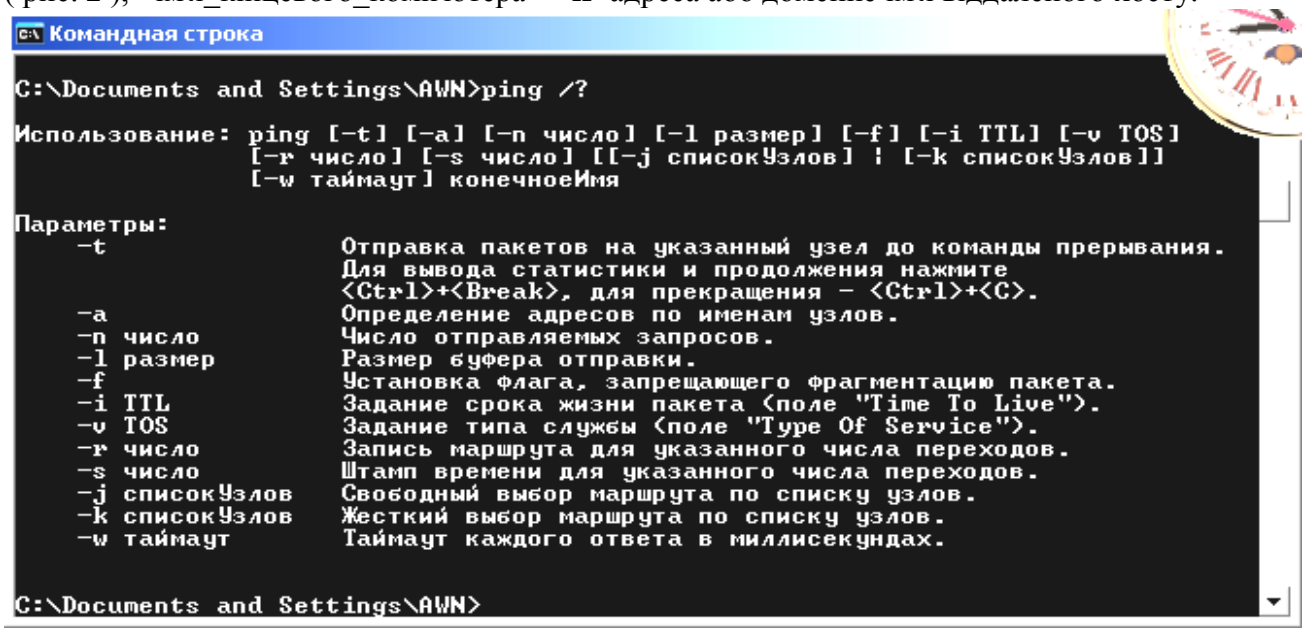


Рис. 2. Додаткові можливості утиліти

За замовчуванням n-4. Максимальний інтервал очікування w-4 сек. За замовчуванням ping посилає на віддалений хост чотири повідомлення з відлунням-запитом. У разі справності хосту після кожної передачі виводиться відповідне повідомлення з відлунням-відповіддю. Якщо ж хост не відповідає, то видається повідомлення з текстом про помилку "Время ожидания запроса истекло". Крім своєї основної функції – тестування з'єднання з віддаленим хостом, ping дозволяє перевірити правильність функціонування DNS-серверів: якщо деякий вузол "відгукується" на IP-адресу, але "не відгукується" на доменне ім'я, то або DNS- сервер непрацездатний, або він неправильно вказаний у конфігурації.

Зверніть увагу на параметр **TTL**, значення якого виводиться для кожного тестового пакету при виконанні команди ping. Цей параметр визначає час життя пакету (**TTL - Time To Live**). Для кожного новонародженого пакету його значення рівне 255. При проходженні через шлюз або маршрутизатор, значення **TTL** зменшується на величину тимчасової затримки на маршрутизаторі. Якщо значення **TTL** стає менше або рівно нулю, пакет знищується. Дане правило прийняти для запобігання нескінченному блуканню пакетів за кільцевими маршрутами Мережі.

Застосування утиліт ipconfig і ping для тестування з'єднання з віддаленим хостом (за рекомендаціями Microsoft)

Для тестування з'єднання Microsoft рекомендує таку процедуру перевірки:

1) Запустіть утиліту ipconfig і визначте такі параметри, як IP- адреса локального комп'ютера (IP_adress_of_Local_host) і маска підмережі, адреса шлюзу за замовченням (IP_adress_of_default_gateway), адреса DNS- сервера (IP_adress_of_DNS_server). Якщо вказані співпадаючі IP-адреси, то маска підмережі буде вказана як 0.0.0.0.
2) Зверніться за IP- адресою "замикання на себе": ping 127.0.0.1.
3) Перевірте відгук власного комп'ютера: ping IP_adress_of_Local_host.

4) Запитайте відгук шлюзу за замовченням: ping IP_adress_of_default_gateway. Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси основного шлюзу і працездатність цього шлюзу (маршрутизатора).

5) Зверніться за адресою віддаленого вузла: ping IP_adress_of_remote_host . Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси віддаленого вузла, працездатність цього вузла, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і віддаленим вузлом.

Зверніться за адресою DNS- сервера : ping IP_adress_of_DNS_server. Якщо команда не була успішно виконана, слід перевірити правильність IP-адреси DNS-сервера, працездатність DNS-сервера, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і DNS-сервером.

1.3. Утиліта Tracert

Утиліта дозволяє прослідкувати маршрут проходження текстового пакету з даними до віддаленого вузла. З її допомогою можна визначити, на яких ланках маршруту затримка пакетів максимальна.Шлях до точки призначення визначається за допомогою посилки в точку призначення відлуння-повідомлень протоколу ICMP. Виведений шлях – це список найближчих маршрутизаторів, що знаходяться на шляху між вузлом джерела і точкою призначення.

Формат команди:

Tracert [-<Sw>] [<ім'я_кінцевого_комп'ютера>],

де -<Sw> - комбінація додаткових параметрів, призначення яких наведено нижче (рис. 3),

<ім'я_кінцевого_комп'ютера> - IP-адреса або доменне ім'я віддаленого вузла,

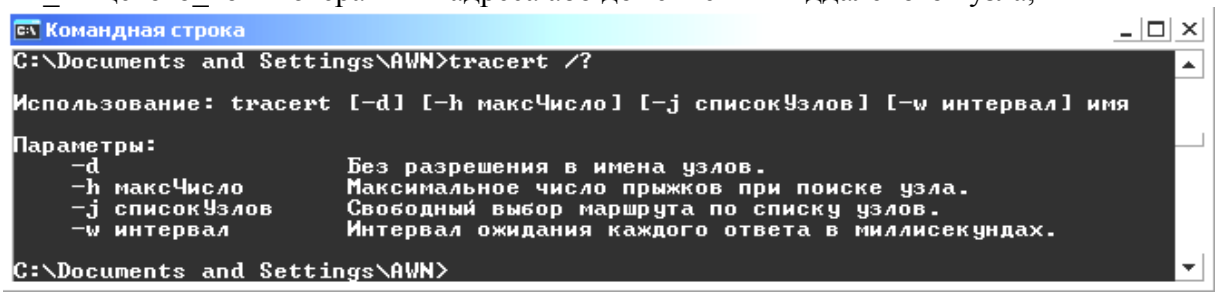


Рис. 3. Додаткові можливості утиліти

За умовчанням h-30. Максимальне число адрес у списку j -9. Максимальний інтервал очікування w-4 сек. Деякі маршрутизатори не видимі для команди tracert. У цьому випадку перехід відображається рядом зірочок (*).

1.4. Утиліта Netstat

Утиліта дозволяє прослідкувати відкриті порти комп’ютера, виконавчі файли, які приймають участь в створенні з'єднання, код процесу кожного і протокол з'єднання, таблицю маршрутів, статистичні дані за протоколами (рис. 4, 5). Формат команди та додаткові параметри відображені на рис. 6.

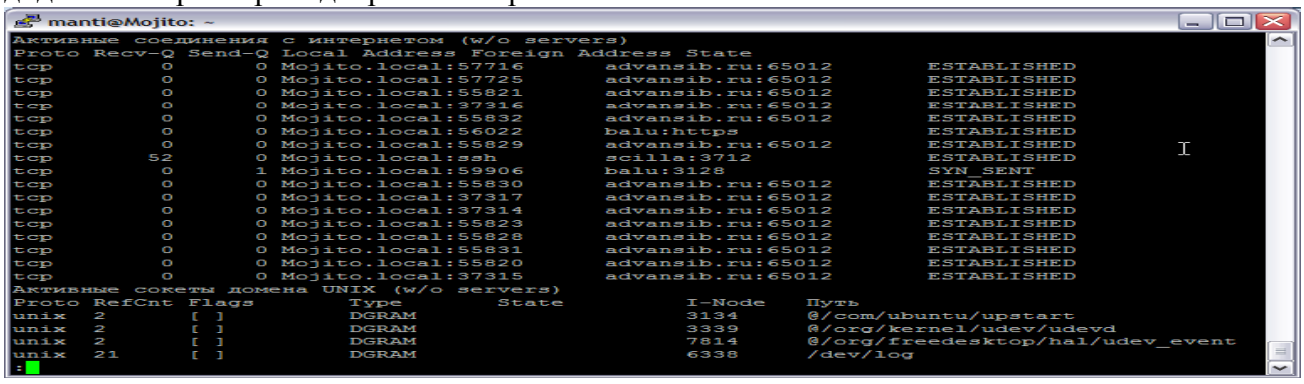


Рис. 4. Виведення активних підключень

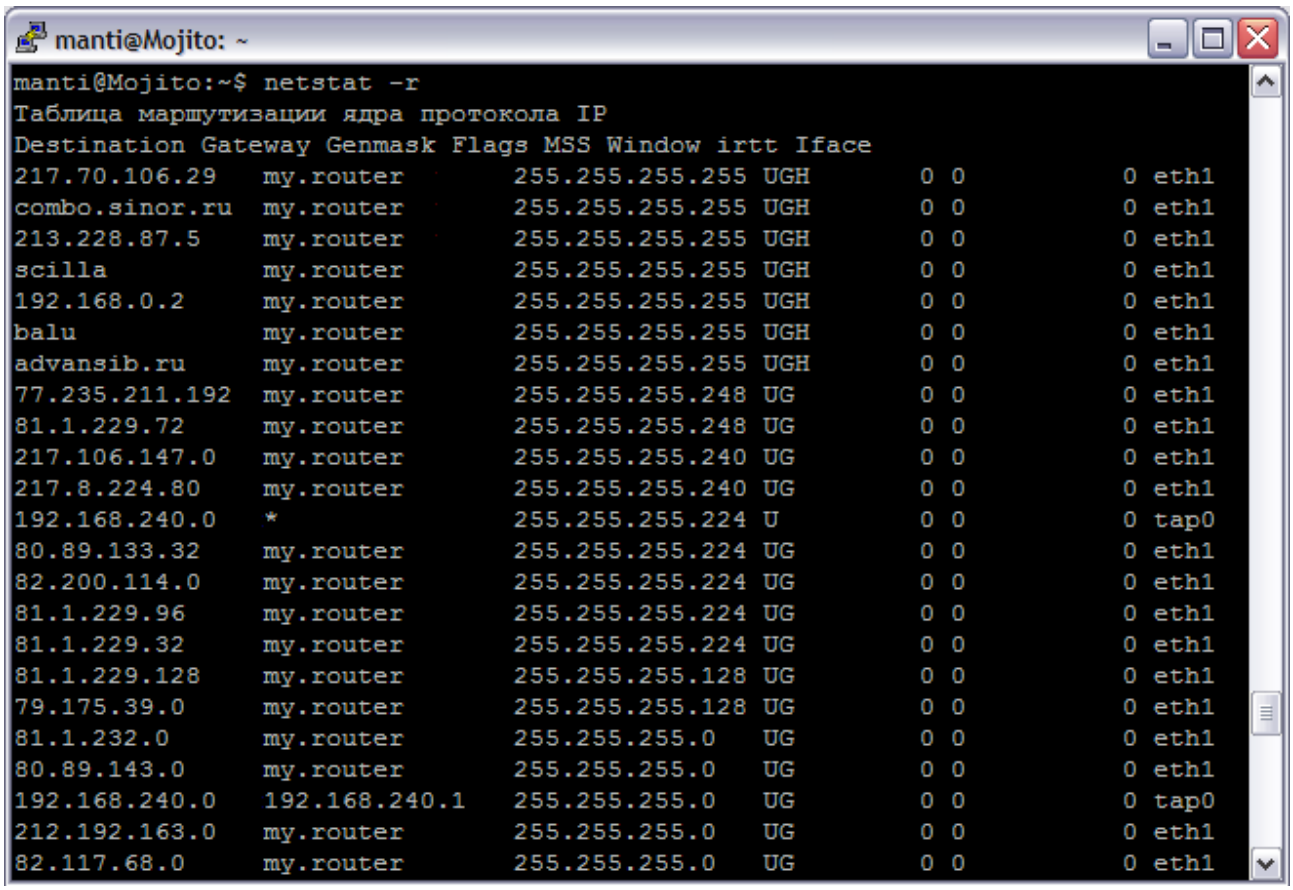


Рис. 5. Виведення таблиці маршрутизації

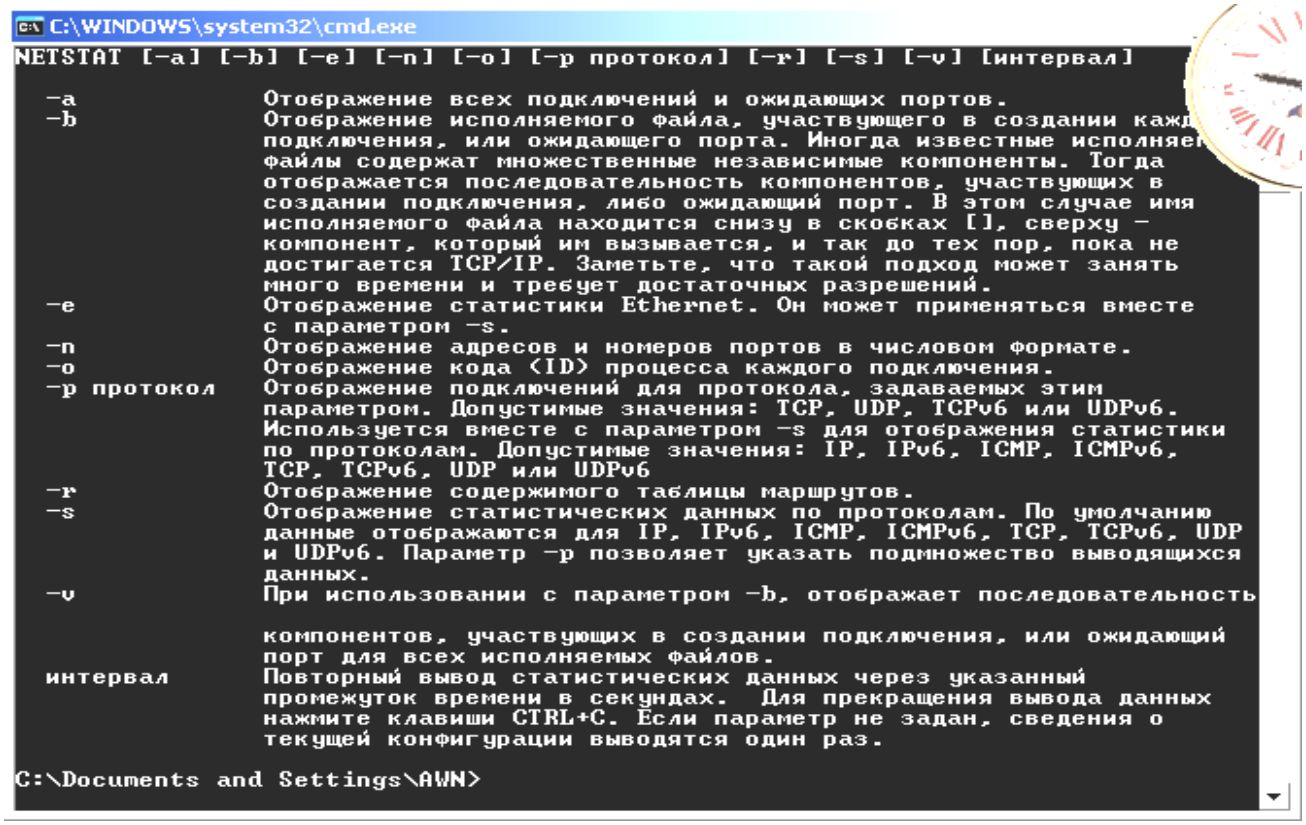


Рис. 6. Додаткові можливості утиліти

1.5. Утиліта Pathping

Надає інформацію про латентності мережі й втратах даних на проміжних вузлах між вихідним пунктом і пунктом призначення.

Команда **Pathping** протягом деякого періоду часу відправляє численні повідомлення з луну-запитом кожному маршрутизатору, що перебуває між вихідним пунктом і пунктом призначення, а потім на підставі пакетів, отриманих від кожного з них, обчислює результати (рис. 7).

```
C:\Documents and Settings\Admin>Pathping 172.29.1.1

Трассировка маршрута к 172.29.1.1 с максимальным числом прыжков 30

  0  pk27 [172.29.10.171]
  1     *        *        *
Подсчет статистики за: 25 сек. ...
          Исходный узел     Маршрутный узел
Прыжок   RTT    Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                              pk27 [172.29.10.171]
                                 100/ 100 =100%    |
  1  ---     100/ 100 =100%      0/ 100 =  0%  pk27 [0.0.0.0]

Трассировка завершена.
```

Рис. 7. Трасування маршруту

Оскільки **pathping** показує коефіцієнт втрати пакетів для кожного маршрутизатора або зв'язку, можна визначити маршрутизатори або субмережі, що мають проблеми з мережею. Команда **Pathping** виконує еквівалентне команді **tracert** дії, ідентифікуючи маршрутизатори, що перебувають на шляху. Потім вона періодично протягом заданого часу обмінюється пакетами з усіма маршрутизаторами й на підставі числа пакетів, отриманих від кожного з них, обробляє статистику. Запущена без параметрів, команда **pathping** виводить довідку.

pathping [-n] [-h максимальне_число_переходів] [-g список_вузлів] [-
період] [-q число_запитів [-w інтервал] [-T] [-R]
ім'я_кінцевого_комп'ютера]

Параметри:

[-n] Запобігає спробам команди pathping зіставити Ip-Адреси проміжних маршрутизаторів з їхніми іменами. Це дозволяє прискорити вивід результатів команди pathping.

[-h максимальне_число_переходів] Задає максимальну кількість переходів на шляху при пошуку кінцевого пункту призначення. Значення за замовчуванням рівно 30.

[-g список_вузлів] Указує для повідомлень із луну-запитом використання параметра вільної маршрутизації в Ip-Заголовку з набором проміжних місць призначення, зазначеним в списку_комп'ютерів. При вільній маршрутизації
послідовні проміжні місця призначення можуть бути розділено одним або декількома маршрутизаторами. Максимальне число адрес або імен у списку рівно 9. Список_адрес являє собою набір Ip-Адрес (у точечно-десятковій нотації), розділених пробілами.

[-p період] Задає час очікування між послідовними перевірками зв'язку (у мілісекундах). Значення за замовчуванням рівно 250 мілісекунд (1/4 секунди).

[-q число_запитів**]** Задає кількість повідомлень із луну-запитом, відправлених кожному маршрутизатору шляху. За замовчуванням —100.

[-w інтервал**]** Задає час очікування кожного відгуку (в мілісекундах). Значення за замовчуванням рівно 3000 мілісекунд (3 секунди).

[-T**]** Приєднує тег пріоритету рівня 2 (наприклад 802.1p) до повідомленням з луну-запитом, що відправляються кожному мережевому пристрою на маршруті. Це допомагає виявити мережеві пристрої, для яких не налагоджений пріоритет рівня 2. Він призначений для перевірки з'єднань, що використовують специфікації Qos.

[-R] Перевіряє, чи всі мережеві пристрої уздовж маршруту підтримують протокол RSVP (Resource Reservation Setup Protocol, протокол налаштування резервування ресурсів), який дозволяє головному комп'ютеру резервувати певну частину пропускної

здатності для потоку даних. Цей параметр призначений для перевірки з'єднань, що використовують специфікації Qos.
[ім'я_кінцевого_комп'ютера] Задає пункт призначення, ідентифікований Ip-Адресою або іменем вузла.
[/?] Відображає довідку в командному рядку.

1.6. Утиліта Route

Виводить на екран і змінює записи в локальній таблиці IP-маршрутизації (рис. 8). Запущена без параметрів, команда **route** виводить довідку (рис. 9).

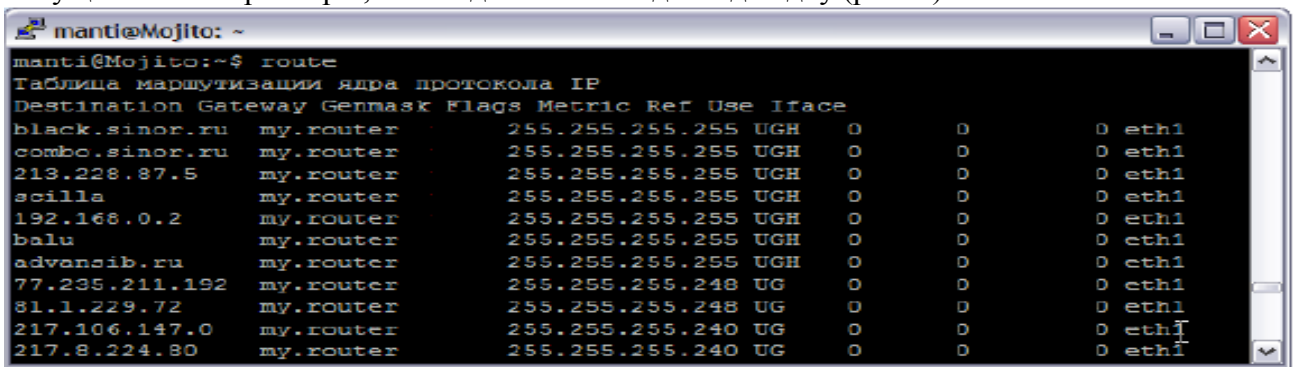


Рис. 8. Вивід таблиці маршрутизації

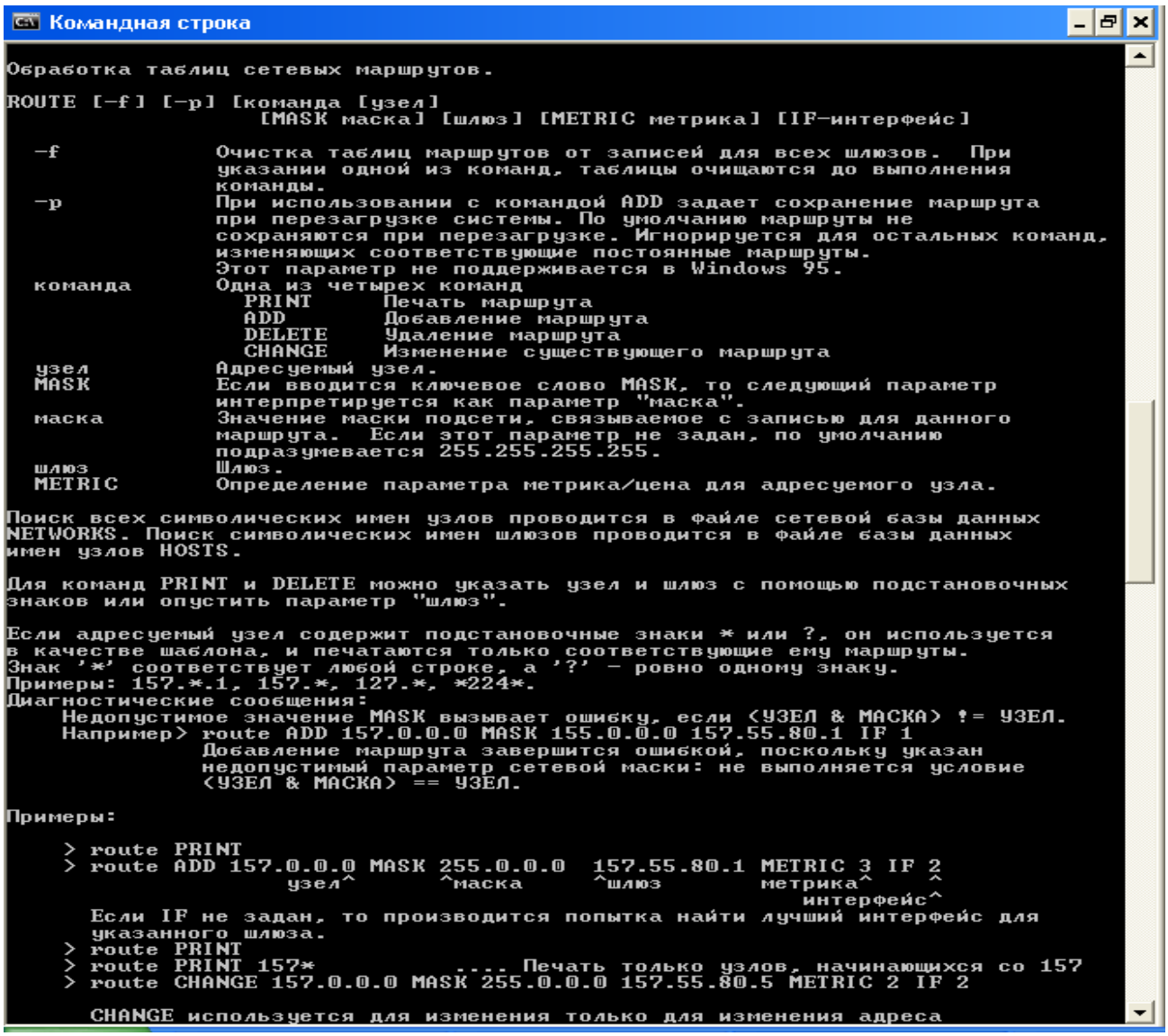


Рис. 9. Утиліта Route

route [-f] [-p] [команда [кінцева_крапка] [mask маска_мережі] [шлюз] [metric метрика]] [if інтерфейс]]

Параметри:

[-f] Очищає таблицю маршрутизації від усіх записів, які не є вузловими маршрутами (маршрути з маскою підмережі 255.255.255.255), мережевим маршрутом замикання на себе (маршрути з кінцевою крапкою 127.0.0.0 і маскою підмережі 255.0.0.0) або маршрутом багатоадресного розсилання (маршрути з кінцевою крапкою. 224.0.0.0 і маскою підмережі 240.0.0.0). При використанні даного параметра разом з однієї з команд (таких, як add, change або delete) таблиця очищається перед виконанням команди.

[-p] При використанні даного параметра з командою add зазначений маршрут додається до реєстру й використовується для ініціалізації таблиці Ip- Маршрутизації щораз при запуску протоколу TCP/IP. За замовчуванням додані маршрути не зберігаються при запуску протоколу TCP/IP. При використанні параметра з командою print виводить на екран список постійних маршрутів. Усі інші команди ігнорують цей параметр. Постійні маршрути зберігаються у реєстрі за адресою *HKEY_LOCAL_ MACHINE\SYSTEM\Currentcontrolset\ ervices\Tcpip\Parameters\Persistentroutes*

[команда] Указує команду, яка буде запущена на вилученій системі. У наступній таблиці представлений список припустимих параметрів.

[кінцева_крапка] Визначає кінцеву крапку маршруту. Кінцевою крапкою може бути мережева Ip-Адреса (де розряди вузла в мережній адресі мають значення 0), Ip-Адреса маршруту до вузла, або значення 0.0.0.0 для маршруту за замовчуванням.

[mask маска_мережі] Указує маску мережі (також відомої як маска підмережі) відповідно до крапки призначення. Маска мережі може бути маскою підмережі відповідної мережевій Ip-Адресі, наприклад 255.255. 255.255 для маршруту до вузла або 0.0.0.0. для маршруту за умовчанням. Якщо даний параметр пропущений, використовується маска підмережі 255.255.255.255. Кінцева крапка не може бути більш точною, ніж відповідна маска підмережі. Інакше кажучи, значення розряду 1 в адресі кінцевої крапки неможливе, якщо значення відповідного розряду в масці підмережі рівно 0.

[шлюз] Указує Ip-Адресу пересилання або наступного переходу, за яким доступний набір адрес, певний кінцевою крапкою й маскою підмережі. Для локально підключених маршрутів підмережі, адреса шлюзу – це Ip-Адреса, призначеного інтерфейсу, який підключений до підмережі. Для вилучених маршрутів, які доступні через один або кілька маршрутизаторів, адреса шлюзу – безпосередньо доступна Ip-Адреса найближчого маршрутизатора.

[metric метрика] Задає цілочисельну метрику вартості маршруту (у межах від 1 до 9999) для маршруту, який використовується при виборі в таблиці маршрутизації одного з декількох маршрутів, найбільше близько відповідного до адреси призначення пакета, що пересилається. Вибирається маршрут з найменшою метрикою. Метрика відбиває кількість переходів, швидкість проходження шляху, надійність шляху, пропускну здатність шляху й засобу адміністрування.

[if інтерфейс] Указує індекс інтерфейсу, через який доступна крапка призначення. Для виводу списку інтерфейсів і їх відповідних індексів використовуйте команду route print. Значення індексів інтерфейсів можуть бути як десяткові, так і шістнадцяткові. Перед шістнадцятковими номерами вводиться 0x. У випадку, коли параметр if пропущений, інтерфейс визначається з адреси шлюзу.

[/?] Відображає довідку в командному рядку.

Приклади команди **route:**

Щоб вивести на екран увесь уміст таблиці Ip-Маршрутизації, уведіть команду:

route print

Щоб вивести на екран маршрути з таблиці Ip-Маршрутизації, які починаються з 10., уведіть команду:

route print 10.*

Щоб додати маршрут за замовчуванням з адресою стандартного шлюзу 192.168.12.1, уведіть команду:

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

Щоб додати маршрут до кінцевої крапки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступною адресою переходу 10.27.0.1, уведіть команду:

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1

Щоб додати постійний маршрут до кінцевої крапки 10.41.0.0 з маскою підмережі 255.255.0.0 і наступною адресою переходу 10.27.0.1, уведіть команду:

route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1

1.7. Команда Ivconfig для пристрою «Ноутбук»

ivconfig [-h] [<interface>] [-e33id <e33id>] [-p <passvord>] [-addre33 <IP>] [-broadcast <broadcast-1P>] [-netmask <netaa3A-IP>] [-enable |di3able]

Засіб конфігурування бездротового інтерфейсу vlano. Команди із вказівкою бездротового інтерфейсу (vlaao), у якості аргументу, виводить поточний статус бездротового з'єднання.

Опція	Призначення
-h	Коротка довідка
interface	Вказівка інтерфейсу -.ЛапО
-e33id <e3sid>	Ідентифікатор бездротової мережі
-p <pa3svord>	Ключ доступу до бездротової мережі
-address <IP>	IP-Адреса інтерфейсу-лапо
-broadcast <broadcast-Ip>	Широкомовні!! адреси мережі
-netmask <netaa3>.-IP>	Маска підмережі
-enable!disable	Взаємовиключні аргументи. Включення (-епаЬ1е або відключення (-disable) безпроводового інтерфейсу >-1ап0

Приклад використання:

ivconfig vlano

ivconfig vlano -essid apl -p scrt -address 10.0.0.2 -netmask 2S5.0.0.0 -enable

ivconfig vlano -disable]

1.8. Утиліта ARP

Служить для виводу й зміни записів кеша протоколу ARP (рис. 10), який містить одну або кілька таблиць, що використовуються для зберігання Ip-Адрес і відповідних їм фізичних адрес Ethernet або Token Ring. Для кожного мережевого адаптера Ethernet або Token Ring, установленого в комп'ютері, використовується окрема таблиця.

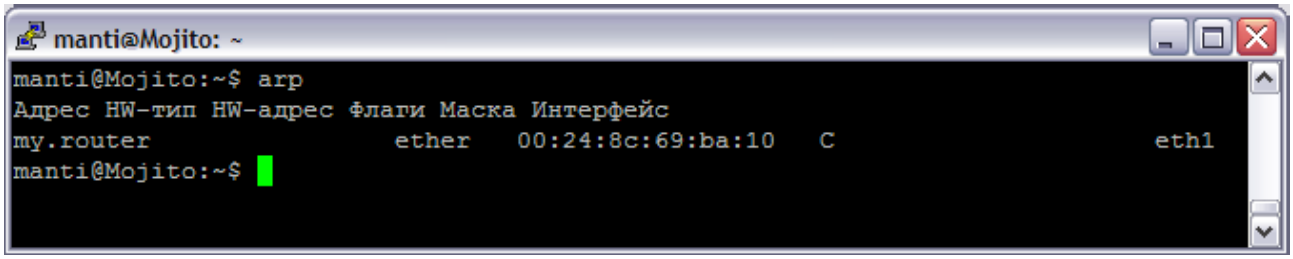


Рис. 10. Виведення таблиці поточного протоколу ARP для всіх інтерфейсів

2. Хід роботи
Варіанти виконання завдань.

Номер варіанту завдання вибирається за першою літерою прізвища студента:

Перша літера прізвища	Номер варіанту
А, Б, В, Г, Д,Е, Є ,Ж	**1**
З, І, Й,К, Л, М,Н,О	**2**
П, Р, С, Т, У,Ф, Х,	**3**
Ц, Ч, Ш, Щ, Ї, Ю, Я	**4**

Варіант 1

1) За допомогою утиліти **ipconfig** визначте параметри IP-конфігурації свого комп'ютера і результати представте у вигляді таблиці:

Параметр	Значення
IP-адреса комп'ютера	
Маска підмережі	
IP-адреса локального сервера імен	
IP-адреса основного шлюзу (маршрутизатора)	

2) За допомогою команди **Пуск- Программы- Стандартные- Связь- Сетевые подключения** відкрийте вікно **Сетевые подключения**. Виберіть в ньому значок мережевого адаптера і відкрийте вікно його стану, вибравши команду **Состояние** з контекстного меню. Порівняйте дані вкладки **Поддержка** з тими, що отримані в п.1.

3) Виходячи з IP-адреси вашого комп'ютера та користуючись даними табл. 1, визначте клас мережі, її номер та номер комп'ютера в мережі. Чи приймає маска мережі значення за замовченням для даного класу?

4) Використовуючи алгоритм, що рекомендується Microsoft, протестуйте з'єднання з віддаленими вузлами, що зазначені в таблиці.

IP-адреса вузла	Результати тестування – позитивний (+), негативний (-)
221.221.2.1	
127.33192.57	
192.168.1.1	
90.0.0.50	
133.15.67.20	
212.109.48.38	
191.12.80.5	
80.64.97.633	
195.35.65.35	
212.109.31.131	

5) За допомогою утиліти **ping** з ключем **– a** визначте доменні імена тих вузлів з попередньої таблиці (п.4), для яких результат тестування виявився позитивним. Результат подайте у вигляді таблиці:

IP-адреса вузла	**Доменне ім'я**

6) За допомогою утиліти **ping** визначте IP-адреси вузлів, чиї доменні імена наведені в таблиці.

Доменне ім'я вузла	**IP-адреса вузла**	**Клас мережі**
www.microsoft.com		
www.nasoa.edu.ua		
news.helsinki.fi		
ftp.funet.fi		
ftp.ipswitch.com		

7) Користуючись даними табл. 1, визначте класи мереж, до яких відноситься вузли з таблиці (п.6). Що можна сказати про розміри цих мереж?
8) За допомогою команди **tracert** визначте маршрути проходження пакетів до вузлів з останньої таблиці (п.6). Результати представте у вигляді схем.
9) За допомогою команди **netstat** визначте відкриті порти комп'ютера. Складіть їх список.

Варіант 2

1) За допомогою утиліти **ipconfig** визначте параметри IP-конфігурації свого комп'ютера і результати представте у вигляді таблиці:

Параметр	**Значення**
IP-адреса комп'ютера	
Маска підмережі	
IP-адреса локального сервера імен	
IP-адреса основного шлюзу (маршрутизатора)	

2) За допомогою команди **Пуск- Программы- Стандартные- Связь- Сетевые подключения** відкрийте вікно **Сетевые подключения**. Виберіть в ньому значок мережевого адаптера і відкрийте вікно його стану, вибравши команду **Состояние** з контекстного меню. Порівняйте дані вкладки **Поддержка** з тими, що отримані в п.1.
3) Виходячи з IP-адреси вашого комп'ютера та користуючись даними табл. 1, визначте клас мережі, її номер та номер комп'ютера в мережі. Чи приймає маска мережі значення за замовченням для даного класу?
4) Використовуючи алгоритм, що рекомендується Microsoft, протестуйте з'єднання з віддаленими вузлами, що зазначені в таблиці.

IP-адреса вузла	**Результати тестування – позитивний (+), негативний (-)**
156.21.4.254	
115.78.31.10	
192.168.1.1	
90.0.0.50	

207.105.75.31	
212.42.64.10	
125.12.31.5	
62.218.15.1	
205.24.238.16	
208.175.238.97	

5) За допомогою утиліти **ping** з ключем – а визначте доменні імена тих вузлів з попередньої таблиці (п.4), для яких результат тестування виявився позитивним. Результат подайте у вигляді таблиці:

IP-адреса вузла	**Доменне ім'я**

6) За допомогою утиліти **ping** визначте IP-адреси вузлів, чиї доменні імена наведені в таблиці.

Доменне ім'я вузла	**IP-адреса вузла**	**Клас мережі**
mail.yahom.com		
www.nasoa.edu.ua		
search.yahom.com		
ftp.ics.org		
meta-ukraine.com.ua		

7) Користуючись даними табл. 1, визначте класи мереж, до яких відноситься вузли з таблиці (п.6). Що можна сказати про розміри цих мереж?
8) За допомогою команди **tracert** визначте маршрути проходження пакетів до вузлів з останньої таблиці (п.6). Результати представте у вигляді схем.
9) За допомогою команди **netstat** визначте протоколи за якими виконані підключення вашого комп'ютера. Складіть їх список.

Варіант 3

1) За допомогою утиліти **ipconfig** визначте параметри IP-конфігурації свого комп'ютера і результати представте у вигляді таблиці:

Параметр	**Значення**
IP-адреса комп'ютера	
Маска підмережі	
IP-адреса локального сервера імен	
IP-адреса основного шлюзу (маршрутизатора)	

2) За допомогою команди **Пуск- Программы- Стандартные- Связь- Сетевые подключения** відкрийте вікно **Сетевые подключения**. Виберіть в ньому значок мережевого адаптера і відкрийте вікно його стану, вибравши команду **Состояние** з контекстного меню. Порівняйте дані вкладки **Поддержка** з тими, що отримані в п.1.
3) Виходячи з IP-адреси вашого комп'ютера та користуючись даними табл. 1, визначте клас мережі, її номер та номер комп'ютера в мережі. Чи приймає маска мережі значення за замовченням для даного класу?
4) Використовуючи алгоритм, що рекомендується Microsoft, протестуйте з'єднання з віддаленими вузлами, що зазначені в таблиці.

IP-адреса вузла	Результати тестування – позитивний (+), негативний (-)
217.20.163.18	
212.42.64.10	
192.168.1.1	
90.0.0.50	
207.105.75.31	
194.87.13.37	
11.240.123.15	
156.21.4.254	
201.105.75.31	
62.218.15.1	

5) За допомогою утиліти **ping** з ключем – а визначте доменні імена тих вузлів з попередньої таблиці (п.4), для яких результат тестування виявився позитивним. Результат подайте у вигляді таблиці:

IP-адреса вузла	Доменне ім'я

6) За допомогою утиліти **ping** визначте IP-адреси вузлів, чиї доменні імена наведені в таблиці.

Доменне ім'я вузла	IP-адреса вузла	Клас мережі
www.borland.com		
ftp.iit.iapm.edu.ua		
news.lucky.net		
ddt.demos.su		
www.nasoa.edu.ua		

7) Користуючись даними табл. 1, визначте класи мереж, до яких відноситься вузли з таблиці (п.6). Що можна сказати про розміри цих мереж?

8) За допомогою команди **tracert** визначте маршрути проходження пакетів до вузлів з останньої таблиці (п.6). Результати представте у вигляді схем.

9) За допомогою команди **netstat** покажіть таблицю маршрутів. Складіть їх список.

Варіант 4

1) За допомогою утиліти **ipconfig** визначте параметри IP-конфігурації свого комп'ютера і результати представте у вигляді таблиці:

Параметр	Значення
IP-адреса комп'ютера	
Маска підмережі	
IP-адреса локального сервера імен	
IP-адреса основного шлюзу (маршрутизатора)	

2) За допомогою команди **Пуск- Программы- Стандартные- Связь- Сетевые подключения** відкрийте вікно **Сетевые подключения**. Виберіть в ньому значок мережевого адаптера і відкрийте вікно його стану, вибравши команду **Состояние** з контекстного меню. Порівняйте дані вкладки **Поддержка** з тими, що отримані в п.1.

3) Виходячи з IP-адреси вашого комп'ютера та користуючись даними табл. 1, визначте клас мережі, її номер та номер комп'ютера в мережі. Чи приймає маска мережі значення за замовченням для даного класу?
4) Використовуючи алгоритм, що рекомендується Microsoft, протестуйте з'єднання з віддаленими вузлами, що зазначені в таблиці.

IP-адреса вузла	**Результати тестування – позитивний (+), негативний (-)**
221.221.2.1	
127.33192.57	
192.168.1.1	
90.0.0.50	
133.15.67.20	
212.42.64.10	
125.12.31.5	
62.218.15.1	
205.24.238.16	
208.175.238.97	

5) За допомогою утиліти **ping** з ключем – а визначте доменні імена тих вузлів з попередньої таблиці (п.4), для яких результат тестування виявився позитивним. Результат подайте у вигляді таблиці:

IP-адреса вузла	**Доменне ім'я**

6) За допомогою утиліти **ping** визначте IP-адреси вузлів, чиї доменні імена наведені в таблиці.

Доменне ім'я вузла	**IP-адреса вузла**	**Клас мережі**
www.borland.com		
ftp.iit.iapm.edu.ua		
news.lucky.net		
ddt.demos.su		
www.nasoa.edu.ua		

7) Користуючись даними табл. 1, визначте класи мереж, до яких відноситься вузли з таблиці (п.6). Що можна сказати про розміри цих мереж?
8) За допомогою команди **tracert** визначте маршрути проходження пакетів до вузлів з останньої таблиці (п.6). Результати представте у вигляді схем.
9) За допомогою команди **netstat** покажіть статистичні дані про підключення вашого комп'ютера. Складіть їх список.

3. Контрольні питання

1. Як при роботі з командним рядком швидко повторити останню команду? Як повторити команду, яка вже вводилась раніше?
2. Як при роботі з командним рядком отримати довідку про використання утиліт ipconfig, ping, tracert?
3. Для чого призначена утиліта ipconfig? Як її викликати?
4. Які дані виводяться у випадку виклику утиліти ipconfig без додаткових ключів? Чи можливо отримати ті ж дані іншим способом?

5. Які існують класи мереж? Що лежить в основі поділу мереж на класи?
6. Яку інформацію можна отримати з аналізу IP-адреси?
7. Яку функцію в мережі виконують DNS-сервери?
8. Як протестувати з'єднання з віддаленим хостом?
9. Як визначити доменне ім'я хосту з відомою IP-адресою?
10. Як визначити IP-адресу хосту з вказаним доменним ім'ям?
11. За допомогою якої утиліти можна з'ясувати, на яких ланках маршруту слідування відбувається затримка пакетів?
12. Як визначити маршрут проходження пакетів до віддаленого вузла?

РОЗДІЛ 2. КОРПОРАТИВНІ МЕРЕЖІ

ЛАБОРАТОРНА РОБОТА 9.

МОНТАЖ І НАЛАГОДЖЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI

Мета роботи: практично освоїти монтаж і налагодження бездротової мережі Wi-Fi

Зміст

1. Теорія
2. Хід роботи
2.1. Налагодження мережі зі статичною адресою комп'ютера клієнта.
2.2. Налагодження крапки доступу Wi-Fi і Dhcp-Сервера.
2.3. Перевірка роботи бездротової мережі.
2.4. Налагодження мережі з динамічною адресою комп'ютера клієнта.
2.5. Перевірка роботи бездротової мережі.
3. Контрольні питання

1. Теорія

У сучасному світі все більше застосування знаходять безпроводові мережі Wi-Fi, що дозволяють давати клієнтам доступ до ресурсів мереж, наприклад до **Internet**, з ноутбука або персонального комп'ютера, використовуючи в якості середовища передачі даних радіоканал, що не вимагає наявності спеціальних провідних з'єднань клієнтів з мережею, забезпечуючи в такий спосіб їх мобільність.

Переваги Wi-Fi

Відсутність проводів. Передача даних у мережі здійснюється за радіоканалом . Можлива установка в місцях, де прокладка кабельної мережі за тими або іншими причинам неможлива або недоцільна, наприклад на виставках, залах для нарад.

Мобільність, як робочих місць, так і самого офісу. Тому що бездротова мережа не прив'язана до кабелів, Ви можете вільно змінювати місце розташування комп'ютерів у зоні покриття крапки доступу, не турбуючись про порушення зв'язку. Мережа легко монтується/демонтуються, при переїзді в інше приміщення Ви можете навіть забрати свою мережу із собою.

Недоліки Wi-Fi

Відносно висока вартість устаткування

Невелика дальність дії 50-100 метрів

Велика небезпека несанкціонованого підключення до мережі сторонніх користувачів

У пропонованій лабораторній роботі ***ми освоїмо*** створення найпростішої мережі Wi-Fi на прикладі підключення ноутбуків до крапки доступу Wi-Fi з використанням статичної й динамічної Ip-Адресації.

Схема мережі має такий вигляд (рис. 1):

1. Включіть ноутбуки. Після завантаження операційної системи на ноутбуках, на обох адаптерах повинні загорітися сигнальні лампочки, що свідчать про установку радіообміну між адаптерами й крапкою доступу.
2. Мережа зібрана, тепер її необхідно налагодити.

2. Хід роботи

2.1. Налагодження мережі зі статичною адресою комп'ютера клієнта.

Налагодження мережі полягає в установці **протоколів ноутбука клієнта**, які необхідні для його роботи, а так само включення й налагодження DHCP-**Сервера**, який перебуває в крапці доступу.

Протокол – це спеціальна програма, за допомогою якої комп'ютери мережі обмінюються між собою даними за спеціальними правилами. У нашій мережі робочим протоколом буде протокол **TCP/IP**. Щоб комп'ютери могли обмінюватися між собою

даними цей протокол повинен бути встановлений на всіх комп'ютерах, які перебувають у мережі.

На **ноутбуці сервері** протокол TCP/IP уже встановлений, нам залишилося встановити й налагодити цей протокол на **ноутбуці клієнтові** (див. схему мережі).

На ноутбуці №2 виконаєте наступні дії:

Рис. 1. Схема мережі

1. Клацніть правою клавішею миші на значку «**Сетевое окружение**» 

, виберіть у меню «**Свойства**». Відкриється список мережевих підключень (рис. 2).

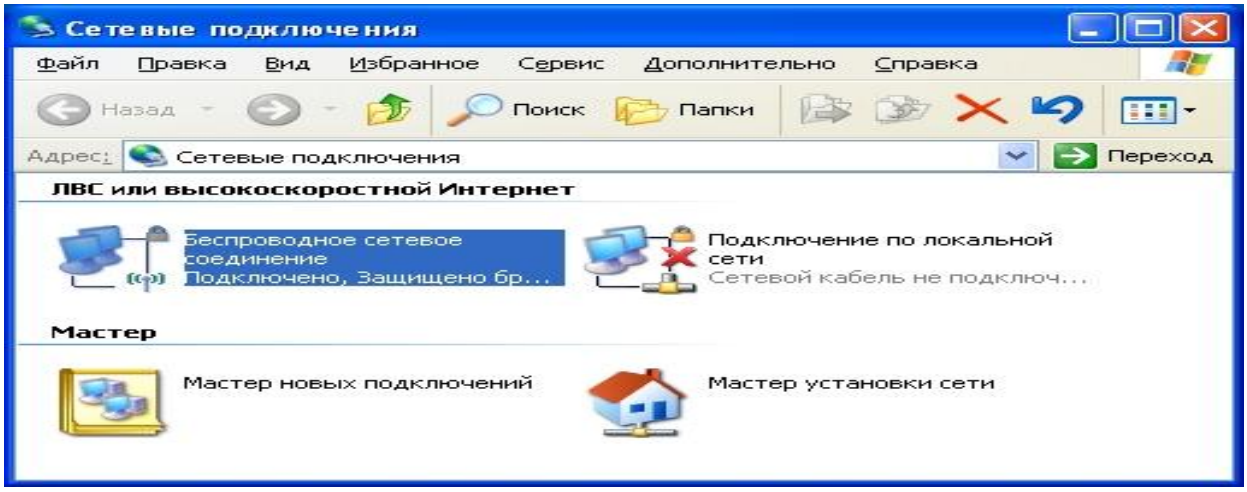


Рис. 2. Схема мережевих підключень

2. Виберіть у списку «**Безпроводовое сетевое соединение**», клацніть по ньому правою клавішею миші й виберіть пункт «**Свойства**». Відкриється вікно властивостей з'єднання (рис. 3).

3. У вікні, що з'явилося, виберіть **«Протокол Интернета (TCP/IP)»**, натисніть **«Свойства»**. Відкриється вікно налагодження протоколу (рис. 3). Активуйте прапорець «**Использовать следующий Ір-Адрес**». Уведіть у поля Ір-**Адреса** й **Маска підмережі** адреси установок, які зображені на рис. 4.

Тут

192.168.0.10 – це Ip-Адреса комп'ютера в мережі.

255.255.255.0 – маска підмережі. Це спеціальний параметр, який разом з адресою однозначно визначає мережу, у якій перебуває комп'ютер.

4. Після введення налагодження, натисніть «**ОК**», вікно «**Свойства: Протокол Інтернета (TCP/IP)**» закриється. У вікні «**Безпроводовое сетевое соединение**» (рис. 2) натисніть «**ОК**».

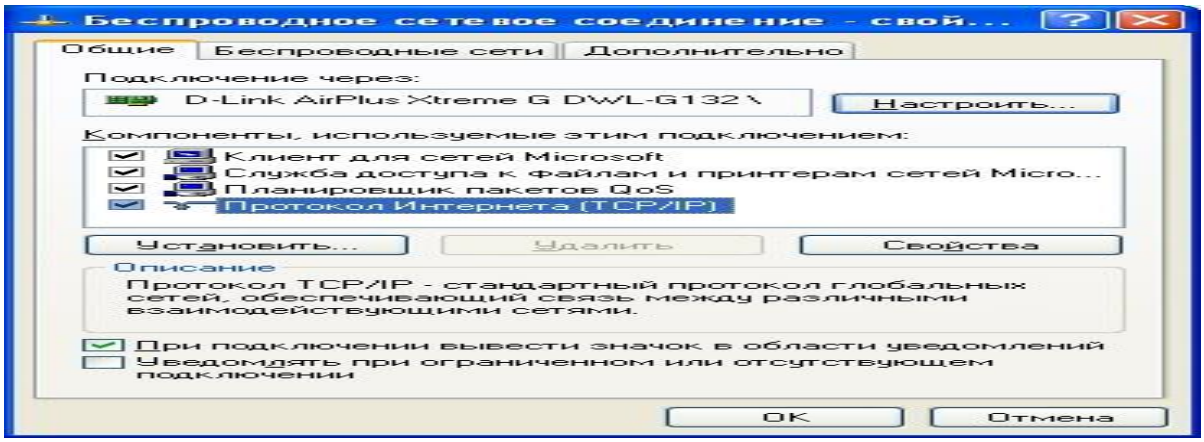


Рис. 3. Вікно властивостей

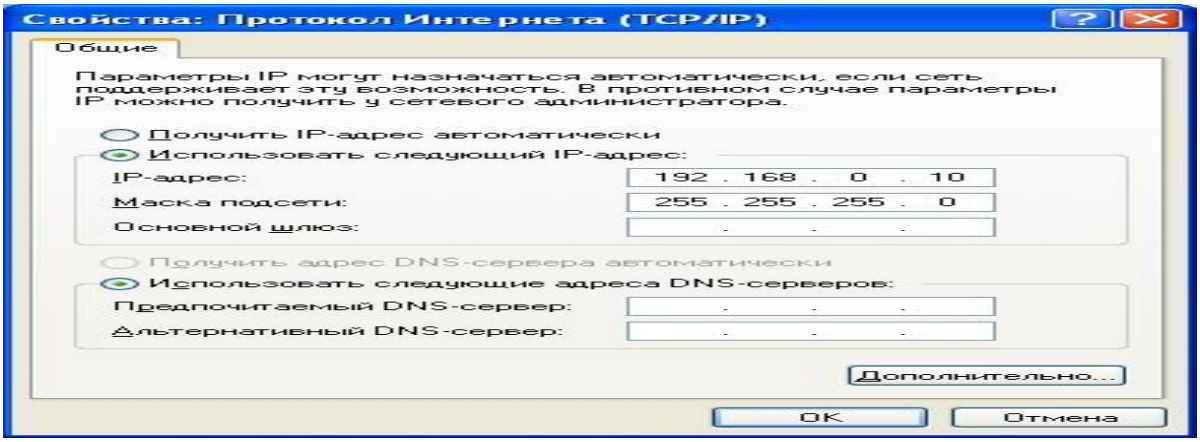


Рис. 4. Введення параметрів мережі

Ми налагодили ноутбук клієнт для роботи з бездротовою мережею. Для ноутбука прописана статична Ip-Адреса, це означає що ми привласнили ноутбуку виділену, постійну Ip-Адресу та інші налагодження, які можна міняти й призначати тільки вручну. Статична Ip-Адреса нам необхідна для того, щоб підключитися до крапки доступу Wi-Fi і щоб інші комп'ютери в мережі могли з ним зв'язуватися.

Для того щоб почала функціонувати мережа **Wi-Fi** необхідно налагодити крапку доступу.

2.2. Налагодження крапки доступу Wi-Fi і DHCP-Сервера.

1. Завантажите оглядач **Internet Explorer**. Уведіть у його адресному рядку адресу: http://192.168.0.50/ Це Ip-Адреса **крапки доступу Wi-Fi**. За цією адресою розташована система її конфігурації. Вхід у систему конфігурації захищений логіном і паролем і на екрані з'явиться вікно для введення цих даних (рис. 5).

Уведіть **Користувач – admin, Пароль – admin (**якщо до цього не міняв записи**)** і натисніть кнопку «**ОК**».

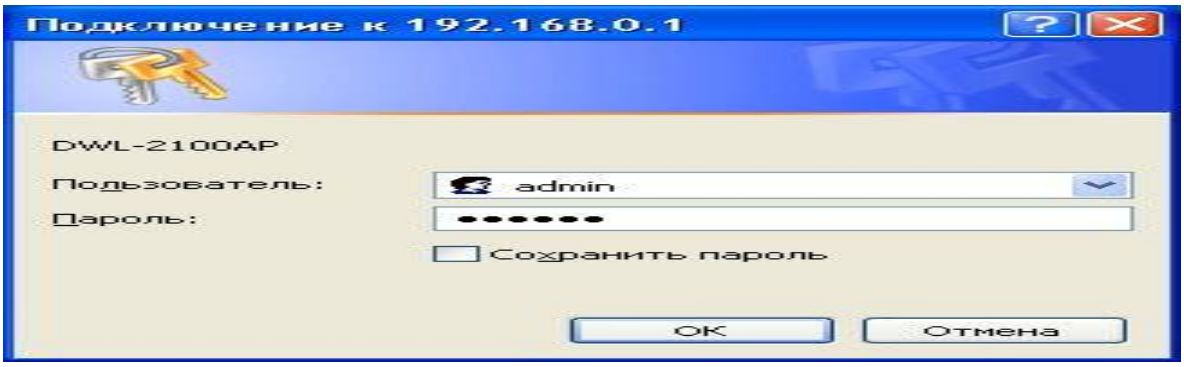


Рис. 5. Введення логіну та паролю

Відкриється головна сторінка систему конфігурації крапки доступу Wi-Fi.

2. Клацніть по кнопці 

. Відкриється сторінка розширених налагодження крапки доступу.

3. Клацніть по кнопці 

. Відкриється сторінка для зміни налагодження Dhcp-**Сервера**.

Установіть наступні параметри **DHCP**, або змініть існуючі, якщо вони не збігаються із зазначеними:

1. Function Enable / Disable – **Enabled**
2. IP Assigned From – **192.168.0.51**
3. The Range Of Pool (1-255) – **200**
4. Submask – **255.255.255.0**
5. lease Time (60 – 31536000 sec) – **10000000**
6. Status **– ON**

Клацніть по кнопці 

щоб зберегти зроблені налагодження. Крапка доступу **Wi-Fi** піде на перезавантаження, яке займає приблизно півхвилини.

Виконані вище налагодження забезпечують виконання наступних функцій:

Function Enable/Disable – Включає (Enabled) або відключає (Disabled) Dhcp-Сервер.

IP Assigned From – задає початкову Ip-адресу, з якої починається діапазон Ip-адрес, що виділяються динамічно користувачам (користувачі, які підключаються тимчасово).

The Range of Pool – задає кінець діапазону Ip-адрес, кінцеве значення останньої цифри Ip-адреси.

У такий спосіб у нашім прикладі ми задали діапазон Ip-адрес від **192.168.0.51** до **192.168.0.200** включно.

Submask – маска підмережі. Це спеціальний параметр, який разом з адресою однозначно визначає мережу, у якій перебуває комп'ютер.

Lease Time – час «життя» виділених користувачеві мережевих налагодження. При динамічній адресації налагодження користувача існують певний час, після чого скидаються й програмне забезпечення користувача запитує нові налагодження. Тут задається час існування виділених користувачеві налагодження (у секундах).

Status – спеціальний параметр, він ставиться в значення **ON**, якщо в мережі використовується спільно **динамічна** й **статична** адресації. У нашім випадку цей параметр установлений в **ON**, оскільки на **ноутбуці клієнта** прописана статична, постійна адреса.

2.3. Перевірка працездатності бездротової мережі.

Після того, як мережа налагоджена, потрібно перевірити її роботу й переконатися, що комп'ютери можуть обмінюватися даними між собою. *Необхідно знати*, що в мережі можуть існувати самі різні служби й сервіси, кожний з який виконує свої завдання. У мережі, яку ми налагодили працюють дві служби: локальний Web-**Сервер**, призначений для розміщення HTML-Сторінок у мережі, і **Мережа Microsoft**, за допомогою якої проводиться обмін файлами й спільна робота із клієнтами.

Спочатку перевіримо роботу Web-**Сервера**.Web-**Сервер** установлений на **ноутбуці сервер**. Для того, щоб перевірити роботу Web-**Сервера**, запустіть на **ноутбуці №2** (комп'ютер Клієнт) оглядач Internet **Internet Explorer** і в його адресному рядку введіть **http://192.168.0.3/wifi/**

Якщо сторінка завантажиться, дійте відповідно до вказівок, написаних на цій сторінці.

Якщо сторінка не завантажилася, значить мережа налагоджена неправильно. Тоді зробіть наступне:

1. Перевірте ще раз налагодження протоколу TCP/IP **ноутбука клієнта** й переконайтеся що вони введені правильно.
2. Якщо помилка не зникає, покличте викладача.

Запам'ятаєте. Статична Ip-адресація має наступні недоліки:

1. Для того, щоб довідатися всі налагодження мережі, необхідно звернутися до адміністратора мережі, який повинен індивідуально виділити для кожного клієнта свій унікальний Ip-адреса. Це незручно як для клієнта, так і для адміністратора.
2. При підключенні до якої-небудь іншої бездротової мережі, налагодження комп'ютера клієнта доводиться знову змінювати параметри під нову мережу, пізнаючи їх в адміністратора.
3. Якщо випадково ваші налагодження збіжаться з налагодженнями іншого клієнта, ви не зможете підключитися до мережі.

УСІХ ЗАЗНАЧЕНИХ НЕДОЛІКІВ ПОЗБАВЛЕНА ДИНАМІЧНА IP-АДРЕСАЦІЯ.

2.4. Налагодження мережі з динамічною адресою комп'ютера клієнта

Динамічна Ip-адресація здійснюється за допомогою DHCP-**Сервера**, який перебуває в крапці доступу. Розберемося що це таке.

DHCP-Сервер використовує **DHCP** протокол **(англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла)** – це мережевий протокол, що дозволяє комп'ютерам автоматично одержувати Ip-адресу й інші параметри, необхідні для роботи в мережі **TCP/IP**. Для цього комп'ютер, що підключається до мережі, звертається до сервера, **DHCP**, який на час проведення сеансу роботи з мережею видає **динамічну Ip-адресу.** Це дозволяє уникнути ручного налагодження комп'ютерів мережі, зменшує кількість помилок і дозволяє клієнтам швидко підключатися до мережі не витрачаючи час на налагодження протоколів зв'язки вручну.

Налагодження ноутбука на динамічну Ip-Адресацію.

1. Поверніться до початку лабораторної роботи, де ви здійснювали налагодження мережі ноутбука №2. (Розділ «**Налагодження мережі**»).
2. Повторіть кроки 1-3, тільки на 3-м кроці, де ви вводили статичний Ip-адресу активуйте прапорець «**Получить Ip-адрес автоматически**». Це опція й включає динамічну Ip-адресацію.
3. Натисніть «**ОК**», вікно «**Свойства: Протокол Інтернета (TCP/IP)**» закриється. У вікні «**Безпроводовое сетевое окружение**» (рис. 2) натисніть «**ОК**».

Динамічна Ip-адресація на ноутбуці налагоджена!

Перевірка динамічної Ip-адресації.

1. Використовуючи процедуру «Безпечного добування пристрою» відключіть Wi-Fi адаптер **від** ноутбука клієнта**.** Вона виконується так само, як і при відключенні флеш-карт.

2. Вилучіть адаптер з роз'єму USB.

3. Почекайте кілька секунд і знову вставте адаптер у роз'єм USB. Відбудеться автоматичне підключення ноутбука клієнта до бездротової мережі Wi-Fi і ноутбуку будуть динамічно привласнені Ip-Адреса та інші мережеві налагодження.

Для того, щоб переконатися в тому, що мережеві налагодження були динамічно привласнені, зробіть наступне:

1. Відкрийте «**Пуск / Стандартные / Командная строка**». З'явиться рядок для введення команд операційної системи**.**

2. Уведіть у рядку команду:

ipconfig **і натисніть** Enter.

Ця команда відображає на екран налагодження протоколу TCP/IP вашого комп'ютера (рис. 6).

Рис. 6. Параметри безпроводової мережі

Якщо зазначена командою Ip-адреса комп'ютера перебуває в діапазоні 192.168.0.51 – 192.168.0.200, значить динамічна Ip-адресація працює нормально.

У випадку, якщо зазначена командою Ip-адреса комп'ютера НЕ перебуває в діапазоні 192.168.0.51 – 192.168.0.200), необхідно:

1. Провести налагодження мережі заново, установивши статичну Ip-адресу, потім, підключившись до крапки доступу Wi-Fi перевірити, чи включений – DHCP-Сервер і чи правильно виставлені його параметри.

2. Якщо помилка не зникла – звертайтеся до викладача.

2.5. Перевірка роботи бездротової мережі.

Спочатку перевіримо роботу Web-Сервера.Web-Сервер установлений на ноутбуці сервері. Для того, щоб перевірити роботу Web-Сервера, запустіть на **ноутбуці клієнтові** оглядач Internet **Internet Explorer** і в його адресному рядку введіть http://192.168.0.3/wifi/

Якщо сторінка завантажиться, дійте відповідно до вказівок, написаних на цій сторінці.

Якщо сторінка не завантажилася, значить мережа налагоджена неправильно. Тоді зробіть наступне:

1. Перевірте ще раз налагодження протоколу TCP/IP ноутбука №2 і переконаєтеся що вони введені правильно. Ip-адрес повинен призначатися динамічно, включіть динамічну адресацію, якщо це не було зроблено.

2. Якщо помилка не зникає, покличте викладача.

3. Контрольні питання

1. Які переваги та недоліки має безпроводова мережа?
2. Як налаштувати мережу зі статичною адресою комп'ютера клієнта?
3. Як налаштувати крапку доступу Wi-Fi і DHCP-Сервера?
4. Як перевірити працездатність бездротової мережі?
5. Як налаштувати мережу з динамічною адресою комп'ютера клієнта?

ЛАБОРАТОРНА РОБОТА 10. НАЛАГОДЖЕННЯ WI-FI РОУТЕРА

Мета роботи: вміти налагоджувати WI-FI роутер.

Зміст

1. Теорія
2. Хід роботи
2. 1. Установлення паролю на доступ до налагодження Wi-Fi роутера
2.2. Установлення паролю на Wi-Fi мережу й установлення типу шифрування
2.3. Приховування імені мережі (SSID)
2. 4. Включення фільтрації пристроїв за MAC адресами
2. 5. Відключення служби QSS (WPS)
3. Контрольні питання

1. Теорія

Маршрутизатор (англ. router) – електронний пристрій, який використовується для об'єднання двох або більш мереж і управляє процесом маршрутизації, тобто на підставі інформації про топологію мережі й установлених правил ухвалює рішення щодо пересилання пакетів мережевого рівня між різними сегментами мережі (рис. 1).

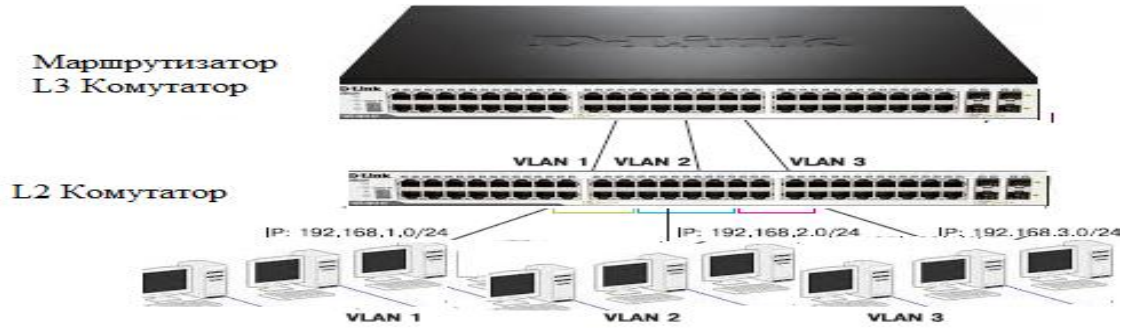


Рис. 1. Мережі

Слід зазначити, що назва "роутер" у пошукових запитах і, відповідно, у повсякденній мові зустрічається набагато частіше, чим "маршрутизатор". Приймання–передача даних за стандартом Wi-Fi може бути в декількох діапазонах. Основні діапазони представлені нижче:

- 2,4 Ггц (найбільш популярний, тому в більшості місць сильно перевантажений, що негативно може позначитися на швидкості передачі даних. У теж час, роботу в цьому діапазоні підтримує більшість сучасних гаджетів. При маркуванні пристрою використовується "2");
- 5 Ггц (менш популярний. Багато провайдерів використовують цей діапазон для подачі Internet, якщо це зробити за дротовим інтерфейсом неможливо. Деякі сучасні пристрої підтримують обоє діапазони. При маркування пристрою використовується "5").

Існують також пристрої для роботи в інших діапазонах (наприклад, 3 Ггц або 900 Мгц). Але 99% домашніх пристроїв такі частоти не підтримують.

Передача даних за Wi-Fi здійснюється згідно з певними стандартами. У таблиці 1 представлені основні характеристики, які необхідно розуміти при виборі Wi-Fi маршрутизатора.

Останній стандарт тільки (802.11ac) в 2014 році почав впроваджуватися. У першу чергу використовується для підключення до провайдера. Але, незважаючи на це, деякі топові моделі телефонів і планшетів уже його підтримують. Більшість телефонів, планшетів, які підтримують стандарт 802.11n, мають тільки одну Wifi антену, тому максимальна реальна швидкість у них 55 Мбіт/с.

У таблиці стандарти представлені в порядку їх появи. Нові стандарти мають зворотну сумісність, тобто якщо у Вас ноутбук працює в стандарті 802.11b, він нормально

Таблиця 1

Основні характеристики Wi-Fi маршрутизатора

Стандарт	**Діапазон**	**Максимальна швидкість передачі, МБіт/сек**		**Особливості**
		канальна	**реальна**	
802.11a	5 ГГц	108	40	чутливий до перешкод
802.11b	2,4 ГГц	11	5	працюють старі пристрої
802.11g	2,4 ГГц	54	24	
802.11n	2,4 ГГц,			
5 ГГц	150	55	при 1 антені	
		300	110	при 2-х антенах
		450	165	при 3-х антенах
		600	220	при 4-х антенах
802.11ac	5 ГГц	433-6770	більш 200	залежить від кількості антен.

підключиться до Wi-Fi роутеру 802.11n, але при цьому швидкість обміну даними буде не більш 11 Мбіт/сек. Слід урахувати, що в цей момент часу вся крапка доступу перемикається в цей режим, тобто всі абонентські пристрої будуть працювати за стандартом 802.11b.

Швидкість Wifi не повинна бути менше швидкості Internet, а то роутер буде "різати" швидкість. Але слід урахувати, що якщо швидкість Wifi вашого ноутбука (планшета) буде нижче швидкості Wi-Fi роутера й Internet, тоді проблема зниження швидкості буде у вашім пристрої. Швидкість за проводами (через Lan-Порту) звичайно вище ніж за Wi-Fi.

При покупці роутера необхідно уточнити максимальну кількість пристроїв, які одночасно можуть бути до нього підключені й ця кількість повинна бути більше, ніж сьогоднішні потреби. До речі, не забувайте про перспективу.

Залежно від інтерфейсу підключення до глобальної мережі (Wan-Порту) маршрутизатори можна розділити на:

- xdsl Wi-Fi роутери (підключення до мережі провайдера здійснюється за однією з технологій сімейства xdsl, наприклад, оператор Укртелеком використовує технологію ADSL. Максимальна швидкість передачі за стандартом ADSL2+ становить 24 Мбіт/с)
- 3G/4G Wi-Fi роутери (використовується бездротове підключення. Максимальна швидкість підключення до Інтертелекому за технологією EVDO-B – 14 Мбіт/с).
- Ethernet Wi-Fi роутери (при підключення до Internet використовується "кручені пари". Максимальна швидкість при підключенні за стандартом Fast Ethernet – 100 Мбіт/с, Gigabit Ethernet – 1 Гбіт/с)
- SFP Wi-Fi роутери (підключення здійснюється за оптоволоконним кабелем й швидкість може досягати 1 Гбіт/с)
- EPON/GEPON/GPON Wi-Fi роутери (підключення здійснюється до PON мережі. Зараз технологія яка найбільш развивається для підключення приватного сектору, сіл і котеджей. Швидкість при використанні технології EPON (GEPON/GPON) до 1 Гбіт/с, 10GEPON – до 10 Гбіт/с)

- DOCSIS Wi-Fi роутери (підключення здійснюється через телевізійний кабель. Максимальна швидкість при використанні технології Eurodocsis 2.0: приймання даних 50 Мбіт/с, передача - 27 Мбіт/с)
- Wi-Fi роутери (підключення до провайдера здійснюється за бездротовим інтерфейсом).
- універсальні Wi-Fi роутери (які дозволяють підключиться за декількома технологіями).

Внутрішня організація пристрою така: у пам'яті в нього зберігається таблиця, яка містить шляхи до всіх пристроїв у мережі, а також до інших маршрутизаторів. Виходить така зв'язана мережа пристроїв, до кожного з яких можна підібрати найбільш оптимальний і короткий шлях. Роутер (рис. 2) періодично відправляє тестові пакети за кожною адресою, щоб довідатися час, за який дійде пакет і чи дійде він взагалі (може пристрій відключився). Таким чином, він завжди підтримує актуальний стан карти мережі за допомогою своєї таблиці маршрутизації.

Але отут слід уточнити, що це відноситься до динамічної маршрутизації, яка дуже діюча й зручна. Однак, бувають випадки, коли потрібно жорстко задати адреси всіх пристроїв у мережі, щоб пакети раптом не йшли «не туди», наприклад, зловмисникам. Тоді застосовується статична маршрутизація, яка хоч і забирає багато часу й сил, особливо якщо мережа більша, але це безпечніше.

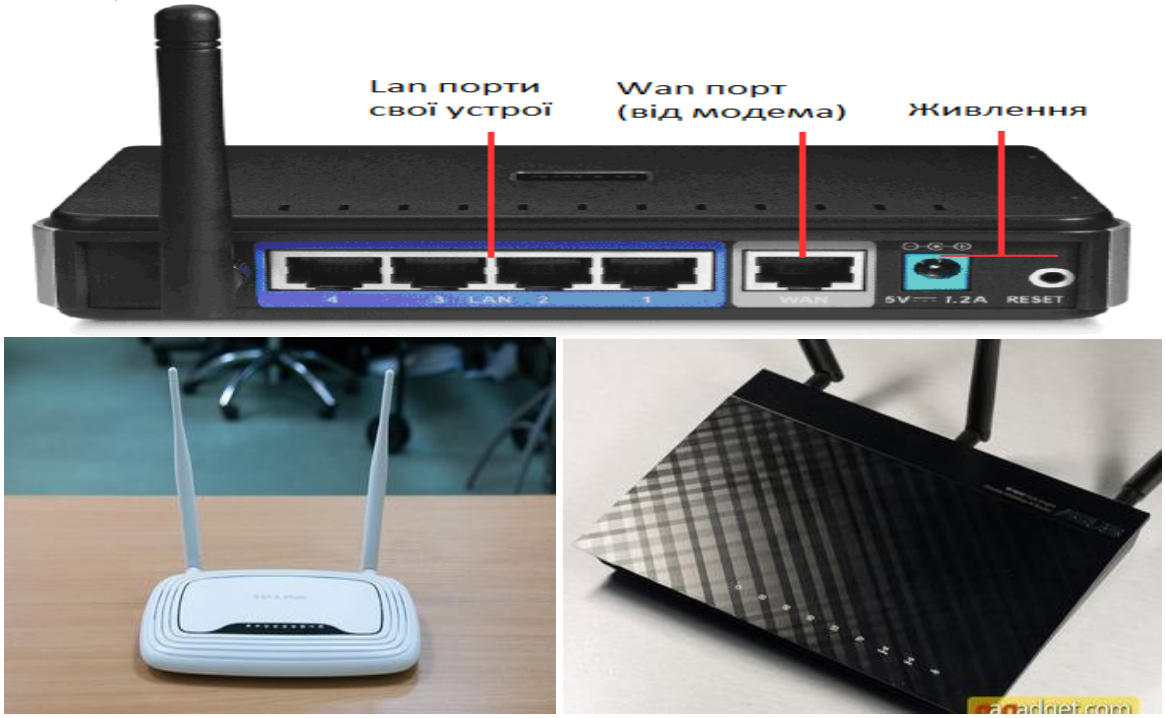


Рис. 2. Роутери

2. Хід роботи

Розглянемо налагодження на прикладі роутера Tp-link TL-WR841N. Але в цьому немає нічого страшного, якщо у вас інший роутер, то думаю, що все буде зрозуміло.

Прагну нагадати, що при налагодженні роутера, потрібно підключати його до комп'ютера за мережевим кабелем. Робити налагодження за Wi-Fi, не раджу!

Хто не знає, як одержати доступ до налагодження роутера, то швидко нагадаю. Потрібно відкрити будь-який браузер і в адресному рядку набрати адресу 192.168.1.1, або 192.168.1.0 потім увести пароль для доступу до налагодження (не плутати з паролем на Wi-Fi мережу). Якщо ви його ще не міняли, то за замовчуванням це admin і admin. Якщо цей не підходить, то знизу роутера звичайно зазначений пароль за замовчуванням.

2.1. Установлення паролю на доступ до налагодження Wi-Fi роутера

Це перше, що потрібно зробити при налагодженні захисту бездротової Wi-Fi мережі. У налаштуванні роутера шукаємо вкладку **System Tools** потім переходимо на вкладку **Password** (рис. 3).

Рис. 3. Вікно налагодження роутера

Уводимо старий логін і пароль, потім у форму нижче вводимо нове ім'я для доступу й два рази новий пароль. Придумайте гарний і складний пароль.Що полягає з букв і цифр. І головне, самі запам'ятаєте його. Для збереження натискаємо **Save.**

2.2. Установлення паролю на Wi-Fi мережу й установлення типу шифрування

В обов'язковому порядку, потрібно вказати тип шифрування, який ви будете використовувати для мережі, і встановити надійний пароль. Переходимо на вкладку **Wireless**, і **Wireless Security** (рис. 4). Біля протоколу WPA/WPA2 – Personal встановлюємо галочку, виставляємо налагодження у рядку, напроти **PSK Password** придумуємо надійний пароль. Цей пароль буде використовуватися для підключення до Wi-Fi. Для збереження натискаємо **Save.**

Роутер запропонує перезавантажити його, але якщо ви ще будете вносити налагодження, то можна поки не перезавантажувати. Але нові налагодження будуть працювати тільки після перезавантаження.

2.3. Приховування імені мережі (SSID)

Ще один відмінний спосіб захисту (рис. 5). Приховуємо назву Wi-Fi мережі, і до неї можна буде підключиться, тільки якщо знати як вона називається. Ваша мережа не буде відображатися в списку доступних мереж.

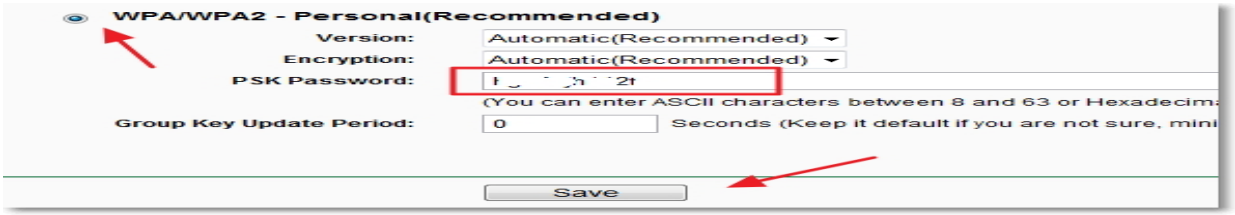


Рис. 4. Вкладка Wireless Security

Шукаємо й переходимо на вкладку **Wireless**. І для того, що б сховати SSID, просто знімаємо галочку з пункту **Enable SSID Broadcast**. Натискаємо кнопку **Save** для збереження змін.

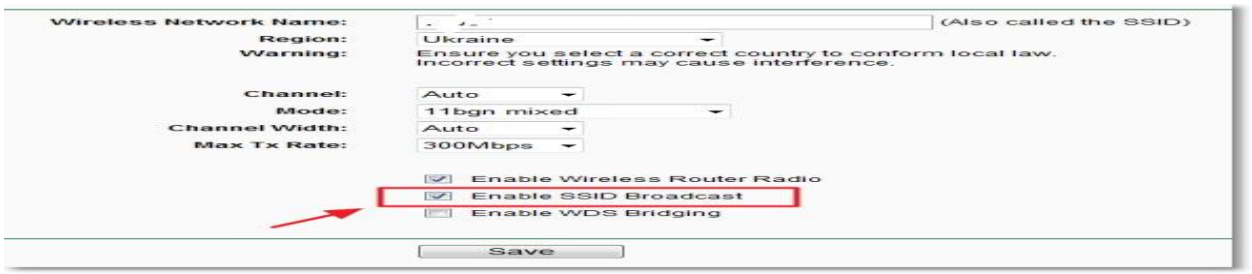


Рис. 5. Вкладка Wireless

2.4. Включення фільтрації пристроїв за MAC адресами

Включення цієї функції, дозволить підключати до роутеру тільки ті пристрої, MAC-адреси яких прописані в налаштуванні і дозволені. Це дуже ефективний захист, але якщо ви часто підключаєте нові пристрої, то буде не дуже зручно щораз заходити в налагодження роутера й прописувати MAC-адреси пристроїв.

Для початку потрібно довідатися MAC- адреси пристроїв, яким ви прагнете дозволити підключення до Wi-Fi мережі. Їх можна подивитися в налаштуванні. Якщо це телефон, або планшет, то можна подивитися адреса в налаштуванні, у розділі **Про телефон.** А якщо пристрій уже підключений до роутеру, то всю необхідну інформацію можна довідатися на вкладці **DHCP – DHCP Clients List.**

Заходимо на вкладку **Wireless**, і переходимо на **Wireless MAC Filtering** (рис. 6). Спочатку включаємо цю службу, нажавши на кнопку **Enable**. Потім установлюємо помітку біля пункту **Allow the stations specified by any enabled entries in the list to access**. Це значить, що до Wi-Fi, зможуть підключатися тільки пристрої, які є в списку.

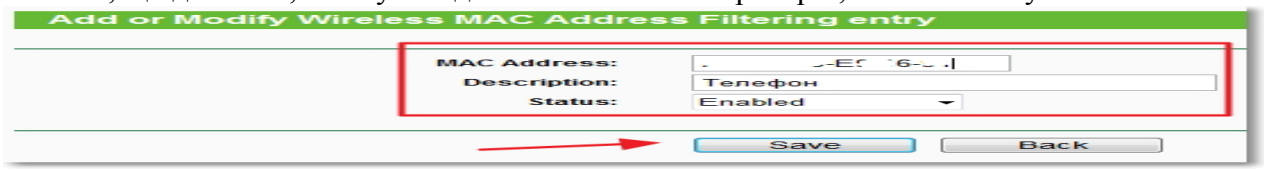


Рис. 6. Вкладка Wireless MAC Filtering

І натискаємо кнопку **Add New…** , для того, що б додати MAC-адреси пристроїв, яким потрібно дозволити доступ. Уводимо MAC-адреси, опис (за бажанням), залишаємо статус **Enable** (дозволити) і натискаємо кнопку **Save.**

2.5. Відключення служби QSS (WPS)

Якщо ви не дуже часто підключаєте нові пристрої і вам не складно ввести пароль від Wi-Fi мережі, то цю службу краще відключити.

Для відключення, переходимо на вкладку **QSS**, у вас вона може називатися ще **WPS**. І натискаємо кнопку **Disabled QSS** (рис. 7).

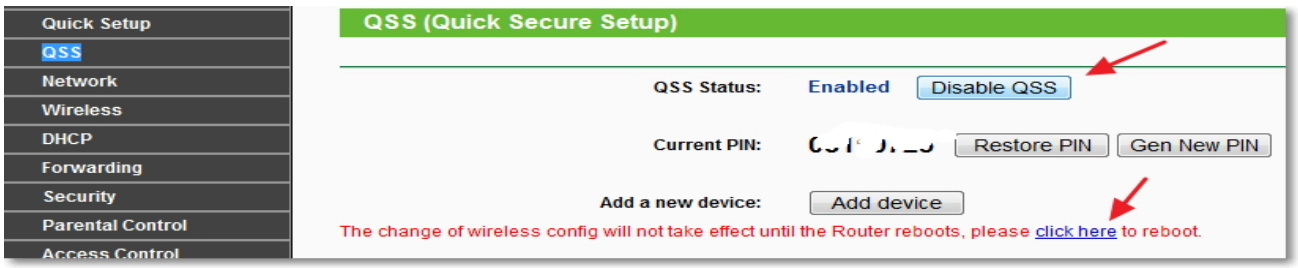


Рис. 7. Вкладка QSS

Залишилося тільки перезавантажити роутер, нажавши на посилання **click here**, або ж нажати цю кнопку на самому роутері.

3. Контрольні питання

1. Як установити пароль на доступ до налагодження роутера?
2. Який тип шифрування включити для Wi-Fi і як установити пароль на мережу?
3. Як сховати ім'я мережі (SSID)?
4. Як провести фільтрацію доступу за MAC – адресами?
5. Як відключити служби QSS (WPS)?

ЛАБОРАТОРНА РОБОТА 11.
НАЛАГОДЖЕННЯМ МЕРЕЖЕВИХ ПАРАМЕТРІВ ОС CISCO IOS, МАРШРУТИЗАТОРА CISCO 2811

Мета роботи: ознайомитися з налагодженням мережевих параметрів ОС Cisco IOS маршрутизатора Cisco 2811 з робочої станції адміністратора мережі**.**

Зміст

1. Теорія
2. Хід роботи
2.1. Налагодження мережевих параметрів ОС Cisco IOS маршрутизатора Cisco 2811 з робочої станції адміністратора мережі.
3. Контрольні питання

1. Теорія

Cisco IOS – це спеціалізована ОС, що забезпечує функціонування мережевого встаткування компанії «Cisco Systems, Inc». Взаємодія з даною ОС можлива або через Web-браузер, або через інтерфейс командного рядка (Cli-Інтерфейс). Дана ОС підтримує дистанційний доступ до інтерфейсу командний рядка за протоколами Telnet або SSH. В Cisco IOS існує кілька режимів.

Користувацький режим (user mode) – стандартний режим першого доступу до ОС. У цей же режим ОС переходить автоматично при тривалій відсутності введення в режимі адміністратора. У режимі користувача доступні тільки прості команди встаткування, що не впливають на конфігурацію. Запрошення командного рядка має такий вигляд:

router>

Адміністративний режим (privileged mode). Відкривається командою *enable*, уведеної в режимі користувача:

router> **enable**

```
WS-C3750G-12S-E>enable
Password:
WS-C3750G-12S-E#
```

В адміністративному режимі доступні команди, що дозволяють одержати повну інформацію про конфігурацію встаткування і його стан, а також команди переходу в режим конфігурування, команди збереження й завантаження конфігурації. Запрошення командного рядка має такий вигляд:

router#

Зворотний перехід у користувацький режим проводиться за командою **disable** або після закінчення встановленого часу не активності. Завершення сесії – команда **exit.**

Глобальний режим конфігурування (конфігураційний режим). Активізується командою **config terminal**, уведеної в адміністративному режимі:

router# configure terminal

Глобальний режим конфігурування організований ієрархічно – він містить як безпосередньо команди конфігурування устаткування, так і команди переходу в режими конфігурування його підсистем (наприклад, інтерфейсів, протоколів маршрутизації, механізмів захисту). Запрошення командного рядка в найбільше часто використовуваних конфігураційних режимах мають такий вигляд:

router(config)#

```
WS-C3750G-12S-E#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
WS-C3750G-12S-E(config)#
```

router(config-if)#

```
WS-C3750G-12S-E(config)#interface gigabitEthernet 1/0/1
WS-C3750G-12S-E(config-if)#
```

rounter(config-router)#

```
WS-C3750G-12S-E(config)#router bgp 1
WS-C3750G-12S-E(config-router)#
```

router(config-ext-nacl)#

```
WS-C3750G-12S-E(config)#ip access-list extended 100
WS-C3750G-12S-E(config-ext-nacl)#
```

switch(config-line)#

```
WS-C3750G-12S-E(config)#line console 0
WS-C3750G-12S-E(config-line)#
```

switch(vlan)#

```
WS-C3750G-12S-E(config)#vlan 1
WS-C3750G-12S-E(config-vlan)#
```

Вихід з будь-якого режиму конфігурування в режим верхнього рівня проводиться командою **exit** або комбінацією клавіш ***Ctrl-Z***. Крім того, команда **end**, подана в кожному з режимів конфігурування негайно завершує процес *конфігурування й повертає користувача в адміністративний режим.*

```
WS-C3750G-12S-E(config)#exit
WS-C3750G-12S-E#
```

Будь-яка команда зміни конфігурації вступає в дію негайно після введення. Усі команди й параметри можуть бути скорочені (наприклад, "*enable*" – "*en*", "*configure terminal*" – "*conf t*", "*show running-config*" – "*sh run*").

В будь-якому місті командного рядка для отримання допомоги може бути використаний знак питання, наприклад:

router#?

```
WS-C3750G-12S-E#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  beep             Blocks Extensible Exchange Protocol commands
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS agents
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  crypto           Encryption related commands.
  cts              Cisco Trusted Security Exec Commands
  debug            Debugging functions (see also 'undebug')
```

router#co?

```
WS-C3750G-12S-E#co?
configure  connect  copy
```

router#conf ?

```
WS-C3750G-12S-E#conf?
configure
```

Імена мережевих інтерфейсів також можуть бути скорочені, наприклад, замість "*fast ethernet*0/1" досить написати "*fa*0/1". Скасування будь-якої команди (відключення опції або режиму, включення, зняття або видалення параметрів, призначених командою) проводиться подачею цієї ж команди із префіксом "*no*", наприклад:

router(config)#int fa0/1
router(config-if)#shutdown
router(config-if)#no shutdown

При завантаженні мережевого встаткування, що працює під управлінням Cisco IOS, відбувається зчитування команд конфігурації із змінюваного постійного запам'ятовуючого пристрою (NVRAM), де вони зберігаються у вигляді текстового файлу, що називається *робочою конфігурацією* (running config). Конфігурація, збережена в NVRAM, називається *початковою конфігурацією* (startup config). В процесі роботи встаткування адміністратор може вводити додаткові конфігураційні команди, у результаті чого робоча конфігурація стає відмінною від початкової.

Розглянемо базові команди одержання інформації про роботу устаткування і його підсистем. Перегляд інформації про встаткування (модель, обсяги пам’яті, версія IOS, число й тип інтерфейсів) виконується за командою:

router#show version

```
WS-C3750G-12S-E#show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(53)SE, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Sun 13-Dec-09 16:25 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(44)SE5, RELEASE SOFTWARE (fc1)

WS-C3750G-12S-E uptime is 21 minutes
System returned to ROM by power-on
System restarted at 16:50:29 EEST Sat Dec 2 2017
System image file is "flash:c3750-ipservicesk9-mz.122-53.SE.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C3750G-12S (PowerPC405) processor (revision K0) with 131072K bytes of memory.
Processor board ID CAT0828R0PB
Last reset from power-on
2 Virtual Ethernet interfaces
12 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:14:1C:AE:23:00
Motherboard assembly number     : 73-9678-04
Power supply part number        : 341-0048-03
Motherboard serial number       : CAT09190LR3
Power supply serial number      : LIT091106VZ
Model revision number           : K0
Motherboard revision number     : A0
Model number                    : WS-C3750G-12S-E
System serial number            : CAT0828R0PB
Top Assembly Part Number        : 800-25856-01
Top Assembly Revision Number    : A0
Version ID                      : V03
CLEI Code Number                : CNM8ZV0GRA
Hardware Board Revision Number  : 0x00


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 12    WS-C3750G-12S      12.2(53)SE            C3750-IPSERVICESK9-M
```

Перегляд умісту флеш-пам'яті:

router#show flash:

```
WS-C3750G-12S-E#show flash:

Directory of flash:/

    2  -rwx    12673801   Jul 6 2011 23:17:29 +03:00  c3750-ipservicesk9-mz.122-53.SE.bin
    3  -rwx         624   Mar 1 1993 02:00:37 +02:00  vlan.dat
    9  drwx          64   Mar 1 1993 02:00:03 +02:00  lost+found
    6  -rwx        5462  May 20 1993 10:36:09 +03:00  backup.conf
    7  -rwx        2047   Mar 1 1993 02:00:55 +02:00  config.text
    8  -rwx        4120   Mar 1 1993 02:00:55 +02:00  multiple-fs
   10  -rwx        3843   Mar 1 1993 02:00:55 +02:00  private-config.text

15998976 bytes total (3300864 bytes free)
WS-C3750G-12S-E#
```

Моніторинг активних процесів:

router#show processes

```
WS-C3750G-12S-E#show processes
CPU utilization for five seconds: 5%/0%; one minute: 5%; five minutes: 5%
 PID QTy       PC Runtime(ms)   Invoked   uSecs    Stacks   TTY Process
   1 Cwe   2A415B0           0        18       0  5464/6000     0 Chunk Manager
   2 Csp   1B8243C           8       292      27  2592/3000     0 Load Meter
   3 Msi   245EDAC          0        97       0  5628/6000     0 MDFS LC Download
   4 Lst   2A4FEB0        1652       177    9333  5744/6000     0 Check heaps
   5 Cwe   2A57F58           0         1       0  5736/6000     0 Pool Manager
   6 Mst   1F3F7F4           0         2       0  5556/6000     0 Timers
   7 Mwe   2A5F10C           0         1       0  5760/6000     0 HRPC asic-stats
   8 Mwe   1381AC8           0         1       0 23668/24000    0 Crash writer
   9 Mwe   1D05E4C         243      1043     232  3408/6000     0 ARP Input
  10 Lwe   1E4E6B0           0         1       0  5760/6000     0 CEF MIB API
  11 Lwe   1F1D410           0         1       0  5764/6000     0 AAA_SERVER_DEADT
  12 Mwe   1F162F0           0         2       0  5548/6000     0 AAA high-capacit
  13 Mwe   1FFBAD8           0         1       0 11732/12000    0 Policy Manager
  14 Lwe   20625FC           8         4    2000  5372/6000     0 Entity MIB API
  15 Mwe   20E7640          16        31     516  7708/9000     0 EEM ED Syslog
  16 Mwe   2270D64           0         1       0  5740/6000     0 IFS Agent Manage
  17 Mwe   22B29DC           0        25       0  5772/6000     0 IPC Dynamic Cach
  18 Mwe   22B2FA4           0         1       0  5784/6000     0 IPC Zone Manager
```

Розглянемо основні команди первісної конфігурації маршрутизатора.

Установити ім'я маршрутизатора:

router(config)#hostname *my_router*

```
WS-C3750G-12S-E(config)#hostname my_router
my_router(config)#
```

Установити пароль адміністратора, необхідний при переході і уведенні команди ***enable***:

router(config)#enable secret *my_secret*

```
WS-C3750G-12S-E(config)#enable secret my_secret
WS-C3750G-12S-E(config)#
```

Відключення дозволу Dns-Імен:

router(config)#no ip domain-lookup

```
WS-C3750G-12S-E(config)#no ip domain-lookup
WS-C3750G-12S-E(config)#
```

Базове налагодження Fastethernet-Інтерфейсу:

router#configure terminal
router(config)#interface fastethernet 0/1
router(config-if)#switchport mode access
router(config-if)#switchport access vlan 1
router(config-if)# spanning-tree portfast
router(config-if)#no shutdown

router(config-if)#exit

Налаштування доступу до комутатора

router#configure terminal

router(config)# interface vlan 1

router(config-if)# ip address 192.168.0.10 255.255.255.0

Для послідовного інтерфейсу пристрою, що виконує роль DCE, необхідно вказувати тактову частоту (пропускну здатність), при цьому дана команда виконується тільки на одній стороні лінії зв'язку:

router(config)#interface serial0

router(config-if)#clock rate 125000

Якщо на послідовному інтерфейсі необхідно використовувати інший протокол 2-го рівня (наприклад, Frame Relay), те це робиться за допомогою команди:

router(config-if)#encapsulation frame-relay

Параметри інтерфейсів, протоколів 2-го рівня, а також статистика відправлених і отриманих кадрів може бути переглянута наступною командою в режимі адміністратора:

router#show interface

Докладна інформація про параметри протоколу IP доступна в режимі адміністратора за командою:

router#show ip interface *interface*

```
WS-C3750G-12S-E#show ip interface vlan 1
Vlan1 is up, line protocol is down
  Internet address is 192.168.0.10/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  Output features: Check hwidb
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
WS-C3750G-12S-E#
```

Коротка зведена таблиця станів Ip-Інтерфейсів:

router#show ip interface brief

```
WS-C3750G-12S-E#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.0.10    YES manual up                    down
[redacted]             [redacted]      YES NVRAM  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
WS-C3750G-12S-E#
```

Розглянемо налаштування статичної маршрутизації. Маршрути, ведучі в мережі, до яких маршрутизатор підключений безпосередньо, автоматично додаються в маршрутну таблицю після конфігурування інтерфейсу за умови, що інтерфейс коректно функціонує.

Для призначення додаткових статичних маршрутів у режимі глобальної конфігурації вводиться команда:

router(config)#ip route *prefix mask gateway*

Маршрут за замовчуванням (стандартний маршрут) призначається наступною командою:

router(config)#ip route 0.0.0.0 0.0.0.0 *gateway*

```
WS-C3750G-12S-E(config)#ip route 0.0.0.0 0.0.0.0 172.24.9.254
```

Переглянути таблицю маршрутів можна за командою:

router#show ip route

```
WS-C3750G-12S-E#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.24.9.254 to network 0.0.0.0

     172.24.0.0/23 is subnetted, 1 subnets
C       172.24.8.0 is directly connected, Vlan607
S*   0.0.0.0/0 [1/0] via 172.24.9.254
WS-C3750G-12S-E#
```

2. Хід роботи

2.1. Налагодження мережевих параметрів ОС Cisco IOS маршрутизатора Cisco 2811 з робочої станції адміністратора мережі.

Виконати первісне налаштування мережевих параметрів ОС Cisco IOS маршрутизатора Cisco 2811 з робочої станції адміністратора мережі, використовуючи дані таблиці 1:

Послідовність дій.

Крок 1. Підключити до маршрутизатора Cisco 2811 робочу станцію через консольний шнур і інтерфейс RS-232.

Крок 2. Запустити термінальний клієнт і перевірити правильність параметрів його налаштування.

Крок 3. Переглянути список команд користувацького режиму. Виконати команду:

router>show version

Крок 4. Перейти в адміністративний режим, виконавши команду:

router>enable

Крок 5. Переглянути рівень доступу в системі й поточну конфігурацію:

router#show privilege

router#show running-config

Таблиця 1

Параметри налаштування маршрутизатора

Параметр	Значення
IP-адреса інтерфейса Fa0/0	10.194.7.1/24
IP-адреса інтерфейса Fa0/1	192.168.100.26/30
Стандартний шлюз	192.168.100.25
Ім'я маршрутизатора	R7
Домен	net.bank
Пароль доступу enable	xkld7Hn434!2&^
Локальний користувач/пароль	noc/nTefa#51

Крок 6. Переглянути список доступних команд. Визначити й виконати всі можливі інформаційні команди. Наприклад:

router#show flash

router#show version

router#show logging

Крок 7. Виконати налагодження маршрутизатора відповідно до зазначених параметрів, виконавши наступні команди:

configure terminal

hostname R7

interface fastethernet 0/1

ip address 192.168.100.26 255.255.255.252

no shutdown

interface fastethernet 0/0

ip address 10.194.7.1 255.255.255.0

no shutdown

ip domain-name net.bank

ip route 0.0.0.0 0.0.0.0 192.168.100.25

Крок 8. Зберегти конфігурацію маршрутизатора, виконавши команду:

write memory

Крок 9. Виключити живлення маршрутизатора. Установити модуль NM-ESW161. Включити живлення маршрутизатора. Перевірити можливість завантаження маршрутизатора з нової конфігурації.

Крок 10. Переглянути список усіх портів і їх імен:

sh ip interface brief

Крок 11. Виконати наступні команди й переглянути їхнім результати:

sh processes

sh file systems

Крок 12. Виключити режим шифрування паролів у файлі конфігурації, створити користувача й переконатися, що пароль в конфігураційному файлі записаний у відкритому вигляді, потім включити режим шифрування паролів і переконатися, що тепер пароль переставляється в зашифрованому вигляді:

no service password-encryption

username noc1 secret test

username noc2 password test

enable secret test2

show running-config

service password-encryption

show running-config

Крок 13. Вилучити всіх створених раніше користувачів, задати стійкі до перебору паролі користувачів і паролі для адміністративного доступу. Перевірити, що для підключення до маршрутизатору й переходу в адміністративний режим потрібен пароль:

line console 0
password n&bbr4d21
login
no username noc1
no username noc2
enable secret xkld7Hn434!2&
username noc secret ntefa#51

Крок 14. Виконати налагодження механізму рольового керування доступом до команд маршрутизатора, що реалізує наступну політику безпеки. Існують наступні ролі й відповідні їм рівні безпеки: адміністратор (15), інженер (5) і оператор (3). Доступ користувачам, авторизованим на роль інженера, може бути наданий тільки через консольну сесію. При цьому можуть бути виконані основні команди з діагностики й налагодженню засобів маршрутизації, комутації й адресації.

Користувачі, авторизовані на роль оператора, можуть тільки переглядати діагностичні дані на маршрутизаторі. Роль адміністратора має всі привілеї:

username admin privilege 15 secret ntefa#51
enable secret 15 secret Rc@sxa&h
username engineer privilege 5 secret Lwqndhr5
enable secret 5 secret Jnfbn&gd
username operator privilege 3 secret *mmfjj&D
enable secret 3 secret Mf88Mmh1
privilege exec level 3 show running-config
privilege exec level 3 show startup-config
privilege exec level 3 show
privilege exec level 3 ping
privilege exec level 3 ssh
privilege exec level 3 telnet
privilege exec level 3 exit
privilege exec level 5 configure terminal
privilege exec level 5 configure
privilege configure level 5 ip
privilege configure level 5 no ip
privilege configure level 5 ip route
privilege configure level 5 no ip route
privilege configure level 5 router
privilege configure level 5 no router
privilege configure level 5 interface
line console 0
privilege 3

3. Контрольні питання

1. Як отримати доступ до налаштувань операційної системи?
2. Як налагодити статичну маршрутизацію?
3. Як розробити шаблон конфігураційного файлу маршрутизатора для зручності налагодження, включити в нього основні вивчені команди?
4. Як запропонувати набір облікових записів і прав доступу для експлуатації маршрутизаторів у великій корпоративній мережі.
5. Як вивчити порядок найменування модулів лінійних карт і мережевих інтерфейсів на маршрутизаторах і комутаторах Cisco?

ЛАБОРАТОРНА РОБОТА 12.
ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ КОМУТАТОРІВ ВІД D-LINK

Мета роботи*:* визначення номера моделі комутатора і його фізичних інтерфейсів, типів кабелів, змінення параметрів програми Hyper-Terminal, підключення до консолі комутатора. За допомогою керуючої консолі комутатора визначити й сконфігурувати його Ір-адресу, перевірити мережеві налагодження робочою станцією (її IP-адреси), фізичне й Ір-з'єднання між коммутатором і робочою станцією

Зміст

1. Теорія
2. Хід роботи
2.1. Необхідне встаткування:
2.2. Визначення та надання параметрів
2.3. Підключення до Web-Інтерфейсу комутатора
3. Контрольні питання

1. Теорія

Комутатори – фундаментальна частина більшості сучасних мереж. Використовуючи мікросегментацію, вони дають можливість одночасно посилати за мережею інформацію безлічі користувачів. Мікросегментація дозволяє створити приватні або виділені сегменти – по одній робочої станції на сегмент (до порту комутатора підключається не сегмент, а тільки робоча станція). Кожна робоча станція при цьому одержує доступ відразу до всієї смуги пропускання, і їй не доводиться конкурувати з іншими станціями. Якщо встаткування працює в дуплексному режимі, то виключаються колізії.

Існує безліч різних типів комутаторів і мереж. Комутатори, які забезпечують виділене з'єднання для кожного вузла внутрішньої мережі компанії, називаються комутаторами локальних мереж (LAN Switches). Більшість перших локальних мереж використовувало концентратори для організації з'єднання між робочими станціями мережі. Використання комутаторів замість концентраторів дозволяє значно підвищити ефективність локальних мереж. У даній лабораторній роботі познайомимося із продукцією компанії D-Link на прикладі комутатора **DES-3226S. DES-3226S** – керований комутатор, що надає при об'єднанні в стек можливість підключення до 192 користувачів за допомогою 10/100 Мбіт/с каналів зв'язку й 8 серверів через порти Gigabit Ethernet.

2. Хід роботи

2.1. Необхідне встаткування:

Робоча станція. Комутатор DES-3226S.

2.2. Визначення та надання параметрів

Крок 1. Дослідити передню й задню панель комутатора.

Відповідайте на наступні питання (занотувати в зошит):

1. Номер моделі комутатора.
2. Має комутатор консольний порт?
3. Чи є вимикач живлення на комутаторі?
4. Яка загальна кількість портів на передній панелі комутатора?
5. Яка кількість портів 10/100 Мбіт/с?
6. Яка кількість портів 1000 Мбіт/с?
7. Які типи конекторів використовуються (перелічити для усіх портів)?
8. Які індикатори перебувають на передній панелі комутатора?

Крок 2. Налагодити параметри програми Hyperterminal. В операційній системі Windows виберіть **Пуск/Программы/Стандартные/Связь/Hyperterminal**. Уведіть назву зв'язку. Виберіть COM-порт, підключений до комутатору. Установіть параметри порту й запишіть їх в табл. 1.

Таблиця 1

Конфігуруємі опції	Установки
COM порт	
Біт у секунду	
Біти даних Керування потоком	
Парність	
Стопові біти	
Керування потоком	

Крок 3. Підключіться до консолі комутатора за допомогою робочої станції із установленою програмою Hyperterminal.

Крок 4. Подивіться налагодження комутатора за допомогою команди **show switch** і заповніть наступну табл. 2.

Таблиця 2

Установки	Значення
Device Type	
MAC-address	
Ip-address	
Subnet Mask	
Default Gateway	
VLAN name	

Крок 5. Створіть облікові записи для членів вашої бригади з різними рівнями привілеїв.

DES-3226S# create account admin/user <*username*>

Крок 6. Установіть комутатору новий Ip-Адресу. Ip-Адреса комутатора повинна бути з того ж діапазону адрес, що і Ip-Адреса робочої станції.

DES-3226S# config ipif System ipaddress
xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy,
де xxx.xxx.xxx.xxx – Ip-Адреса,
yyy.yyy.yyy.yyy. - маска підмережі.

Крок 7. Задайте інтерфейсу 5 швидкість рівну 10 Мбіт/с і дуплексний режим роботи.

DES-3226S# config ports 5 speed 10_full

Крок 8. Подивіться створені облікові записи.

DES-3226S#show account

Крок 9. Перевірте конфігурацію IP.

DES-3226S#show ipif

Крок 10. Перевірте конфігурацію портів.

DES-3226S#show ports

Крок 11. Подивіться поточну конфігурацію комутатора.

DES-3226S#show switch

2.3. Підключення до Web-Інтерфейсу комутатора

Крок 1. Підключіться до консолі комутатора за допомогою робочої станції із установленою програмою Hyperterminal.

Крок 2. За допомогою команди **show switch** визначите Ip-Адресу комутатора.

Крок 3. Якщо необхідно, установіть комутатору нову IP-адресу. Ip-Адреса комутатора повинен бути з того ж діапазону адрес, що й Ip-Адреса робочої станції.

DES-3226S# config ipif System ipaddress
xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy,
де xxx.xxx.xxx.xxx – Ip-Адреса,
yyy.yyy.yyy.yyy. - маска підмережі.

Крок 4. З'єднайте комутатор і робочу станцію кабелем Ethernet.

Крок 5. Перевірте мережеві налагодження робочої станції і якщо треба, змініть її Ip-Адресу.

Крок 6. Протестуйте з'єднання між робочою станцією й комутатором. У командному рядку Windows наберіть

C:/Windows> ping xxx.xxx.xxx.xxx,

де xxx.xxx.xxx.xxx – Ip-Адреса комутатора.

Крок 7. Перевірте мережу командою Ping.

Підключіться до комутатора за допомогою протоколу Telnet. В командному рядку Windows наберіть

C:/Windows> Telnet xxx.xxx.xxx.xxx,

де xxx.xxx.xxx.xxx – Ip-Адреса комутатора.

Крок 8. Використовуючи браузер, підключіться до комутатора.

Крок 9. Двічі клацніть на банері Login для одержання доступу до налаштувань комутатора.

Крок 10. Подивіться конфігурацію комутатора, використовуючи Web-Інтерфейс.

3. Контрольні питання

1. Що дозволяє мікросегментація мереж?
2. Скільки користувачів одночасно можна підключити до комутатора DES-3226S?
3. Скільки серверів одночасно можна підключити до комутатора DES-3226S?
4. Які параметри COM-портів в комутаторі DES-3226S?
5. Яке призначення програми Hyperterminal?
6. Як створити облікові записи в комутаторі DES-3226S?
7. Як задати інтерфейсу швидкість передачі даних та режим роботи?
8. Як продивитися поточну конфігурацію комутатора?
9. Як визначити Ip-Адресу комутатора.
10. Як протестувати з'єднання між робочою станцією й комутатором?
11. Як отримати доступ до налаштувань комутатора?

ЛАБОРАТОРНА РОБОТА 13. ВИВЧЕННЯ СТРУКТУРИ IP-АДРЕС

Мета роботи: вивчення принципів адресації в мережах TCP/IP і придбання практичних навичок застосування й призначення Ip-адрес із використанням масок.

Зміст

1. Теорія
1.1 Типи адрес стека TCP/IP
1.2 Класи Ip-адрес
1.3 Особливі Ip-адреси
1.4 Використання масок в Ip-адресації
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Типи адрес стека TCP/IP

У стеці TCP/IP використовуються три типи адрес: локальні (які називаються також апаратними), Ip-адреси й символьні доменні імена.

У термінології TCP/IP під локальною адресою розуміється такий тип адреси, яка використовується засобами базової технології для доставки даних у межах підмережі, що є елементом інтермережі. У різних підмережах припустимі різні мережеві технології, різні стеки протоколів, тому при створенні стека TCP/IP передбачалася наявність різних типів локальних адрес. Якщо підмережею інтермережі є локальна мережа, то локальна адреса – це Mac-адреса. Однак протокол IP може працювати й над протоколами більш високого рівня, наприклад, над протоколом IPX або X.25. У цьому випадку локальними адресами для протоколу IP відповідно будуть адреси IPX і X.25. Комп'ютер у локальній мережі може мати кілька локальних адрес навіть при одному мережевому адаптері. Деякі мережеві пристрої не мають локальних адрес. Наприклад, до таких пристроїв відносяться глобальні порти маршрутизаторів, призначені для з'єднань типу « крапка-крапка».

Ip-адреси являють собою основний тип адрес, на підставі яких мережевий рівень передає пакети між мережами. Ці адреси складаються з 4 байт, наприклад, 109.26.17.100. Ip-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. Ip-адреса складається із двох частин: номера мережі й номера вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Internet Network Information Center, Internic), якщо мережа повинна працювати як складова частина Internet. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор за визначенням входить відразу в кілька мереж. Тому кожний порт маршрутизатора має власну Ip-адресу. Кінцевий вузол також може входити в декілька мереж. У цьому випадку комп'ютер повинен мати Ip-адресу, за числом мережевих зв'язків. Таким чином, Ip-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

Символьні доменні імена. Символьні імена в Ip-Мережах називаються доменними й будуються за ієрархічною ознакою. Між доменним іменем і Ip-Адресою вузла немає ніякої алгоритмічної відповідності, тому необхідно використовувати якісь додаткові таблиці або служби, щоб вузол мережі однозначно визначався як за доменним ім’ям, так і по Ip-адресі. У мережах TCP/IP використовується спеціальна розподілена служба Domain Name System (DNS), яка встановлює цю відповідність на підставі створюваних адміністраторами мережі таблиць відповідності. Тому доменні імена називають також DNS-Іменами.

1.2. Класи Ip-адрес

Ip-адреса має довжину 4 байта й звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі й розділених крапками, наприклад:

128.10.2.30 – традиційна десяткова форма представлення адреси;

10000000 00001010 00000010 00011110 – двійкова форма представлення цієї ж адреси.

Адреса складається із двох логічних частин – номера мережі й номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка – до номера вузла, визначається значеннями перших біт адреси. Значення цих біт є також ознаками того, до якого класу відноситься та або інша Ip-Адреса.

Якщо адреса починається з 0, то мережу відносять до класу А і номер мережі займає один байт, інші 3 байта інтерпретуються як номер вузла в мережі. Мережі класу А мають номера в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче.)

Кількість вузлів у мережах класу А може досягати 2, тобто 16 777 216 вузлів.

Клас А.	Occccccc yyyyyyyy yyyyyyyy	yyyyyyyy
Клас В.	10cccccc cccccccc yyyyyyyy	yyyyyyyy
Клас С.	110ccccc cccccccc cccccccc	yyyyyyyy
Клас D.	1110aaaa aaaaaaaa aaaaaaaa	aaaaaaaa
Клас Е.	11110zzz zzzzzzzz zzzzzzzz	zzzzzzzz

(с - біт, що входить у номер мережі; у - біт, що входить у номер вузла; а - біт, що входить на адресу групи multicast; з - біт, що входить у зарезервовану адресу)

Якщо перші два біти адреси рівні 10, то мережа відноситься до класу В. У мережах класу В під номер мережі й під номер вузла приділяється по 16 біт. Таким чином, мережа класу В є мережею середніх розмірів з максимальним числом вузлів 216, що становить 65 536 вузлів.

Якщо адреса починається з послідовності 110, то це мережа класу С. У цьому випадку під номер мережі приділяється 24 бита, а під номер вузла - 8 біт. Мережі цього класу найпоширеніші, число вузлів у них обмежено 2, тобто 256 вузлами.

Якщо адреса починається з послідовності 1110, то віна є адресою мережі класу D і позначає особливу, групову адресу - multicast. Якщо в пакеті в якості адреси призначення зазначена адреса класу D, то такий пакет повинні одержати всі вузли, яким привласнена дана адреса.

Якщо адреса починається з послідовності 11110, то це значить, що дана адреса відноситься до класу Е. Адреси цього класу зарезервовані для майбутніх застосувань.

1.3. Особливі Ip-адреси

У протоколі IP існує кілька угод про особливої інтерпретації Ip-адрес:

- Якщо вся Ip-адреса складається тільки із двійкових нулів, то вона позначає адресу того вузла, який згенерував цей пакет; цей режим використовується тільки в деяких повідомленнях ICMP.
- Якщо в поле номера мережі знаходяться тільки нулі, то за замовчуванням уважається, що вузол призначення належить тієї ж самій мережі, що й вузол, який відправив пакет.
- Якщо всі двійкові розряди Ip-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що перебувають у тій же мережі, що й джерело цього пакета. Таке розсилання називається обмеженим широкомовним повідомленням (limited broadcast).
- Якщо в поле номера вузла призначення знаходяться тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21.0. Таке розсилання називається широкомовним повідомленням (broadcast).

При адресації необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких Ip-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси випливає, що максимальна кількість вузлів, наведена для мереж кожного класу, на практиці повинна бути

зменшена на 2. Наприклад, у мережах класу С під номер вузла приділяється 8 біт, які дозволяють задавати 256 номерів: від 0 до 255. Однак на практиці максимальне число вузлів у мережі класу С не може перевищувати 254, тому що адреси 0 і 255 мають спеціальне призначення. Із цих же міркувань випливає, що кінцевий вузол не може мати адреса типу 98.255.255.255, оскільки номер вузла в цій адресі класу А складається з одних двійкових одиниць.

Особливий зміст має Ір-адреса, перший октет якого рівний 127. Він використовується для тестування програм і взаємодії процесів у межах однієї машини. Коли програма посилає дані за Ір-адресою 127.0.0.1, то утворюється як би «петля». Дані не передаються за мережею, а вертаються модулям верхнього рівня як тільки що прийняті. Тому в Ір-Мережі забороняється привласнювати машинам Ір-адреси, що починаються з 127. Ця адреса має назва loopback.

У протоколі IP немає поняття широкомовності в тому розумінні, у якім воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно всім вузлам. Як обмежена широкомовна Ір-адреса, так і широкомовна Ір-адреса мають межі поширення в інтермережі – вони обмежені або мережею, до якої належить вузол-джерело пакета, або мережею, номер якої зазначений в адресі призначення.

Уже згадувана форма групової Ір-адреси – multicast – означає, що даний пакет повинен бути доставлений відразу декільком вузлам, які утворюють групу з номером, зазначеним у полі адреси. Вузли самі ідентифікують себе, тобто визначають, до якої із груп вони відносяться. Той самий вузол може входити в кілька груп. Члени якої-небудь групи multicast не обов'язково повинні належати одній мережі. Групова адреса не ділиться на поля номера мережі й вузла й обробляється маршрутизатором особливим чином.

Групова адресація призначена для економічного поширення в Internet або великої корпоративної мережі аудіо – або відео програм, призначених відразу великий аудиторії слухачів або глядачів. Якщо такі засоби знайдуть широке застосування, то Internet зможе створити серйозну конкуренцію радіо й телебаченню.

1.4. Використання масок в Ір-адресації

Важливим елементом розбивання адресного простору Internet є підмережі. Підмережа – це підмножина мережі, що не перетинається з іншими підмережами. Це означає, що мережа організації може бути розбита на фрагменти, кожний з яких буде становити підмережу. Реально кожна підмережа відповідає фізичній локальній мережі (наприклад, сегменту Ethernet). Підмережі використовуються для того, щоб обійти обмеження фізичних мереж на число вузлів у них і максимальну довжину кабелю в сегменті мережі. Наприклад, сегмент тонкого Ethernet має максимальну довжину 185 м і може включати до 32 вузлів. Сама маленька мережа класу С може складатися з 254 вузлів. Для того щоб досягти цього значення, необхідно об'єднати кілька фізичних сегментів мережі. Зробити це можна або за допомогою фізичних пристроїв (наприклад, повторювачів), або за допомогою машин-шлюзів. У першому випадку розбивання на підмережі не потрібна, тому що логічно мережа виглядає як одне ціле. При використанні шлюзу мережа розбивається на підмережі.

Розбивання мережі на підмережі використовує ту частину Ір-адреси, яка закріплена за номерами комп'ютерів. Адміністратор мережі може замаскувати частину Ір-адреси й використовувати її для призначення номерів підмереж. Фактично спосіб розбивання адреси на дві частини, тепер буде застосовуватися до адреси комп'ютера з Ір-адреси мережі, у якій організовано розбивку на підмережі.

Маска підмережі – це чотири байти, які накладаються на Ір-адресу для одержання номера підмережі. Наприклад, маска 255.255.255.0 дозволяє розбити мережу класу В на 254 підмережі по 254 вузла в кожній. Підмережі не тільки вирішують, але й створюють ряд проблем. Наприклад, відбувається втрата адрес, але вже не через фізичні обмеження, а

через принцип побудови адрес підмережі. Так, виділення трьох битів на адресу підмережі приводить до створення не восьми, а тільки шести підмереж, тому що номера 0 і 7 не можна використовувати в силу спеціального значення Ір-адрес, що складаються із нулів або з одиниць.

Для стандартних класів мереж маски мають наступні значення:

клас А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

клас В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

клас ІЗ - 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

Постачаючи кожну Ір-адресу маскою, можна відмовитися від понять класів адрес і зробити систему адресації більш гнучкою. Наприклад, адреса 185.23.44.206 попадає в діапазон 128-191, тобто адреса відноситься до класу В. Отже, номером мережі є перші два байти, доповнені двома нульовими байтами - 185.23.0.0, а номером вузла - 0.0.44.206. Якщо ця адреса асоціювати з маскою 255.255.255.0, те номером підмережі буде 185.23.44.0, а не 185.23.0.0, як це визначене системою класів.

У масках кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинна бути кратною 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для Ір-адреси 129.64.134.5 зазначена маска 255.255.128.0, тобто у двійковому вигляді:

Ір-адреса 129.64.134.5 - 10000001.01000000.10000110.00000101 Маска 255.255.128.0 - 11111111.11111111.10000000.00000000 Якщо використовувати для визначення границі номера мережі маску, то 17 послідовних одиниць у масці, «накладені» на Ір-адресу, визначають у якості номера мережі у двійковім вираженні число:

10000001. 01000000. 10000000. 00000000 або в десятковій формі запису -

номер мережі 129.64.128.0, а номер вузла 0.0.6.5.

Нижче наведені відповідності масок кількості підмереж і максимальному числу вузлів у підмережі для різних класів.

Клас А

Перша група цифр – клас Ір-адреси

Розподіл 1 і 0 в 3 групах, що залишилися, говорить про:

- Кількості підмереж ($N_{пс}=2^{n-2}$) (n - до-в 1) і
- максимальнім числі вузлів у підмережі ($N_{maxy}=2^{m-2}$)(m - до-в 0)

{ n+m=24}

Ір-адреса першого вузла в першої підмережі

- перша група цифр залишається такою ж
- друга група цифр: 0(якщо всі одиниці в масці) або 2^{tw} (якщо не всі одиниці в масці, tw - до-у нулів)
- третя група цифр: 0(якщо всі одиниці в масці) або 2^{th} (якщо не всі одиниці в масці, th - до-у нулів)
- четверта група цифр: 1 (якщо всі нулі) або $2^{f}+1$ (f - до-у нулів, f<8)

Для адреси 10.131.2.155 і маски підмережі 255.192.0.0 визначте

клас Ір-адреси (A,B,C)

число підмереж, яке можна утворювати з використанням даної маски

максимальне число вузлів у підмережі

Ір-адреса першого вузла в першої підмережі

Відповіді записуються в один рядок через пробіл{ 192=128+64=11000000 22-2=4-2 222-2=4194304-2

A 2 4194302 10.64.0.1#

Для адреси 105.52.132.19 і маски підмережі 255.240.0.0

240=128+64+32+16=11110000

24=16-2 220-2=1048576-2 24 0 1

A 14 1048574 105.16.0.1#

}

Для адреси 107.166.146.243 і маски підмережі 255.255.128.0
255.128=11111111.1000000
29-2=512-2 215-2=32768-2 0 27 1

A 510 32766 107.0.128.1#
}
Для адреси 116.151.159.241 і маски підмережі 255.255.248.0
255.248=11111111.11111000
213-2=8192-2 211-2=2048-2 0 23 1
A 8190 2046 116.0.8.1#
}
Для адреси 118.103.150.82 і маски підмережі 255.224.0.0
224=128+64+32=11100000
23-2=8-2 221-2=2097152-2 25 0 1
A 6 2097150 118.32.0.1#
}
Для адреси 118.118.33.130 і маски підмережі 255.255.224.0
255.224=255.128+64+32=11111111.11100000
211-2=2048-2 213-2=8192-2 0 25 1
A 2046 8190 118.0.32.1#
}
Клас В
Перша група цифр – клас Ір-адреси
Друга група цифр – не враховується
Розподіл 1 і 0 в 2 групах, що залишилися, говорить про:
- кількість підмереж ($N_{пс}=2^{n-2}$) (n - до-в 1) і
- максимальнім числі вузлів у підмережі ($N_{maxy}=2^{m-2}$)(m - до-в 0)

{ n+m=16}
Ір-адреса першого вузла в першої підмережі
- перша група цифр залишається такою ж
- друга група цифр залишається такою ж
- третя група цифр: 0(якщо всі одиниці в масці) або 2^{th} (якщо не всі одиниці в масці, th - до-у нулів)
- четверта група цифр: 1 (якщо всі нулі) або $2^{f}+1$ (f - до-у нулів, f<8)

Для адреси 128.144.250.68 і маски підмережі 255.255.255.240
255.240=255.128+64+32+16=11111111.11110000 212=4096-2 24-2=16-2
B 4094 14 128.144.0.17#
}
Для адреси 128.194.33.158 і маски підмережі 255.255.254.0
254.0=254.128+64+32+16=11111110.00000000
27=128-2 29-2=512-2 21 1
B 126 510 128.194.2.1#
}
Для адреси 129.153.160.170 і маски підмережі 255.255.255.240
255.240=255.128+64+32+16=11111111.11110000
212=4096-2 24-2=16-2 0 1 24+1
B 4094 14 129.153.0.17#
}
Для адреси 129.35.84.248 і маски підмережі 255.255.192.0
192.0=128+64=11000000.00000000
22=4-2 214-2=16384-2 26 1
B 2 16382 129.35.64.1#

}
Для адреси 129.64.116.185 і маски підмережі 255.255.224.0
224.0=128+64+32.0=11100000.00000000
23=8-2 213-2=8192-2 25 1
B 6 8190 129.64.32.1#
}
Для адреси 130.194.135.140 і маски підмережі 255.255.255.224
255.224=255.128+64+32=11111111.11100000
211=2048-2 25-2=32-2 0 25+1
B 2046 30 130.194.0.33#
}
Клас С
Перша група цифр – клас Ір-адреси
Друга група цифр – не враховується
Розподіл 1 і 0 в 2 групах, що залишилися, говорить про:
- кількість підмереж ($N_{пс}=2^{n-2}$) (n - до-в 1) і
- максимальнім числі вузлів у підмережі ($N_{maxy}=2^{m-2}$)(m - до-в 0)

{ n+m=8}
Ір-адреса першого вузла в першої підмережі
- перша група цифр залишається такою ж
- друга група цифр залишається такою ж
- третя група цифр залишається такою ж
- четверта група цифр: 1 (якщо всі нулі) або $2^{f}+1$ (f - до-у нулів, f<8)

Для адреси 192.237.133.204 і маски підмережі 255.255.255.248
248=128+64+32+16+8=11111000
25-2=32-2 23-2=8-2 23+1
C 30 6 192.237.133.9#
}
Для адреси 193.236.141.56 і маски підмережі 255.255.255.240
240=128+64+32+16=11110000
24-2=16-2 24-2=16-2 24+1
C 14 14 193.236.141.17#
}
Для адреси 194.114.114.252 і маски підмережі 255.255.255.224
224=128+64+32=11100000
23-2=8-2 25-2=32-2 25+1
C 6 30 194.114.114.33#
}
Для адреси 194.171.50.80 і маски підмережі 255.255.255.192
192=128+64=11000000
22-2=4-2 26-2=64-2 26+1
C 2 62 194.171.50.65#
}
Для адреси 195.41.117.22 і маски підмережі 255.255.255.248
248=128+64+32+16+8=11111000
25-2=32-2 23-2=8-2 23+1

C 30 6 195.41.117.9#
}
Для адреси 195.71.162.218 і маски підмережі 255.255.255.248
248=128+64+32+16+8=11111000
25-2=32-2 23-2=8-2 23+1

C 30 6 195.71.162.9#

}

Для адреси 195.90.131.223 і маски підмережі 255.255.255.248

248=128+64+32+16+8=11111000

25-2=32-2 23-2=8-2 23+1

C 30 6 195.90.131.9#

2. Хід роботи

2.1. Завдання на лабораторну роботу

1. Ознайомитися з теоретичним матеріалом.
2. Завдання 1. Для заданих Ір-адрес класів А, В і С і запропонованих масок визначити:
   - клас адреси;
   - максимально можливу кількість підмереж, яке можна утворювати з використанням даної маски;
   - діапазон зміни адрес підмереж;
   - максимальне число вузлів у підмережах.
3. Завдання 2. За заданими класами (А, В або С), кількості підмереж N і максимальній кількості комп'ютерів М1...MN у кожної підмережі визначити маску для розбивання на підмережі. Зробити висновок про можливість такої розбивання. Якщо розбивання неможлива, то сформулювати рекомендації зі зміни яких-небудь вихідних даних для забезпечення можливості розбивання.

Для адреси X.X.X.X і маски підмережі A.A.A.A визначите

- клас Ір-адреси (A,B,C)
- число підмереж, яке можна утворювати з використанням даної маски
- максимальне число вузлів у підмережі
- Ір-адресу першого вузла в першій підмережі

Відповіді записуються в один рядок через пробіл

4. За результатами роботи оформити звіт. Зміст звіту: вихідні дані, розрахунки зазначених параметрів, виводи й рекомендації.

3. Контрольні питання

1. Типи адрес, які використовувані в стеці TCP/IP, їхнє призначення й застосовувані схеми адресації.
2. Класи Ір-адрес.
3. Для яких цілей використовуються домовленості про особливі адреси?
4. Використання масок при призначенні адрес.
5. Вид маски, принцип її використання й методика вибору маски.

ЛАБОРАТОРНА РОБОТА 14. СЛУЖБА ДОМЕННИХ ІМЕН (DNS). УСТАНОВКА Й НАЛАГОДЖЕННЯ DNS-СЕРВЕРА НА БАЗІ WINDOWS 2003 SERVER

Мета роботи: навчитись встановлювати *DNS*-сервер на базі Windows *2003 SERVER*

1. Розібратися з поняттям доменних імен.
2. Розібратися с призначенням і принципом функціонування служби доменних імен (DNS).
3. Вивчити базові поняття протоколу DNS.
4. Навчитися встановлювати найпростіший варіант DNS сервера.

Зміст

1. Теорія
1.1. Доменні імена
1.2. Служба трансляції імен в Internet
1.3. Функції DNS
1.4. Загальні принципи функціонування DNS
2. Установка й налагодження DNS сервера на базі ОС Windows 2003 Server
3. Контрольні питання
4. Завдання на лабораторну роботу

1. Теорія

1.1. Доменні імена

Домен – область ієрархічного простору мережі Інтернет, яка позначається унікальним доменним іменем.

Доменне ім'я – символьне ім'я домену. Повинне бути унікальним у рамках одного домену. Повне ім'я домену складається з імен усіх доменів, у які він входить, розділених крапками. Наприклад, повне ім'я *www.ukr.net* (с крапкою наприкінці) позначає домен третього рівня *www*, який входить у домен другого рівня *ukr*, який входить у домен. *net*, який входить у кореневий домен. Доменне ім'я служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (Web-сайтів, серверів електронної пошти, мережевих сервісів) у зручній для людини формі.

Доменна зона – сукупність доменних імен певного рівня, що входять у конкретний домен. Наприклад, зона *ctam. ukr.net.* означає всі доменні імена третього рівня в цьому домені. Термін «доменна зона» в основному застосовується в технічній сфері, при настроюванні Dns-Серверів (підтримка зони, делегування зони, трансфер зони).

Для забезпечення унікальності й захисту прав власників доменні імена 1-го й 2-го (в окремих випадках і 3-го) рівнів можна використовувати тільки після їхньої реєстрації, яка проводиться уповноваженими на те реєстраторами. Відомості про власника (адміністратора) того або іншого домену можна довідатися, скориставшись службою «whois» – наприклад, http://www.ripn.net:8080/nic/whois

Домени верхнього рівня загального призначення

.aero – для суб'єктів авіатранспортної індустрії
.biz – тільки комерційні організації
.cat – для використання каталонским мовним і культурним співтовариством
.com – комерційні організації (без обмежень)
.coop – кооперативи
.edu – вищі навчальні заклади, що визнаються в якості таких Департаментом США
.info – інформаційні ресурси (без обмежень)
.jobs – кадрові агентства
.mobi – для продавців і постачальників мобільного контенту й послуг, пов'язаних з мобільним зв'язком
.museum – музеї
.name – фізичні особи

.net – організації, що мають відношення до функціонування Internet (без обмежень)
.org – некомерційні організації (без обмежень)
.pro – сертифіковані професіонали й суміжні теми
.travel – для суб'єктів туристичного бізнесу

Домени верхнього рівня, призначувані країнам

Для зручність розподілу й призначення доменних імен для кожної із країн були виділені власні (в основному дві символьні) домени верхнього рівня. Правда, це зовсім не означає обов'язкову прив'язку серверів у даних доменні до їхнього географічного розташування. Приклади доменів першого рівня для країн:

.au – Australia (Австралія)
.be – Belgium (Бельгія)
.ru – Russia (Росія)
.ua – Ukraine (Україна)
.uk – United Kingdom (Англія)

1.2. Служба трансляції імен в Internet

Первісне перетворення між доменними й Ip-адресами проводилося з використанням спеціального текстового файлу ***DHOSTS.TXT***, який складався централізовано й обновлявся на кожній з машин мережі вручну. З ростом мережі виникла необхідність в ефективному, автоматизованому механізмі, яким і стала **DNS** (***Domain Name System***) – система доменних імен.

Примітка. Насправді на кожній мережній машині є текстовий файл hosts (Windows – ***%windir%\system32\drivers\etc\hosts***; *nix – ***/etc/hosts***), у якім можна самостійно зіставляти з деяким Ip-Адресою доменні імена. Правда, ці дії валідні тільки для поточної машини.

1.3. Функції DNS

Існують два принципово різні способи ідентифікації хостів: за допомогою імен і за допомогою Ip-адрес. Ім'я хосту зручно для людей у силу своєї мнемонічності, а Ip-адреса, що є компактної числовою величиною фіксованого розміру, простіше обробляти прикладним програмами й маршрутизаторами. Для того щоб встановити зв'язок між цими двома ідентифікаторами, використовується *система доменних імен*. DNS являє собою, з одного боку, базу даних, розподілену між ієрархічно структурованими *серверами імен*, і, з іншого боку, протокол прикладного рівня, що організує взаємодію між хостами й серверами імен для виконання операцій перетворення.

DNS функціонує на принципі делегування повноважень. Кожна машина або знає відповідь на запитання, або знає кого запитати. При правильнім функціонуванні система замкнена, тобто якщо запитана інформація є в кого-небудь, то вона буде знайдена й повідомлена клієнтові, або, якщо на питання не має відповіді, клієнт одержить повідомлення про неможливість одержання відповіді на запитання.

В основі роботи **DNS** лежить відповідний мережевий протокол також з назвою **DNS.** DNS-Протокол використовує для роботи TCP- або Udp-Порт 53 для відповідей на запити. Традиційно запити й відповіді відправляються у вигляді однієї UDP датаграми. TCP використовується у випадку, якщо відповідь більше 512 байт, або у випадку Axfr-Запиту.

Прикладні мережеві програми й протоколи найчастіше маніпулюють IP адресами. Для можливості обробки символьних імен, необхідно попередньо одержати Ip-адресу вилученого вузла. А для цього необхідно сформувати й надіслати запит до DNS серверу.

Наприклад, браузер перед запитом деякого ресурсу виділяє з URL ім'я хосту (усе, що йде до першого одинарного символу «/»), надсилає запит на перетворення DNS серверу, який у свою чергу у випадку успішного перетворення, повертає пакет із запитаної клієнтом інформацією. Після чого браузер може виконувати необхідні операції за запитом ресурсів із сервера із заданим IP-адресою.

Очевидно, що процес одержання Ip-адреси не є миттєвим і вносить додаткову затримку в сумарний час установлення з'єднання (до речі кажучи, також відбувається деяка витрата мережевого трафіка). Оптимізація за зменшенням часу запиту (і трафіка) до Dns-Серверу вирішується введенням так званих кешуючих Dns-Серверів.

Крім перетворення імені хостів в Ip-адреси, DNS виконує ще кілька важливих функцій:

- Підтримка псевдонімів серверів.
- Підтримка псевдонімом поштових серверів.
- Розподіл завантаження.

Основні специфікації DNS утримуються в документах RFC 1034 і RFC 1035. Крім того, деякі доповнення можна знайти й в інших RFC.

1.4. Загальні принципи функціонування DNS

Сервіс DNS можна було б представити у вигляді спеціального виділеного сервера, що містить інформацію про всі існуючі домени. Але, якщо вдуматися, то на практиці таке реалізувати не те що не можливо, а навіть просто не доцільно й не вигідно. Централізованій системі властиві деякі «уроджені» недоліки:

- Єдина крапка можливої відмови. Вихід з ладу DNS сервера паралізує роботу всього Internet.
- Обсяг трафіка. Сервер імен є «вузьким місцем» з погляду завантаження, оскільки змушений обробляти всі запити із усіх хостів у мережі Internet.
- Далекість централізованої бази. Єдиний сервер неможливо розташувати на прийнятній відстані від усіх клієнтів.
- Обслуговування. База даних повинна не тільки зберігати адреси всіх існуючих хостів, але постійно обновлятися з появою нових хостів.

Для того щоб розв'язати проблему зберігання більших обсягів інформації, система DNS була спроектована у вигляді сукупності численних серверів імен, розосереджених по усьому світу й організованих у вигляді ієрархічної структури. Жоден сервер не містить інформацію про всі Ip-адресах хостів – ця інформація розподілена між безліччю хостів. *DNS – **це яскравий приклад побудови на практиці розподіленої бази даних!***

За функціональністю й призначенню можна виділити наступні DNS сервери: локальні, кореневі й повноважні.

- *Локальні сервери* імен є в кожного Internet-Провайдера (ще їх називають серверами імен за замовчуванням). Коли користувацький хост посилає DNS- запит, цей запит спочатку попадає на локальний сервер імен. Звичайно локальні сервера імен розташовуються досить близько до користувача а також при запиті «популярних» ресурсів беруть інформацію зі свого кешу, що для користувача значно скорочує відгук. Dns-Сервера за замовчуванням звичайно задаються в налаштуваннях мережевого підключення. Вони прописуються у вигляді Ip-адреси.
- *Кореневі сервери* імен є наступним щаблем в ієрархії серверів DNS. Існує 13 кореневих серверів (позначаються латинськими буквами від A до M), розташованих по усьому світу й прив'язаних до свого регіону, вони управляються різними організаціями, що діють за узгодженням з **ICANN** (***ICANNnet Corporation for Assigned Names and Numbers***). Їхні адреси ніколи не міняються, а інформація про них є в будь-якій операційній системі. От список (можна подивитися, наприклад, в %windir%\system32\dns\cache.dns) цих серверів на даний момент:

A.ROOT-SERVERS.NET. 198.41.0.4
B.ROOT-SERVERS.NET. 192.228.79.201
C.ROOT-SERVERS.NET. 192.33.4.12
D.ROOT-SERVERS.NET. 128.8.10.90
E.ROOT-SERVERS.NET. 192.203.230.10
F.ROOT-SERVERS.NET. 192.5.5.241

G.ROOT-SERVERS.NET. *192.112.36.4*
H.ROOT-SERVERS.NET. *128.63.2.53*
I.ROOT-SERVERS.NET. *192.36.148.17*
J.ROOT-SERVERS.NET. *192.58.128.30*
K.ROOT-SERVERS.NET. *193.0.14.129*
L.ROOT-SERVERS.NET. *199.7.83.42*
M.ROOT-SERVERS.NET. *202.12.27.33*

- *Повноважний сервер* – це сервер, на якім зареєстрований даний хост. Звичайно хости реєструються на локальних серверах імен Internet-Провайдерів (на практиці для забезпечення надійності реєстрація проводиться не менш ніж на двох серверах)

Як працює перетворення імен

Запити, які генеруються хостом, є рекурсивними, тобто в якості відповіді на такий запит вертається або шукана інформація, або повідомлення про її відсутність. Запити, генеруємі Dns-Сервером частіше є ітерактивними (нерекурсивними) і, на відміну від рекурсивних, допускають відповідь у вигляді посилання на інший сервер, який краще обізнаний про місце розташування шуканої інформації. *Варто відзначити, що на практиці найближчі до користувача доменні сервера повинні бути налаштовані як рекурсивні.*

Розглянемо Dns-Алгоритм вилученого пошуку Ip-адреси за іменем. Хост посилає на Ip-адресу найближчого (за замовчуванням) Dns-Сервера Dns-Запит, у якім указує ім'я сервера, Ip-адресу якого необхідно знайти.

Dns-Сервер, одержавши таке повідомлення, шукає у своїй базі імен зазначене ім'я. Якщо зазначене в запиті ім'я знайдене, а отже, знайдена і відповідний йому Ip-адреса, то DNS-Сервер відправляє на хост Dns-Відповідь, у якій указує шукану Ip-адреса. Якщо ж Dns-Сервер не виявив такого імені у своїй базі імен, то він пересилає DNS-Запит на один з відповідальних за домени верхнього рівня DNS-Серверів, адреси яких утримуються у файлі налаштувань Dns-Сервера (cache.dns, про який вище вже було згадування), і описана в цьому пункті процедура повторюється, поки ім'я не буде знайдено (або буде не знайдене).

Зворотний Dns-Запит (Reverce DNS)

DNS використовується в першу чергу для перетворення символьних імен в Ip-адреси, але він також може виконувати зворотний процес. Для цього використовуються вже наявні засоби DNS. Справа в тому, що із записом DNS можуть бути зіставлені різні дані, у тому числі і яке-небудь символьне ім'я. Існує спеціальний домен *in-addr.arpa.*, записи в якім використовуються для перетворення Ip-адрес у символьні імена. Наприклад, для одержання Dns-Імені для адреси 192.168.128.5 можна запросити в Dns-Сервера запис *5.128.168.192.in-addr.arpa*, і той поверне відповідне символьне ім'я. Зворотний порядок запису частин Ip-адреси пояснюється тим, що в Ip-адресах старші біти розташовані на початку, а в символьних Dns-Іменах старші (що перебувають ближче до кореня) частини розташовані наприкінці.

Одна із проблем полягає в тому, що зворотну зону можна виділити тільки на мережу класу A, B або C (на 16777216, 65536 або 256 адрес відповідно) і ніяк інакше (маски тут не працюють).

Dns-Записи

Найбільш важливі категорії DNS записів:

- Запис A (address record) або запис адреси зв'язує хост із адресою IP.
- Запис CNAME (canonical name record) або канонічний запис імені використовується для перенапрямку на інше ім'я
- Запис MX (mail exchange) або поштовий обмінник указує сервер обміну поштою для даного домену.
- Запис PTR (pointer) або запис покажчика зв'язує ім'я хосту з його канонічним іменем. Створення запису в домен in-addr.arpa поверне IP-адреса даного хосту (див. Зворотний Dns-Запит). Наприклад, (на момент написання), www.icann.net має адресу 192.0.34.164, але запис PTR 164.34.0.192.in-addr.arpa до його канонічному імені referrals.icann.org.

- Запис NS (name server) указує на Dns-Сервер для даного домену.
- Запис SOA (start of authority record) указує, на якому сервері зберігається еталонна інформація про даний домен.

Формат Dns-Повідомлення

Рис. 1. Формат пакета DNS протоколу

Доповнення

Останнім часом розвивається технологія **DDNS** динамічного відновлення ресурсних записів зони **DNS** зовнішніми вузлами (**Dynamic DNS**; RFC-2136). Клієнти з можливостями **DDNS** можуть самі обновляти записи локальних серверів імен. Ще більш цікавий розв'язок базується на інтеграції служб **DHCP** і DNS. У цьому варіанті сервери DHCP, що підтримують DDNS, посилають відповідному до сервера DNS дані для відновлення записів, включаючи імена Netbios клієнтів DHCP. Запис оновляється після виділення Ip-Адреси. При реалізації DDNS виникають проблеми безпеки. Частина цих проблем може бути вирішена шляхом використання цифрових підписів (RFC-2137).

Ще однієї проблемою, зв'язаної зі службою імен, є атаки, які сполучені з імітацією DNS. Для подолання таких атак розроблений метод транзакційних підписів TSIG (Transaction Signarure).

У системах Windows часто використовується додаткова служба імен WINS (Windows Internet Naming Service, див. RFC-2136 і RFC-2137). Ця служба сумісна із системою динамічного конфігурування мережі DHCP. В WINS, також як і в DHCP, є частини, що працюють у клієнта й на сервері. WINS автоматично встановлюється й конфігурується при установці системи DHCP. Ця система має зручну вбудовану діагностику, що дозволяє контролювати процес обробки запитів до служби імен. WINS здійснює перетворення Netbios-Імен в Ip-Адреси. Ця техніка припускає використання протоколу Netbios поверх TCP/IP (Netbt).

2. Установка й налагодження DNS сервера на базі ОС Windows 2003 Server

Налагодження й керування Dns-Сервером здійснюється через консоль керування dnsmgmt (див. рис. 2). (Адміністрування → DNS).

Далі розглянемо на прикладі налагодження простого варіанти Dns-Сервера, який буде обслуговувати наш локальний домен «localdomain.» у мережі 192.168.1.0/24 і виконувати кешування DNS запитів з Dns-Сервера 10.0.0.10.

Необхідно попередньо налаштувати адресацію!!!

Рис. 2. Консоль управления DNS-сервером

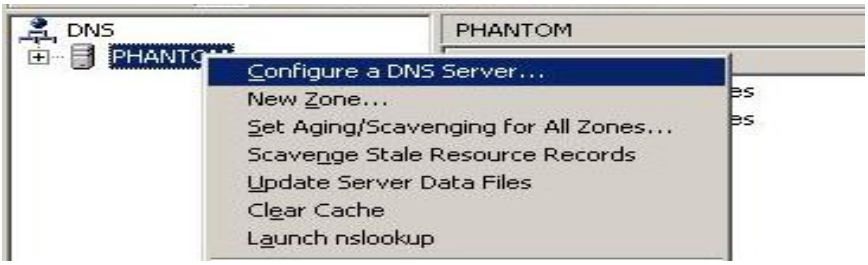


Рис. 3. Початкове налаштування DNS-сервера

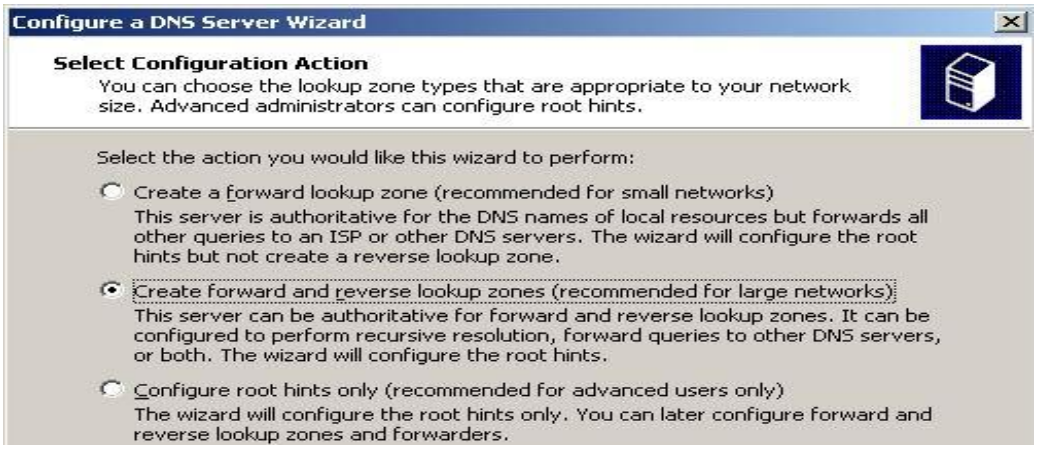


Рис. 4. Додавання прямої і зворотної DNS-зон

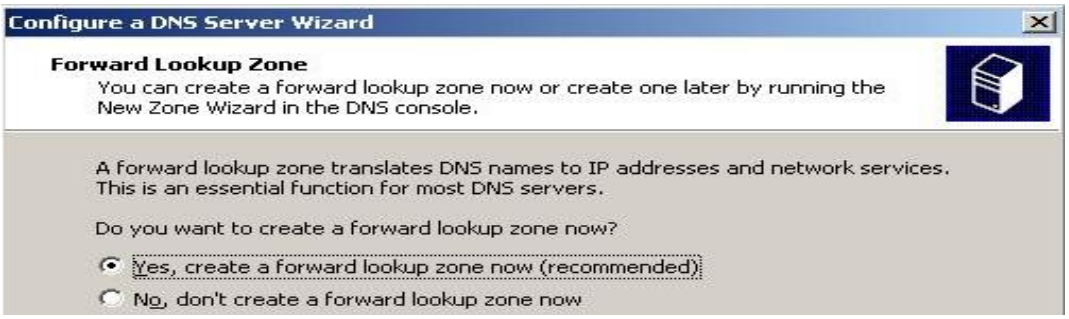


Рис. 5. Створення прямої зони

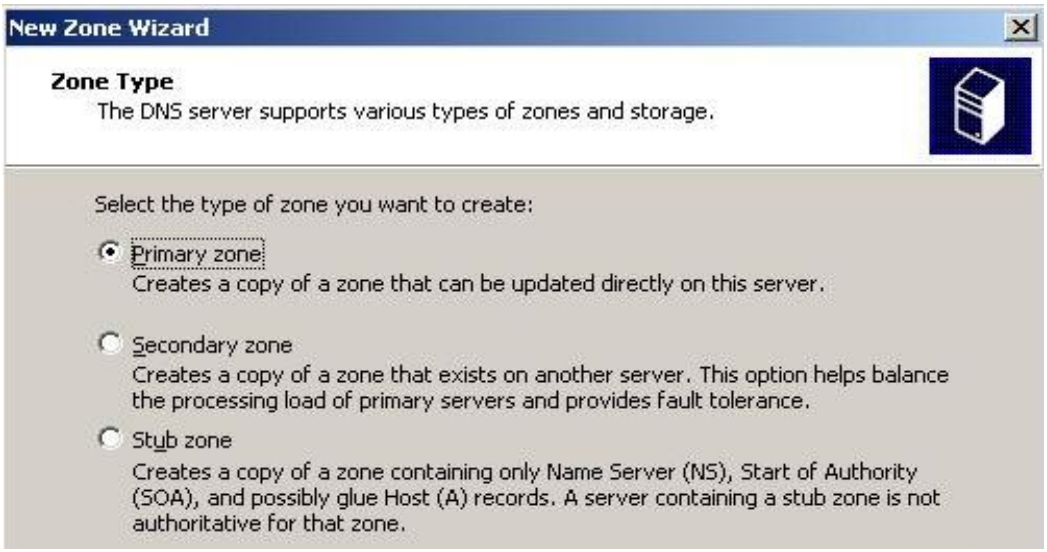


Рис. 6**.** Пряма зона буде головною

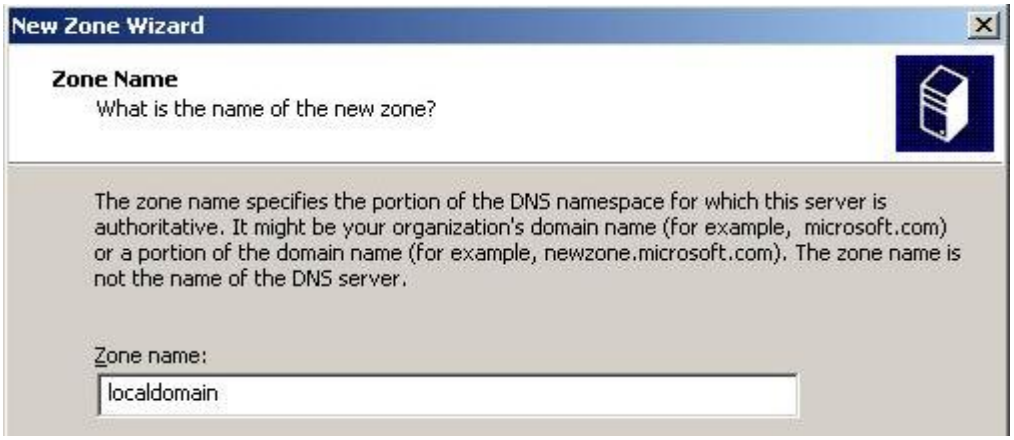


Рис. 7. Завдання імені зони (домена)

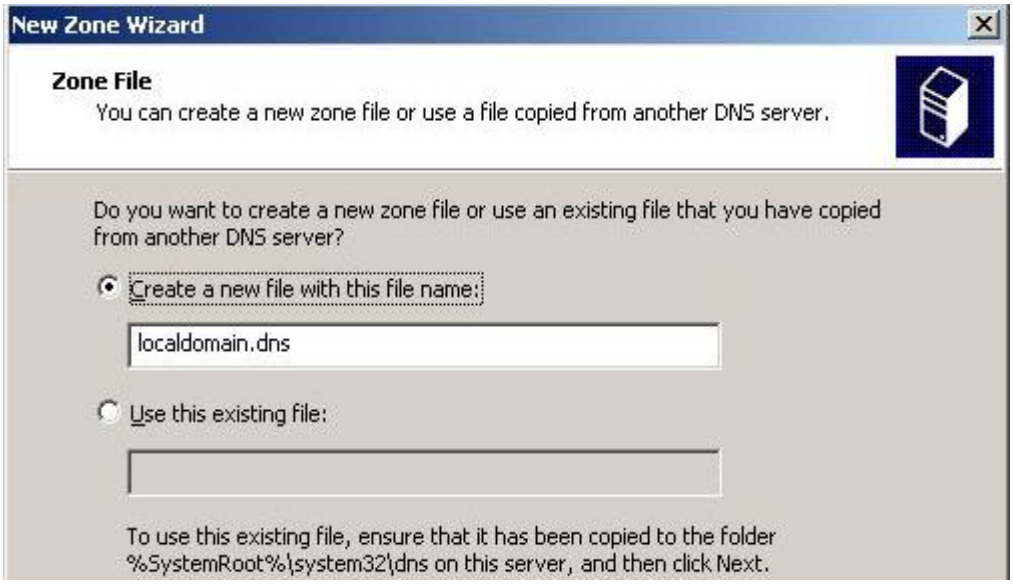


Рис. 8. Завдання імені файла, в якому буде зберігатися опис зони

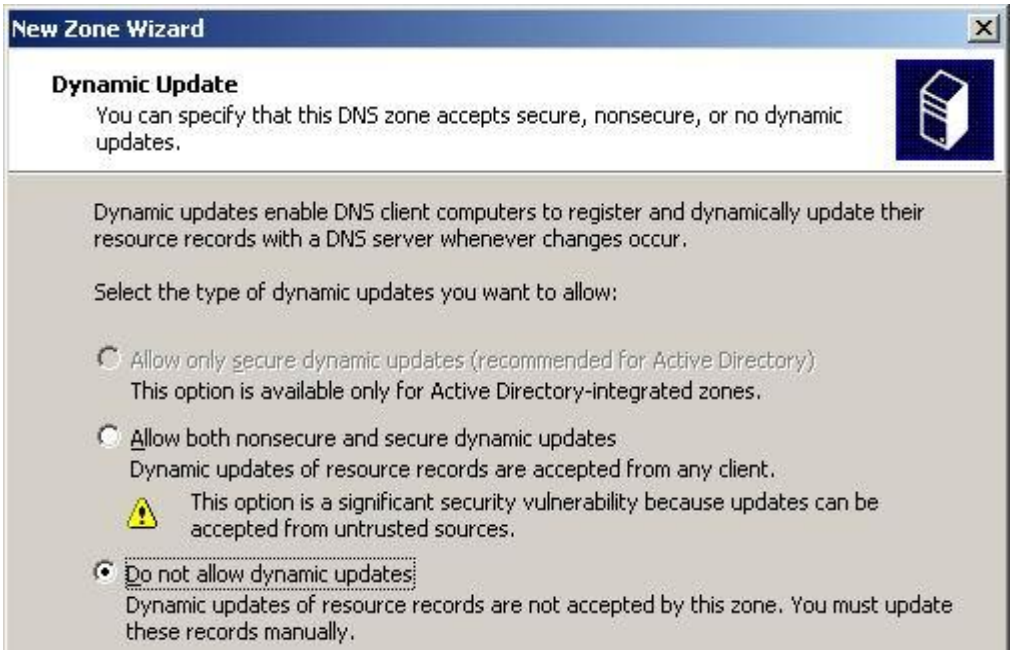


Рис. 9. Забороняємо виконувати динамічне оновлення зони

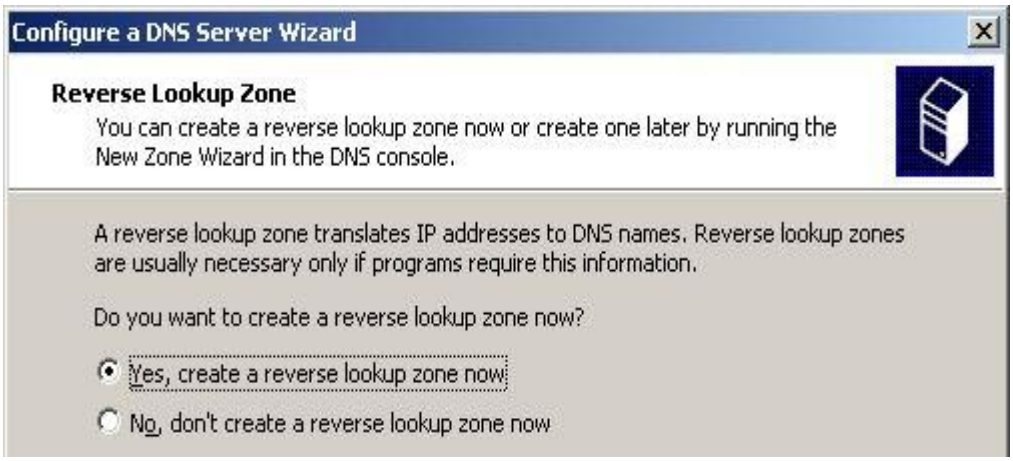


Рис. 10. Створюємо обернену зону

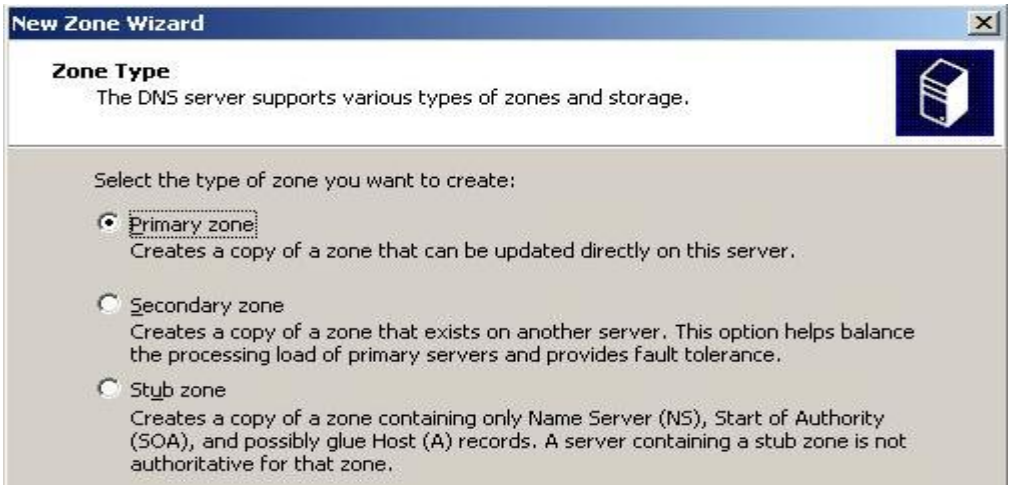


Рис. 11. Обернена зона може бути головною

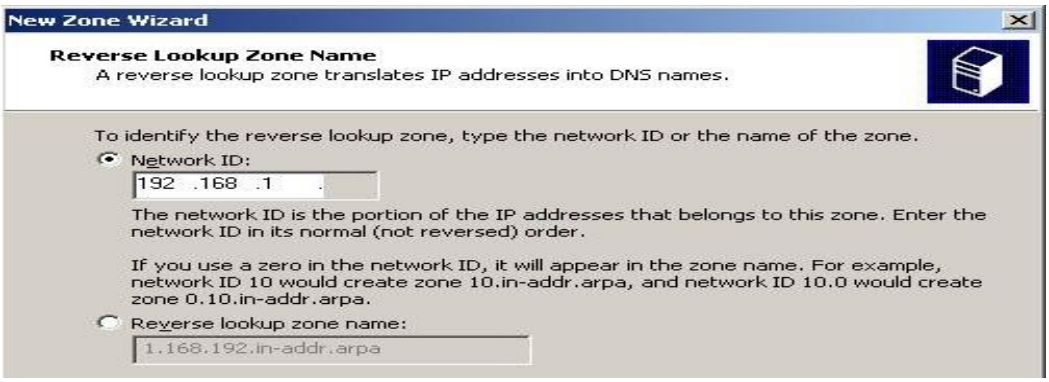


Рис. 12. Задаємо підмережу оберненої зони

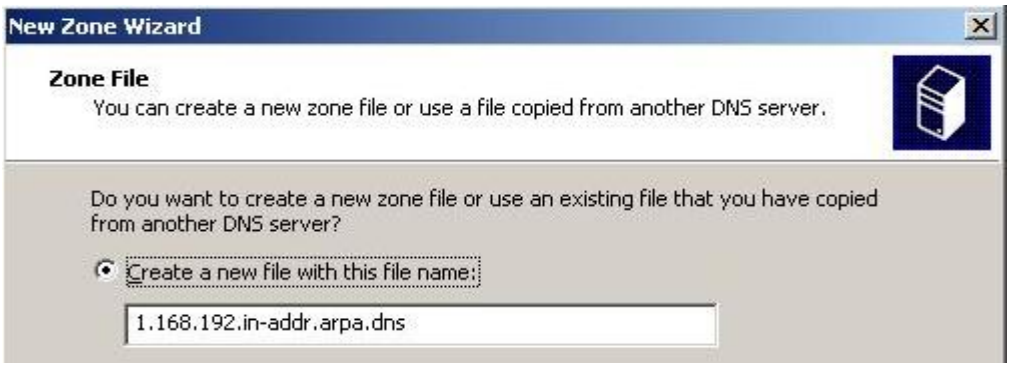


Рис. 13. Задаємо ім'я файла, в якому буде зберігатися опис оберненої зони

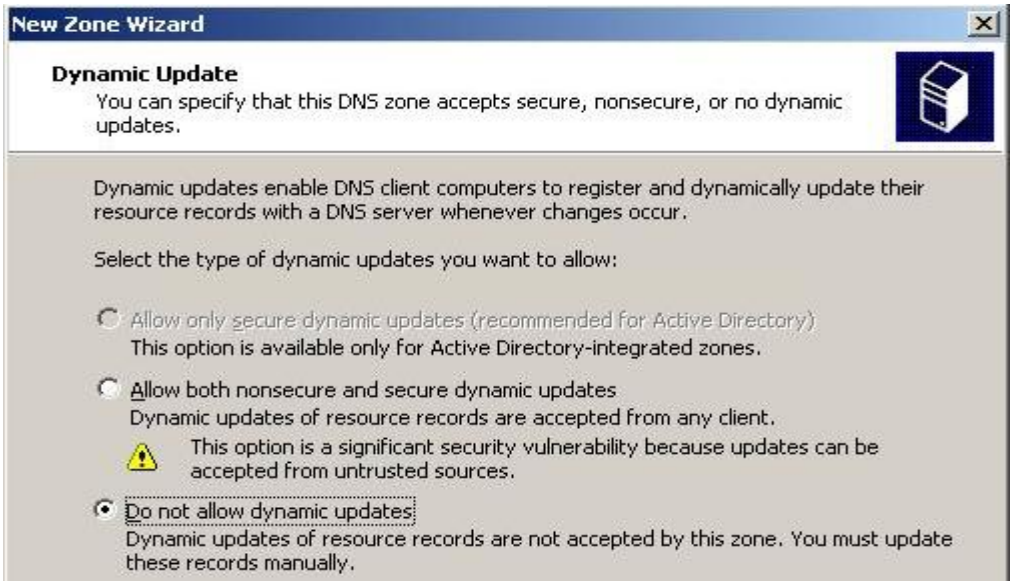


Рис. 14. Заборона динамічного оновлення зони

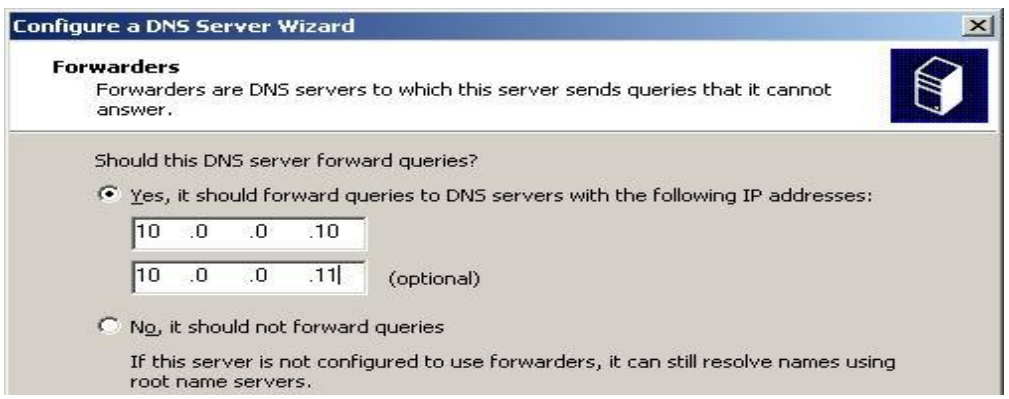


Рис. 15. Завдання первинного и вторинного DNS-серверів, до яких буде йти запит в випадку відсутності інформації на сервері що налагоджується

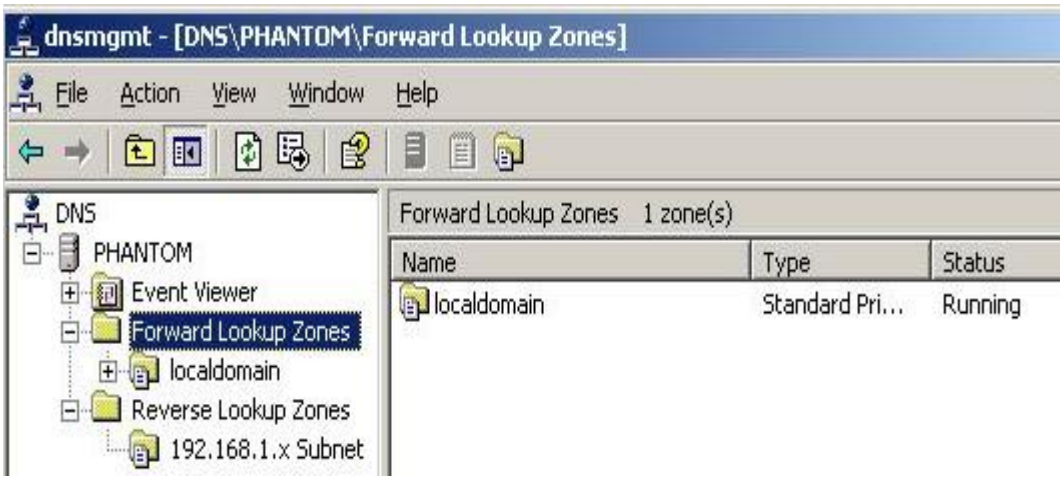


Рис. 16. Перегляд списку створених зон

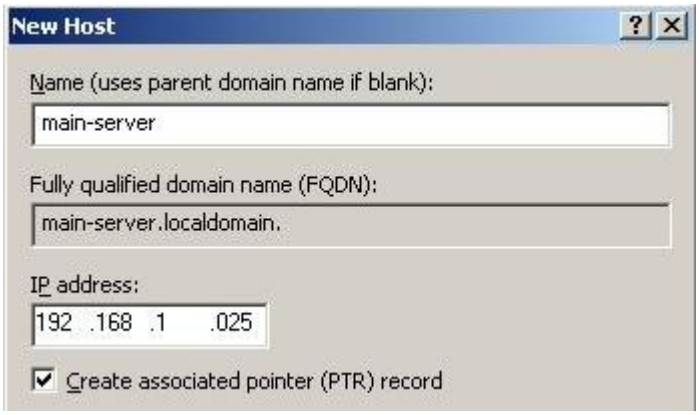


Рис. 17. Створення запису в прямій и обернених зонах для ПК з адресою 192.168.1.25

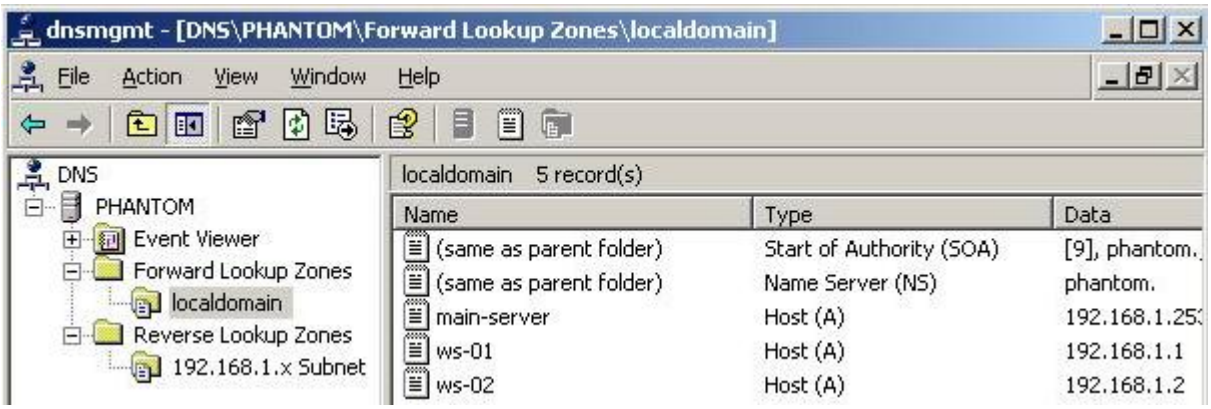


Рис. 18. Перегляд прямої зони сервера

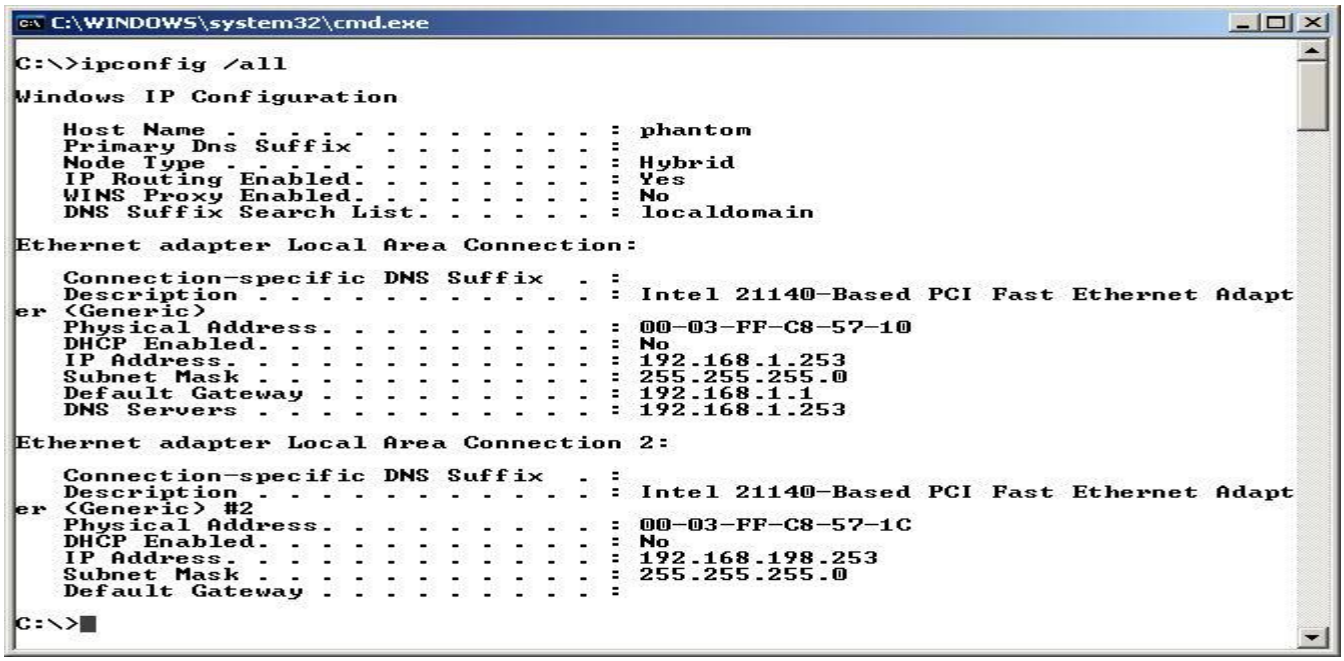


Рис. 19. Перегляд мережевих налаштувань DNS-сервера

3. Контрольні питання

1. Що таке доменні імена? Яке їхнє призначення?
2. Що таке система доменних імен?
3. Чому дана система повинна бути розподіленою?
4. Що таке DNS-Сервер? Які його функції?
5. Що таке прямій і зворотні DNS-Запити?
6. У чому відмінність рекурсивних Dns-Запитів від ітеративних? У яких випадках вони застосовні?
7. Чи може з однією Ip-адресою бути асоційовано кілька доменних імен? Відповідь пояснити.
8. Чи може бути з одним доменним іменем асоційовано кілька Ip-адрес? Відповідь пояснити.
9. Яким чином DNS допомагає розподіляти навантаження на сервери?
10. Перелічіть основні типи DNS-Записів. Поясніть їхнє призначення.

4. Завдання на лабораторну роботу

1. З'ясувати зразкове географічне місце розташування кореневих серверів імен (можна скористатися скористайтеся одним із сервісів **whois**).
2. Налаштувати DNS сервер на базі Windows 2003 Server (у якості forward сервера рекомендується використовувати DNS-Сервери 192.168.128.1 або 192.168.128.5).
3. Перевірити працездатність налаштованого сервісу.
4. За допомогою сніфера **wireshark** досліджувати механізм роботи утиліти **nslookup**.
5. Зробити висновки. Підготувати звіт з результатами проробленої роботи.

ЛАБОРАТОРНА РОБОТА 15. БАЗИ ДАНИХ DNS СЕРВЕРА

Мета роботи: отримати навички з режимів роботи DNS сервера, записів ресурсів у базі даних домену, установки ПЗ сервера DNS його конфігурування та тестування.

Зміст

1. Теорія
1.1. Режими роботи DNS сервера
1.2. Записи ресурсів у базі даних домену
1.3. Особливості розміщення й конфігурування серверів для корпоративної мережі
1.4. Установка ПЗ сервера DNS
1.5. Конфігурування сервера DNS
1.6. Тестування роботи сервера імен
2. Хід роботи

1. Теорія

1.1. Режими роботи DNS сервера

Розрізняють 3 режиму роботи сервера DNS:

master (primary). Даний режим використовується адміністратором зони, файли баз даних ведуться вручну на цьому сервері. Даний сервер є абсолютним авторитетним джерелом інформації для даної зони;

slave (secondary). Даний режим використовується на прохання адміністратора зони, яка автоматично регулярно копіюється з master сервера. Даний сервер є авторитетним джерелом інформації для даної зони;

hint (caching). Режим кешування всіх запитів, що попадають у певну зону, звичайно ".", тобто кешуються всі запити. Такий сервер звичайно використовується для прискорення роботи з мережею.

Для кожної зони, що обслуговується даним сервером, може бути обраний той або інший режим. Звичайно для зони "." усі сервери конфігуруються за типом hint, що дозволяє кешувати усі запити користувацьких робочих станцій на час життя конкретному запису DNS. Це значно прискорює обробку локальних запитів.

База даних DNS для кожного домену в найпростішому випадку являє собою набір текстових файлів, які системний адміністратор веде на головному сервері імен цього домену. У цих файлах утримуються директиви синтаксичного аналізатора ($ORIGN, $TTL) і записи про ресурси.

1.2. Записи ресурсів у базі даних домену

Файл будь-якої зони починається із запису Start Of Authority, ***SOA***. Цей запис є заголовним і містить інформацію про розміщення зони, про поштову адресу відповідальної особи й про базові тимчасові параметри записів даної зони.

Файл прямої зони містить стандартні записи ресурсів бази даних DNS для перетворення доменних імен хостів у даній зоні в Ip-адреси, визначення авторитарних DNS-Серверів даної зони, визначення хостів-оброблювачів пошти для доменних імен у даній зоні й ін.

Файли баз даних DNS складаються зі стандартних записів ресурсів. У загальному виді стандартний запис ресурсу зв'язує дані певного типу з деяким іменем і формується за шаблоном:

ім'я [час_життя_запису] IN тип_запису дані

Іменем є деяке доменне ім'я (необов'язкове ім'я фізично існуючих хосту або домену). Якщо поле "ім'я" порожнє, то значення цього поля береться з попереднього запису. Даними може бути, наприклад, Ip-адреса хосту, якщо ім'я ставиться до хосту, або DNS-Сервер домену, якщо ім'я ставиться до домену, і т.п.

Час життя запису визначає час зберігання інформації цьому запису в кеші сервера, що запросив запис, у секундах і вказується, тільки якщо воно відрізняється від часу життя, дійсного для всієї зони в записі SOA.

Основні типи записів:

SOA (Start Of Authority) – заголовок зони;

NS (Name Server) – сервер DNS;

A (Address) – Ip-адреса для хосту;

MX (Mail Exchanger) – поштовий обмінник;

CNAME (Canonical Name) – канонічне ім'я, псевдонім хосту;

PTR (Pointer) – покажчик за зворотною зоною, фактично – ім'я хосту;

Пряма зона DNS.

Розглянемо приклади файлів бази даних DNS. Першою розглянемо пряму зону для приватної частини корпоративної мережі, домен “stu.”, файл db.stu.

```
        $ORIGIN .
stu 28800 IN SOA ns.stu. dnsmaster.stu. (
                                        2005033100 ; Serial
                                        28800 ; Refresh
                                        7200 ; Retry
                                        604800 ; Expire
                                        86400 ; Time To Live)
        ; authoritative name servers for zone
 28800 IN NS ns.stu.
28800 IN NS ns1.stu.
        ; mail exchangers for entire zone
 28800 IN MX 10 stalker.stu.
28800 IN MX 20 cs.stu.
        $ORIGIN stu.
; name servers glue records
 ns IN A 192.168.0.10
 ns1 IN A 192.168.0.14
 ;servers
 dragon IN A 192.168.0.17
 auth IN CNAME dragon.stu.
cs IN A 192.168.0.14
 stalker IN A 192.168.0.10
 www IN CNAME stalker.stu.
mail IN CNAME stalker.stu.
ftp IN CNAME stalker.stu.
www.docs IN CNAME cs.stu.
kid IN A 192.168.0.12
 ; workstations
 ie-21-7 IN A 192.168.3.40
 ie-21-8 IN A 192.168.3.41
 ie-21-9 IN A 192.168.3.42
 vc-105-1 IN A 192.168.66.2
```

Перший рядок – це макрос, що говорить, що всі імена далі випливають безпосередньо за доменом “крапка”. Таким чином, для приватної мережі ми використовуємо імена в нашім приватнім дереві щодо нашого власного кореня “.”. Слід пам'ятати, що для сервера, що дозволяє одночасно й імена в корпоративній мережі, і імена в Internet, ім'я зони слід вибирати з 3-х символів, що не збігаються з іменами TLD.

Першим записом завжди йде ***SOA*** (Start of Authority), у якій вказується ім'я зони (“stu.”, або макрос @), TTL, тобто час життя цьому запису, далі – ключові слова IN (Internet records) і ***SOA***. Далі йдуть параметри зони: ім'я основного сервера DNS, поштова адреса адміністратора зони, однак замість символу “@” там стоїть крапка, оскільки @ – це посилання на ім'я зони. Відразу за дужкою, що відкривається, перебуває серійний номер даного файлу, звичайно у форматі ггггммддnn. Серійний номер необхідно збільшувати при кожній зміні файлу, що б ведені сервера ідентифікували зміни й обновили файли баз даних з головного сервера. Далі випливають стандартні часи в секундах для даної зони:

Refresh – час, після закінчення якого вторинні сервери повинні обновити дані з первинних серверів (zone transfer);

Retry – час, через який вторинні сервери повинні зробити повторну спробу відновлення, якщо попередня спроба не вдалася;

Expire – час, через який вторинні сервери повинні викинути запис про зону й уважати її недоступною, якщо відновлення не вдалися.

TTL – стандартний час життя записів з даної зони для кешуючих серверів.

Наступна група записів є так само обов'язковою й указує на авторитетні сервера імен для даної зони – запису типу ***NS***. Авторитетним є сервер, на якім інформація відповідає реальному стану зони, тобто регулярно оновлюється. Украй бажано, щоб імена, зазначені в цій секції, мали відповідні адресні ***IN A*** записи в цій же базі даних.

Нижче знаходиться секція поштових обмінників, тобто записи типу ***MX*** (Mail Exchanger). Вони вказують на сервери електронної пошти, які здатні ухвалювати пошту для всього домену за протоколом SMTP. Чим менше цифра перед іменем, тем більший пріоритет має даний поштовий сервер. Як правило, запис із найвищим пріоритетом ставиться до сервера, на якім пошта закінчує свій шлях, а інші записи ставляться до серверів-релеїв, на яких пошта може зберігатися якийсь час, поки основний поштовий сервер для зони не доступний. Природно, записи ***MX*** на релеї не можна розставляти довільно, оскільки релей обов'язково повинен бути сконфігурований для приймання пошти даного домену. При відсутності запису MX для якого-небудь доменного імені, пошта, адресована із цим доменним іменем, буде доставлятися безпосередньо на хост, що має таке ім'я. Однак, такого хосту може не бути, у цьому випадку пошта повернеться відправникові з повідомленням про помилку.

Нижче, після макросу “$ORIGIN stu.”, що задає суфікс для всіх записів нижче, випливають записи типу ***IN A***, призначені для завдання відповідності між іменем хосту в зоні і його IP адресою.

Для завдання псевдонімів хостам використовується запис ***CNAME*** (Canonical Name). Псевдоніми зручні для вказівки на стандартні сервіси, такі як www, mail, ftp, а так само для завдання псевдонімів, використовуваних для створення віртуальних серверів.

Розглянемо тепер файл зони stu.cn.ua. Дана зона мало чому відрізняється від попередньої зони зовні.

```
        $ORIGIN .
stu.cn.ua 28800 IN SOA ns.stu.cn.ua. nsmaster.stu.cn.ua(
                                        2005033100 ; Serial
                                        28800 ; Refresh
                                        7200 ; Retry
                                        604800 ; Expire
                                        86400 ; Time To Live
                                        )
        ; authoritative name servers for zone
 IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
IN NS ns.cn.ua.
```

```
        ; mail exchangers for entire zone
 IN MX 10 stalker.stu.cn.ua.
IN MX 15 cs.stu.cn.ua.
IN MX 20 relay1.cn.ua
        ; name servers glue records
 ns.cn.ua IN A 212.86.96.10
 $ORIGIN stu.cn.ua.
ns IN A 195.69.76.130
 ns1 IN A 195.69.76.134
 ;servers
 dragon IN A 195.69.76.137
 auth IN CNAME dragon.stu.cn.ua.
cs IN A 195.69.76.134
 stalker IN A 195.69.76.130
 www IN CNAME stalker.stu.cn.ua.
mail IN CNAME stalker.stu.cn.ua.
ftp IN CNAME stalker.stu.cn.ua.
www.docs IN CNAME cs.stu.cn.ua.
; workstations
 admin IN A 195.69.76.139
```

Конфігурація даної зони практично повторює попередню зону, однак відмінність у тому, що дана зона є субдоменом домену cn.ua. Виходить, вона повинна бути делегована у відповідній зоні cn.ua приблизно так, як показано в наступному фрагменті:

```
        $ORIGIN cn.ua.
stu IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
IN NS ns.cn.ua.
        $ORIGIN .
ns.stu.cn.ua IN A 195.69.76.130
 ns1.stu.cn.ua IN A 195.69.76.134
```

Як видно з наведеного фрагмента, в “материнській” зоні cn.ua. перебувають тільки записи про сервери імен для делегованої зони stu.cn.ua. Керування іншою інформаційною базою зони передається на сервера ns.stu.cn.ua і ns1.stu.cn.ua.

Зворотна зона DNS

Тепер розглянемо файли зворотних зон, призначені для проведення зворотного DNS-Перетворення, тобто " Ір-адреса – в доменне ім'я".

Для приватних блоків адрес, таких як 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16 ніяких проблем з делегуванням, у загальному немає, оскільки ці адреси не маршрутизуються в Internet й потрібні тільки усередині приватної мережі.

```
        $ORIGIN .
        0.168.192.IN-ADDR.ARPA. 86400 IN SOA ns.stu. dnsmaster.stu.
        (                               2006060200
                                        86400
                                        14400
                                        3600000
                                                345600
```

)
86400 IN NS ns.stu.
86400 IN NS ns1.stu.
$ORIGIN 0.168.192.IN-ADDR.ARPA.
10 IN PTR stalker.stu.
14 IN PTR cs.stu.
17 IN PTR dragon.stu.
12 IN PTR kid.stu.

Варто звернути увагу, що ім'я зони складається з розгорнутих стосовно запису адреси цифр. Для адресного блоку 192.168.0.0/24 ім'я зони 0.168.192.IN-ADDR.ARPA. INADDR.ARPA. – це спеціальний домен верхнього рівня, відведений для делегування зворотних зон. У файлі зворотної зони присутній, звичайно ж, запис ***SOA***, як мінімум пари записів типу ***NS*** про офіційні авторитетні сервери й запису типу ***PTR*** (Pointer) імена, що ставлять у відповідність адреси. Зворотна зона для публічних адрес 195.69.76.0/24 наведена нижче:

$ORIGIN .
76.69.195.IN-ADDR.ARPA. 86400 IN SOA ns.stu.cn.ua dnsmaster.stu.cn.ua (2004060200
86400 14400 3600000 345600)
IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
$ORIGIN 0.168.192.IN-ADDR.ARPA.
10 IN PTR stalker.stu.cn.ua.
14 IN PTR cs.stu.cn.ua.
17 IN PTR dragon.stu.cn.ua.
12 IN PTR kid.stu.cn.ua.

Відмінність даної зони від попередньої знову ж тільки в тому, що вона є публічною й повинна делегуватися відповідно до правил видачі й реєстрації IP-адрес. Коротенько необхідно відзначити наступне. Видача блоків адрес споживачам проводиться локальними Інтернет реєстраторами (LIR), які, у свою чергу, одержують їх від регіональних реєстратур. У Європі це – безприбуткова організація RIPE (http://www.ripe.net/),фінансована провайдерами. Основні функції регіональних реєстратур – координація використання IP адрес і, відповідно, маршрутизації в регіоні. Для одержання свого блоку публічних адрес необхідно заповнити відповідні форми RIPE і направити їхньому LIR.

1.3. Особливості розміщення й конфігурування серверів для корпоративної мережі

Оскільки сервіс DNS є критичним для функціонування мережі, то в мережі повинно бути як мінімум 2 сервери. Звичайно розміщають їх так, як показано на рис 1. Для внутрішньої мережі доступні обоє сервера, а для зовнішньої – тільки зовнішній сервер. Внутрішній сервер є первинним для внутрішніх доменів і використовує зовнішній у якості форварда (forwarding server), оскільки прямо не бачить домен “.” . Зовнішній сервер у загальному випадку не повинен відповідати на рекурсивні запити ззовні, оскільки він може бути використаний як платформа для Ddos атак на інші сервера.

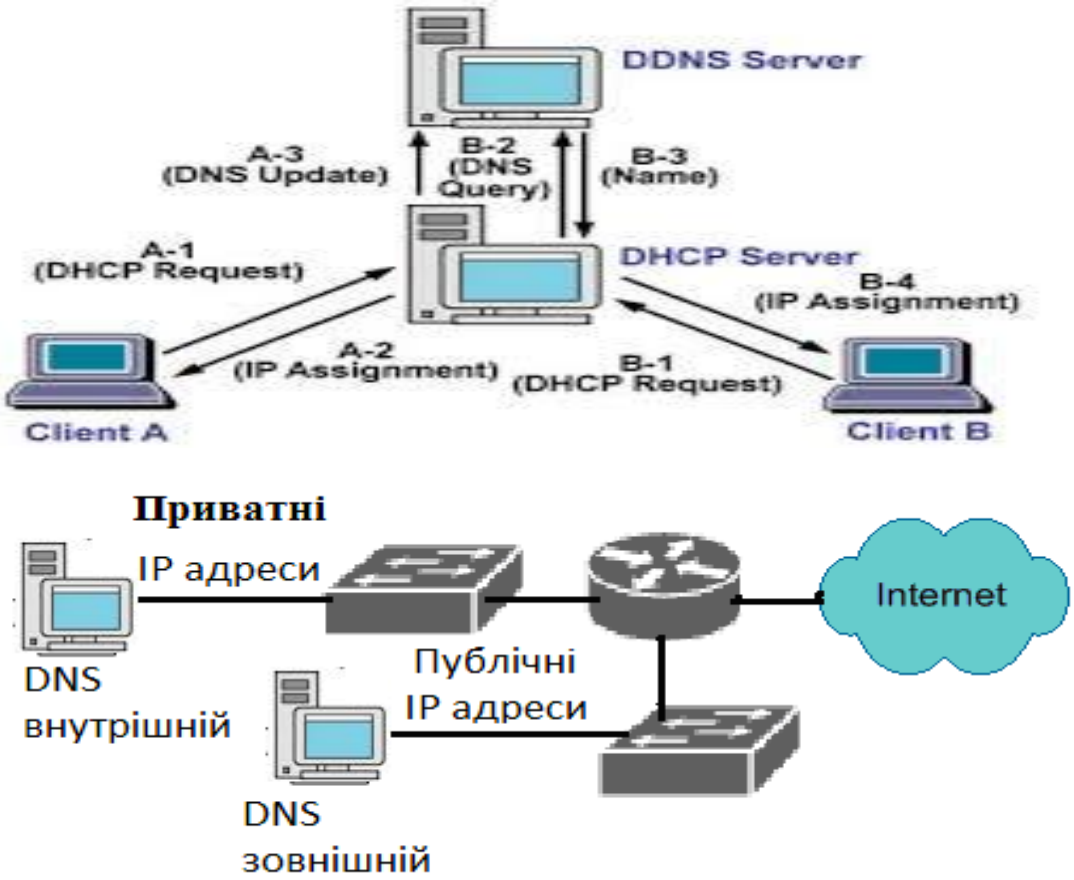


Рис. 1. Розташування серверів імен у мережі

1.4. Установка ПЗ сервера DNS

Одним із найбільш популярним ПЗ, що реалізують сервіс DNS, є сервер ***bind*** (Berkeley Internet Name Daemon), підтримуваний Internet Software Consortium (http://www.isc.org). Існують легкі реалізації, призначені для роботи в якості кешуючих серверів, є реалізації, специфічні для конкретних комерційних ОС, однак на практиці краще використовувати bind, оскільки він розповсюджується під ліцензією GPL, тобто разом з вихідним кодом, що гарантує відсутність уразливостей, що давно не виправляються, і інших неприємностей закритого коду.

Пакет bind поставляється практично з усіма дистрибутивами Linux і xbsd.

Для роботи сервера в ОС Fedora Linux необхідно встановити наступні пакети: bind-utils – утиліти для роботи з DNS і тестування сервера, bind – властиво сервер, bind-chroot – файли, необхідні для запуску сервера в індивідуальному оточенні в режимі chroot. Запуск сервера в цьому режимі мінімізує втрати при зломі системи через працюючий сервіс.

Перевірити, установлені пакети чи ні, можна командою:

rpm –qa | grep bind

Якщо пакети не встановлені, установіть їхньою командою:

yum install bind-utils bind bind-chroot

При установці сервера автоматично створюється конфігурація для кешуючого сервера зони «.» і для первинних серверів локальних зон.

Для невеликого сервера на кілька дрібних зон конфігурації зони звичайно зберігаються в текстових файлах. У нашім випадку – це **/var/named/chroot/var/named/*.** Для більших зон, що містять мільйони записів, використовуються спеціальні модулі зберігання, які можуть зберігати дані зон у реляційних БД (Postgresql) або на сервері LDAP.

1.5. Конфігурування сервера DNS

Розглянемо докладніше приклад файлу конфігурації для такого випадку: наш сервер є основним для внутрішньої корпоративної мережі 192.168.0.0 і внутрішнього домену “stu.”, і кешуючим для домену “.”. Усі шляхи, наведені нижче, у випадку роботи сервера в оточенні chroot, потрібно понищать як відносні до **/var/named/chroot.** Файл конфігурації **/etc/named.conf** наведений нижче:

```
        options {
 directory "/etc/namedb";
 forward first;
 forwarders {
  195.69.76.130;
 };
};

        // caching server for root domain
zone "." {
 type hint;
 file "named.root";
};

// it's not neccesary but good to resolve localhost
zone "0.0.127.IN-ADDR.ARPA" {
 type master;
 file "localhost.rev";
        };
        // private zone for our network
zone "stu" {
 type master;
 file "db.stu.private";
 allow-transfer{
   195.69.76.130;
 };
 allow-query{
   192.168.0.0/16;
 };
};
// Inverse zone for private zone stu
zone "0.168.192.IN-ADDR.ARPA" {
 type master;
 file "db.192.168.0";
 allow-transfer{
  195.69.76.130;
 };
 allow-query{
  192.168.0.0/16;
 };
};
```

У наведеному вище файлі конфігурації все інтуїтивно зрозуміло, однак варто особливо відзначити, що сервер в DNS з адресою 195.69.76.130 використовується як форвард і як вторинний сервер для внутрішніх доменів. Пропозиція ***allow-transfer***

використовується для обмеження повного перекачування зони тільки на вторинний сервер. Пропозиція ***allow-query*** указує серверу, що відповідати на запити за даними зон можна тільки хостам з наведеного блоку адрес.

Нижче наведена конфігурація другого сервера. Крім того, він є первинним для публічних зон stu.cn.ua і 76.69.195.IN-ADDR.ARPA.

```
        options {
 directory "/etc/namedb";
 forward first;
 forwarders {
   212.86.96.10;
 };
};

        // caching server for root domain
zone "." {
 type hint;
 file "named.root";
};

// it's not neccesary but good to resolve localhost
zone "0.0.127.IN-ADDR.ARPA" {
 type master;
 file "localhost.rev";
        };
        // private zone for our network
zone "stu" {
 type slave;
 file "db.stu.private";
 master {
   192.168.0.10;
 };
 allow-query{
   192.168.0.0;
 };
};
// Inverse zone for private zone stu
zone "0.168.192.IN-ADDR.ARPA" {
 type slave;
 file "db.192.168.0";
 masters {
  192.168.0.10;
 };
 allow-query{
   192.168.0.0;
 };
};

// public zone for our network
zone "stu.cn.ua." {
 type master;
 file "db.stu.cn.ua";
```

```
 allow-transfer{
   212.86.96.10;
 };
};
        // Inverse zone for public zone stu.cn.ua.
zone "76.69.195.IN-ADDR.ARPA" {
 type master;
 file "db.195.69.76";
 allow-transfer{
   212.86.96.10.
 };
};
```

Відмітимо, що тут з'явилася пропозиція ***allow-query***, необхідна для того, щоб даний сервер міг відповідати на запити внутрішньої зони тільки у внутрішню мережу. Пропозиція allow-transfer використовується так само, як і в попередньому випадку й обмежує повне перекачування всієї зони тільки серверу з адресою 212.86.96.10, який є вторинним для даної зони. Цей же сервер використовується і як форвард. Суворо кажучи, такої необхідності немає, але в ситуації, коли чомусь пів-Internet не видно, а цей форвард перебуває в межах досяжності й бачить увесь Інтернет, використання форварда виявляється виправданим.

1.6. Тестування роботи сервера імен

Тестування роботи сервера проводиться командою dig, яка дозволяє робити довільні запити до зазначеного в командному рядку сервера. Нижче наведений приклад запиту до DNS сервера, розташованого на локальному комп'ютері на предмет запису SOA для зони stu.

```
        al@stalker$>dig @127.0.0.1 SOA stu
        ; <<>> Dig 8.3 <<>> @127.0.0.1 SOA stu
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
        ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12648
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
;; ADDITIONAL: 2
;; QUERY SECTION:
;; stu, type = SOA, class = IN
        ;; ANSWER SECTION:
stu. 8H IN SOA ns.stu. dnsmaster.stu. (
2005033100 ; serial
8H ; refresh
2H ; retry
1W ; expiry
1D ) ; minimum
        ;; AUTHORITY SECTION:
stu. 8H IN NS ns.stu.
stu. 8H IN NS ns1.stu.
        ;; ADDITIONAL SECTION:
ns.stu. 8H IN A 192.168.0.10
ns1.stu. 8H IN A 192.168.0.14
        ;; Total query time: 19 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
```

```
;; WHEN: Wed Sep 14 14:37:22 2005
;; MSG SIZE sent: 21 rcvd: 134
```

Розберемо вивід команди. Слід зазначити, що вивід містить власне відповідь на задане питання й додаткові відомості, відзначені як коментарі знаками “;;” на початку рядка. Оскільки ми запитували запис SOA, то він й показаний в секції відповідей. Далі слідує секція авторитетності, у якій вказуються авторитетні сервери для даної зони, і, нарешті, додаткова секція, де звичайно вказуються IP адреси (записи IN A) для авторитетних серверів даної зони. Нижче наведений ще один приклад запиту типу A.

```
        al@stalker$dig @127.0.0.1 A stalker.stu
        ; <<>> Dig 8.3 <<>> @127.0.0.1 A stalker.stu
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14417
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
;; ADDITIONAL: 2
        ;; QUERY SECTION:
;; stalker.stu, type = A, class = IN
        ;; ANSWER SECTION:
stalker.stu. 8H IN A 192.168.0.10
        ;; AUTHORITY SECTION:
stu. 8H IN NS ns.stu.
stu. 8H IN NS ns1.stu.
        ;; ADDITIONAL SECTION:
ns.stu. 8H IN A 192.168.0.10
ns1.stu. 8H IN A 192.168.0.14
        ;; Total query time: 3 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
;; WHEN: Wed Sep 14 14:47:33 2005
;; MSG SIZE sent: 29 rcvd: 112
```

Як видно із прикладу, крім зажаданого запису A, видані знову ж дві секції про авторитетні сервери, тобто ті сервери, де інформація про дану зону найбільш достовірна.

Якщо запит попадає до кешуючого серверу, то інформація про зону в ньому може бути застарілою. Запити для перевірки зворотної зони потрібно давати у формі повного імені записи PTR. Див. приклад нижче:

```
        alukin@stalker$dig @127.0.0.1 SOA 1.1.168.192.IN-ADDR.ARPA
        ; <<>> Dig 8.3 <<>> @127.0.0.1 SOA 1.1.168.192.IN-ADDR.ARPA
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
;;ADDITIONAL: 0
        ;; QUERY SECTION:
;; 1.1.168.192.IN-ADDR.ARPA, type = SOA, class = IN
        ;; AUTHORITY SECTION:
1.168.192.IN-ADDR.ARPA. 4D IN SOA ns.stu. dnsmaster.stu. (
2001101800 ; serial
```

1D ; refresh
4H ; retry
5w6d16h ; expiry
4D) ; minimum
;; Total query time: 8 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
;; WHEN: Wed Sep 14 14:54:58 2005
;; MSG SIZE sent: 42 rcvd: 94

2. Хід роботи

Виконання даної лабораторної роботи складається з наступних кроків:

1. Створіть файли зон для прямої і зворотної приватної зони. Виберіть блок адрес 172.16.X.0, де X – номер машини в класі. Сконфігуруйте первинний сервер DNS для цих зон на локальному комп'ютері й запустіть його. Не забудьте, що всі повідомлення виводяться не на консоль, а в системний журнал. Повідомлення зручніше за все переглядати в окремому терміналі командою:

tail -f /var/log/messages

2. Проведіть тестування створених прямої і зворотної зон за допомогою команди ***dig***.

3. Проведіть тестування дозволу зовнішніх імен вашим сервером. Запросіть, наприклад інформацію про зону slashdot.org.

4. Сконфігуруйте ваш сервер як вторинний для зон, які створив ваш сусід по лабораторії. Зробіть корегування й перевірку записів зон на предмет записів типу NS. Зробіть перевірку командою ***dig***, звертаючи особливу увагу на секцію “AUTHORITY SECTION”.

3. Контрольні питання

1. Чому для корпоративних зон зручніше використовувати 3-х буквені імена?
2. У якому випадку сервер імен уважається авторитетним?
3. Які параметри відповідають за час відновлення зони вторинним сервером?
4. Як забезпечити захист зони від копіювання й від перегляду?
5. Який запис RR застосовується при створенні віртуальних серверів?
6. Який запис RR задає поштовий обмінник для всієї зони?
7. Який файл містить адреси кореневих серверів імен, необхідних для ініціалізації кешу й рекурсивних запитів?
8. Що таке рекурсивний запит?
9. Як проводиться установка головного сервера для конкретної зони?

ЛАБОРАТОРНА РОБОТА 16.
РЕЗЕРВНЕ КОПІЮВАННЯ В WINDOWS SERVER 2012

Мета роботи: познайомитися із засобами організації резервного копіювання в операційній системі Microsoft Windows Server 2012.

Зміст

1. Теорія
1.1. Створення копії
1.2. Організація резервного копіювання за розкладом.
1.3. Відновлення даних
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Створення копії

З погляду керування ризиками, важливість процедури резервного копіювання дуже висока. У тих випадках, коли реалізація погрози приведе до зміни або видалення даних, ушкодження програмних компонентів системи, резервне копіювання дозволяє знизити заподіяний збиток і значно прискорити відновлення системи.

При розробці політики резервного копіювання потрібно визначити, як мінімум параметри копіювання:

- частоту виконання резервних копій;
- порядок відновлення даних з резервних копій;
- обсяг носіїв інформації, які виділяються для зберігання резервних копій;
- кількість збережених копій;
- питання забезпечення безпеки носіїв резервних копій.

Утиліти резервного копіювання Windows Server 2012 суттєво відрізняються від того, що було в Windows Server 2003 (де ці завдання вирішувалися за допомогою утиліти ntbackup). Щоб їх використовувати, для початку потрібно їх установити (за замовчуванням, вони не встановлюються). Робиться це за допомогою **Server Manager** (рис. 1) **(Диспетчер серверів)**, де треба вибрати пункт **Компонента Система архівації Windows Server** (рис. 2).

Як видно на рис. 2, пропонується вибрати наступні опції:

- Windows Server Backup;
- Command-line tools (*утиліти командного рядка*).

Установка останніх, дозволяє управляти резервним копіюванням за допомогою сценаріїв і вимагає установки Windows Powershell. Але для виконання лабораторної буде досить установити тільки Windows Server Backup.

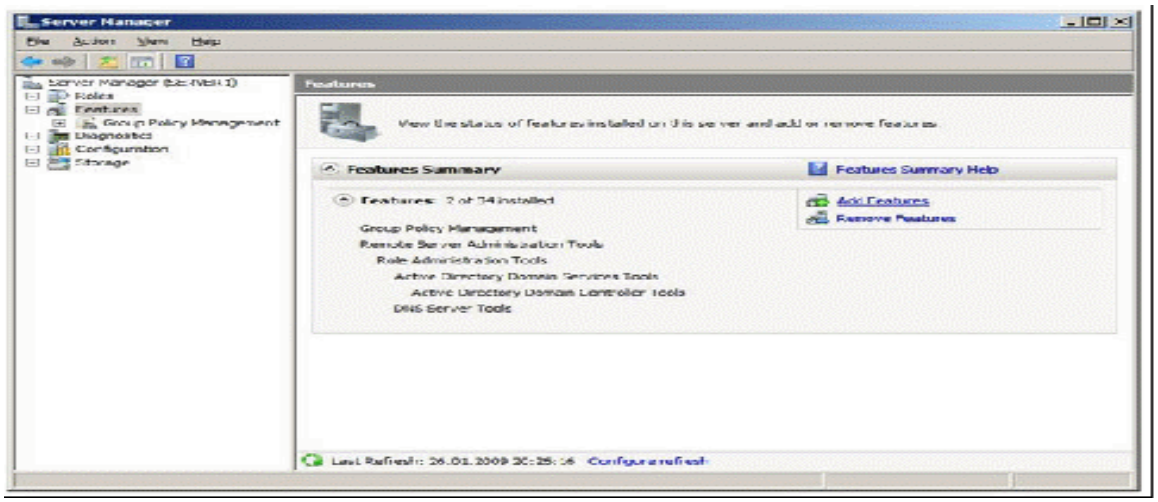


Рис. 1. Оснащення Server Manager дозволяє додати компоненти

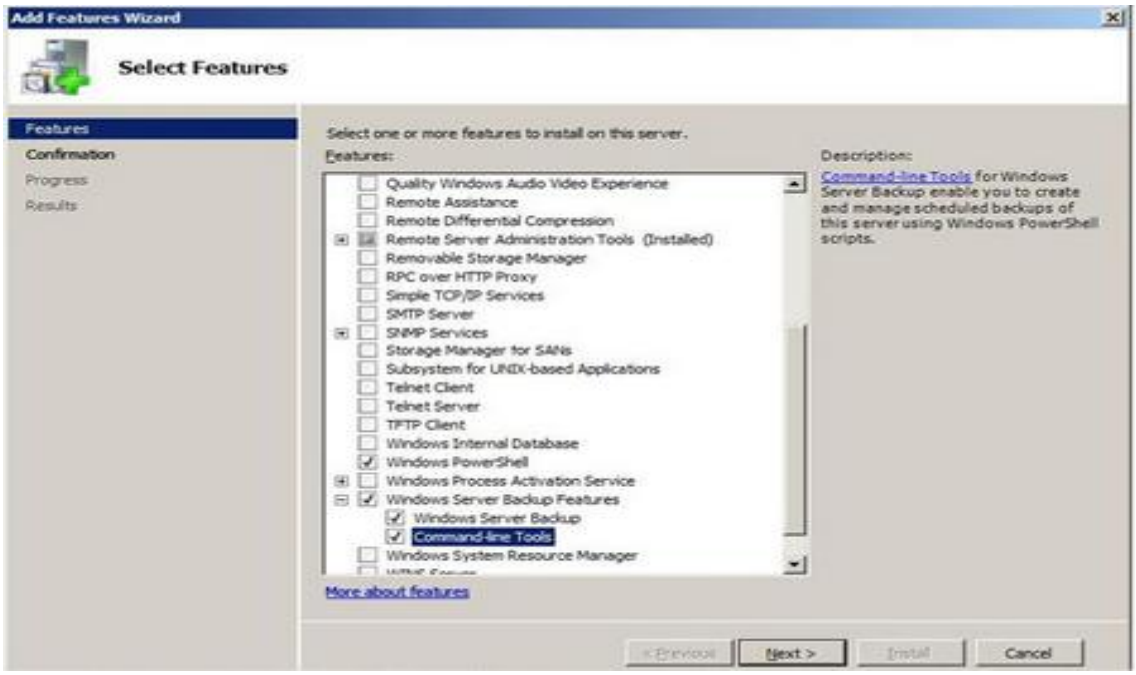


Рис. 2. Добавлення утиліт резервного копіювання

Після установки, у меню **Administrative Tools** стає доступною оснащення **Windows Server Backup**. З його допомогою можна проводити резервне копіювання даних на локальному або віддаленому комп'ютері (якщо це дозволено налаштуваннями).

Розглянемо, як це відбувається. Запустимо утиліту. Резервне копіювання може проводити користувач, що належить групі **Administrators** (Адміністратори) або **Backup Operators** (Оператори архіву). При цьому, у членів групи **Backup Operators** при запуску оснащення **Windows Server Backup** буде додатково запитуватися пароль (у вікні **User Account Control**), тому що ці операції ставляться до розряду потенційно небезпечних.

У вікні оснащення в списку доступних дій (**Actions**), розташованому в правій частині екрану, виберемо опцію **Backup Once …** (тобто однократна архівація). майстер, що запустився, резервного копіювання запропонує вибір між налаштуваннями для вже запланованого копіювання **(The same options that you used in the Backup Schedule Wizard for scheduled** backups) і новими **(Different** options). Потрібно вибрати другий варіант (якщо, як у нашім прикладі, утиліта раніше не використовувалася, то перший пункт списку буде неактивний).

Наступне вікно майстра дозволяє вибрати, чи робити повне резервне копіювання або копіювання окремих розділів (рис. 3). Тут проявляється перша відмінність нових інструментів – резервне копіювання окремих папок і файлів робити не можна, тільки логічний диск цілком.

Хотілося б також звернути увагу на напис у нижній частині екрана, там дається посилання на розділ довідки, що описує виконання за допомогою *утиліти командного рядка* резервного копіювання тільки стану системи (**System State**).

Виберемо варіант **Custom**.

Тоді на наступному екрані з'явиться список дисків (рис. 4). Установлюючи або знімаючи оцінки, можна вказати, дані резервну копію.

Опція **Enable System Recovery** включає в архів розділи, де перебувають компоненти операційної системи й файли необхідні для завантаження (тобто оцінку напроти цих розділів буде не зняти).

Припустимо, нам потрібно зробити резервну копію диска E:, на якім перебувають користувацькі дані. Тоді оцінки встановлюємо так, як це зроблене на рис. 4 і переходимо до наступної стадії, на якій потрібно визначити, куди буде проводитися копіювання. Це може бути локальний диск (жорсткий диск, DVD-Привод і т.д.) або мережева папка. Треба

враховувати, що архівна копія не може зберігатися на диск, що входить у перелік, які архівуються. Також не можна зберегти архів на диск, де зберігаються файли операційної системи

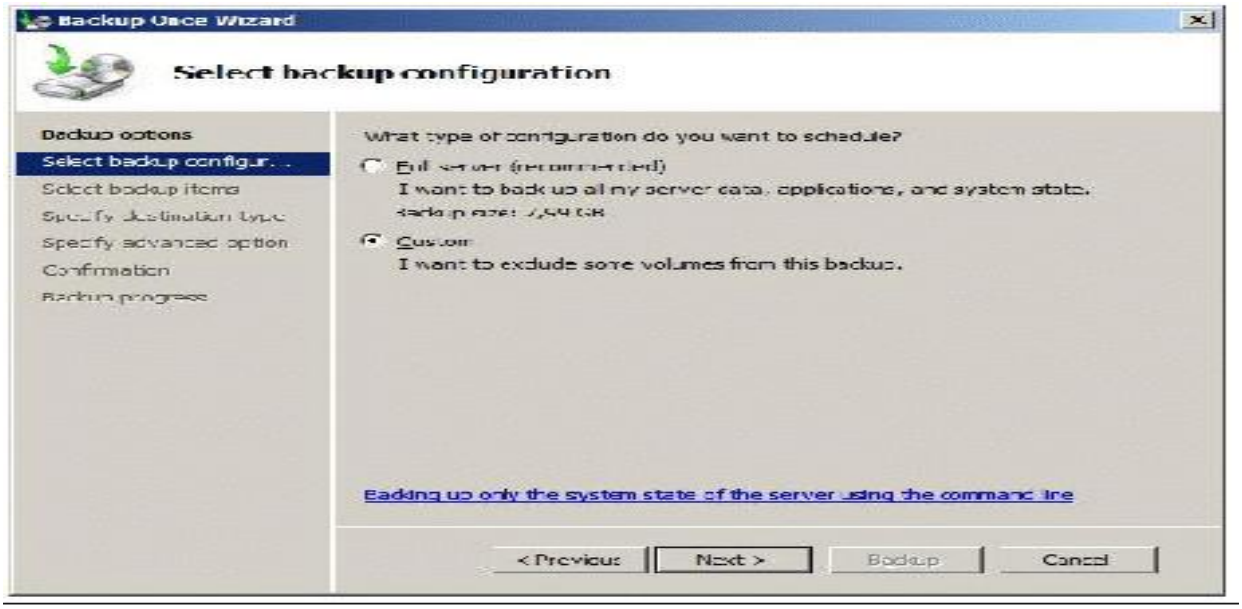


Рис. 3. Вибір типу копіювання

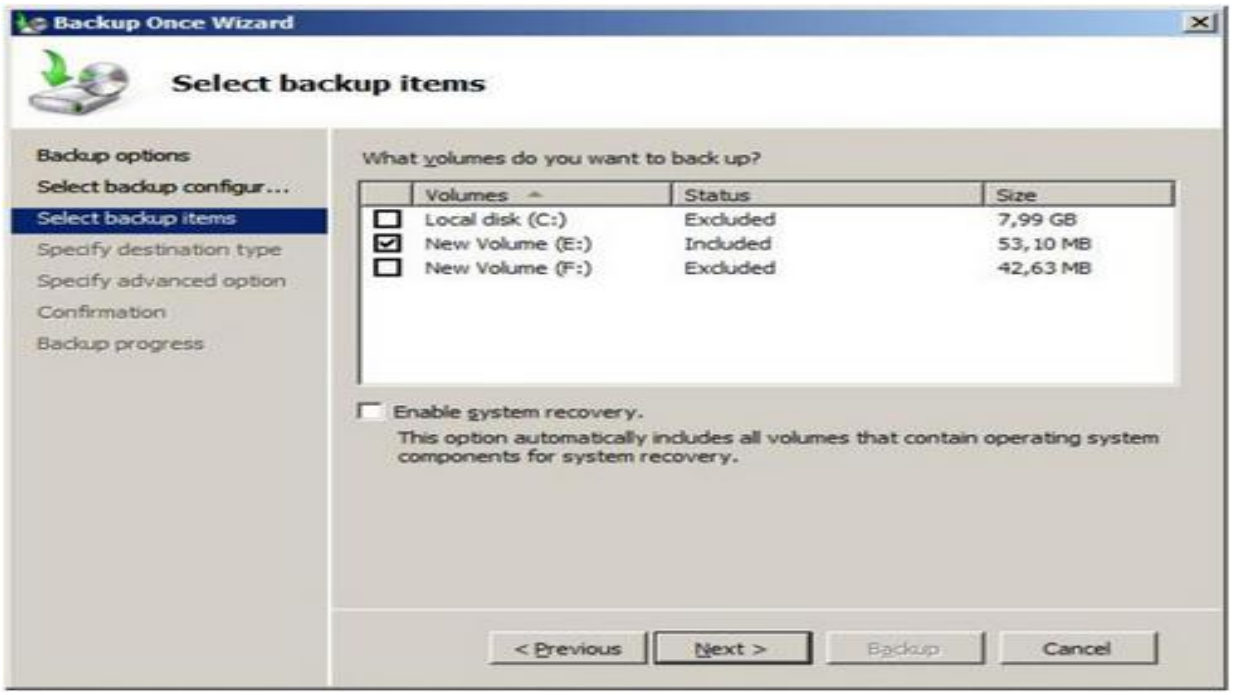


Рис. 4. Вибір дисків для резервного копіювання

Враховуючи все вищевикладене, у розглянутому прикладі можна зробити резервну копію диска E: на диск F:, у мережеву папку або на DVD -Диск. Виберемо перший варіант, що й укажемо в наступнім вікні майстра. Після чого буде запропоновано вибрати тип резервного копіювання (рис. 5).

Служба Volume Shadow Copy Service (*VSS*) може при резервнім копіюванні відзначати файли, як поміщені в архів, або не робити це. Якщо крім засобів Windows Server 2012 використовуються й інші продукти для резервного копіювання, рекомендується вибрати варіант **VSS copy backup**. Якщо такого ні, можна сміло вибирати варіант **VSS full backup**.

У наступнім вікні майстра буде запитане підтвердження й, якщо воно отримане, запуститься резервне копіювання.

У результаті, у нашім прикладі на диску F: з'явиться каталог **Windowsimagebackup**, у ньому буде створений підкаталог, названий за іменем сервера з якого проходить архівування, куди й потрапить копія.

Рис. 5. Вибір типу копіювання

1.2. Організація резервного копіювання за розкладом.

Для цього в **Windows Server Backup** виберемо опцію **Backup Schedule**. Перше вікно майстра, що запустився, інформує, що перш ніж установлювати резервне копіювання за розкладом, потрібно визначити:

- що буде копіюватися (повне резервне копіювання сервера або окремі диски);
- як часто треба проводити копіювання;
- де розміщати копії.

При цьому треба враховувати:

1. навіть при виборі резервного копіювання окремих розділів, у їхній список обов'язково повинен бути внесений розділ (-и) з операційною системою;
2. копіювання може виконуватися один або кілька разів у день;
3. для зберігання результатів резервного копіювання повинен виділятися окремий диск, внутрішній або зовнішній (наприклад, що підключається за USB). Перед початком використання, він буде відформатований майстром архівації. Рекомендується, щоб він був не менш ніж в 1,5 рази більше за обсягом за архівуємі диски.

Нехай потрібно щодня робити резервне копіювання диска з ОС. У вікні майстра аналогічному рис. 3, вибираємо варіант Custom, у вікні аналогічному рис. 4 – диск С (на якім розташована операційна система). Указуємо розклад (рис. 6).

Далі визначається диск (рис. 7), він може бути не відформатований. Диску буде призначене «ім'я» схоже з назвою сервера й датою визначення резервного копіювання, після чого буде проведено форматування.. Диску не призначається буква й він не буде доступний користувачам як звичайний диск.

Коли робота з налаштування автоматичної архівації завершена, можна зробити додаткові налагодження, що підвищують швидкодію для окремих дисків. Для цього в

списку **Actions** в оснащенні **Windows Server Backup** виберіть пункт **Configure Performance Settings**. У вікні, що відкрилося (рис. 8) можна встановити, який тип резервного копіювання робити для диска – повне (**full**) або додаткове (**Incremental**). За замовчуванням використовується повне. Додаткове поміщає в архів тільки змінені з моменту останнього архівування файли, це дозволяє провести копіювання швидше, але більш суттєво знижує продуктивність сервера в період копіювання (тому що треба проводити перевірку).

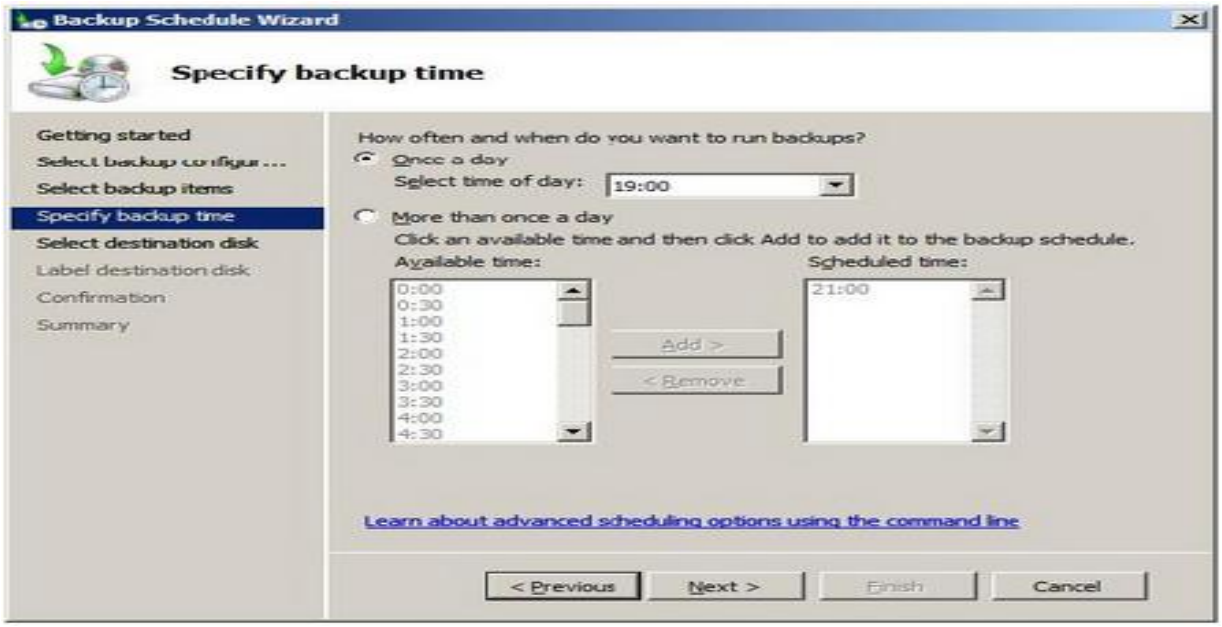


Рис. 6. Розклад резервного копіювання

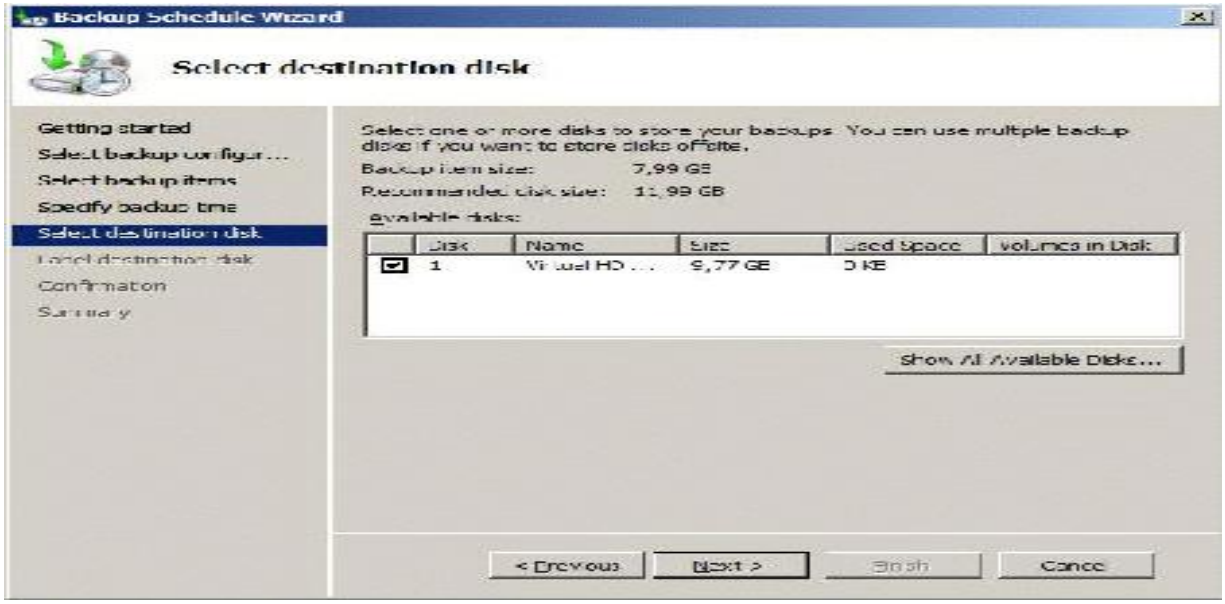


Рис. 7. Диск для зберігання резервних копій

Порядок відновлення такий же, як і при однократнім копіюванні.

До речі, подивитися параметри запланованого резервного копіювання можна за допомогою оснащення **Task Scheduler** (рис. 9).

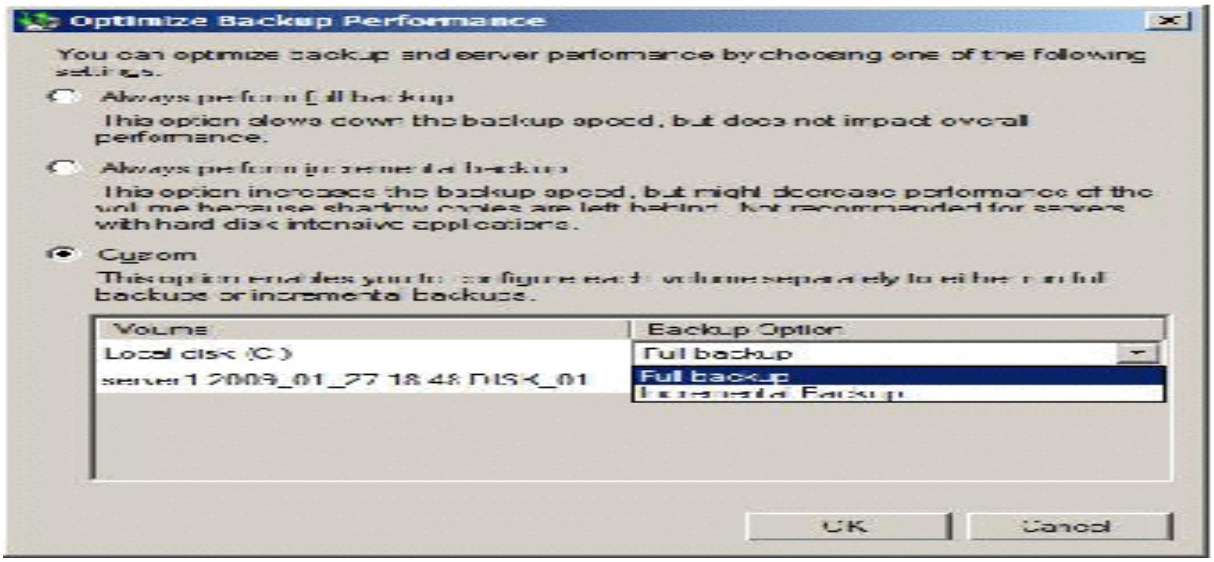


Рис. 8. Вибір типу резервного копіювання для диска

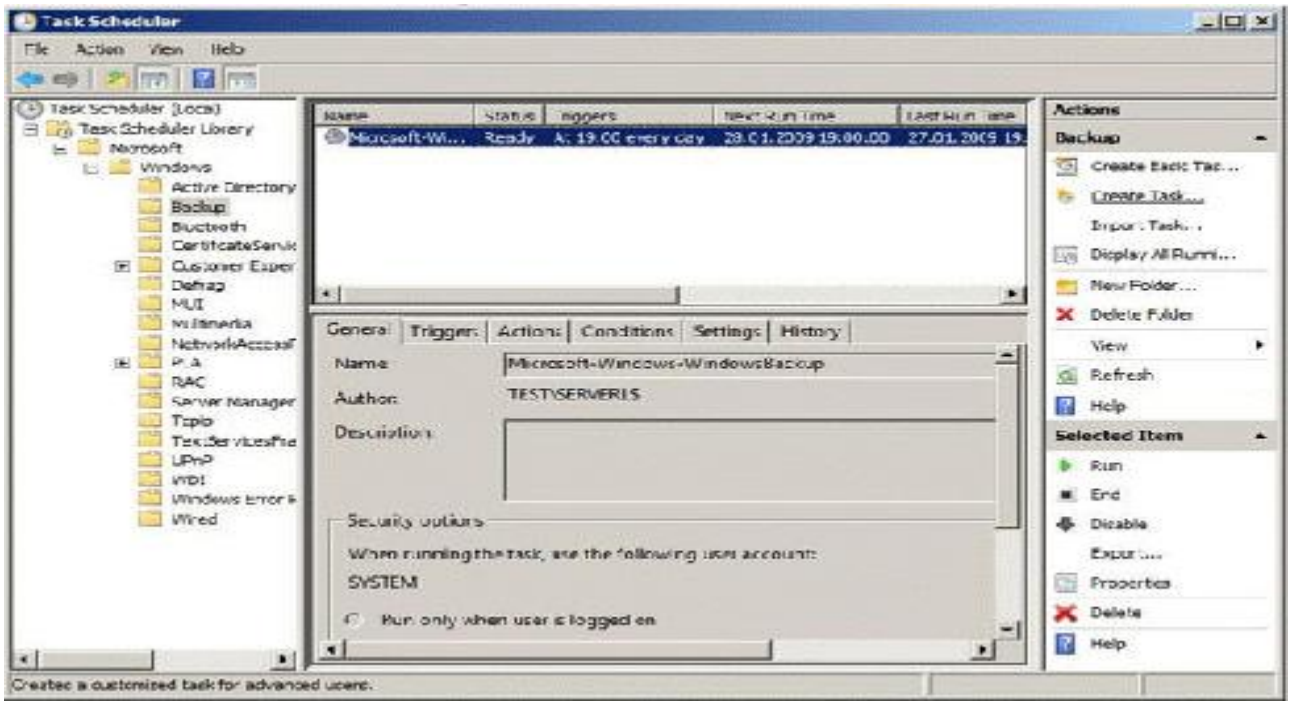


Рис. 9. Параметри створеного завдання

1.3. Відновлення даних

Тепер розглянемо порядок відновлення даних з резервної копії.

У першій частині лабораторної роботи була зроблена резервна копія розділу E:. Нехай знадобилося відновити вміст однієї з папок із вказаного розділу. При цьому потрібно зрівняти поточний уміст папки з архівною копією, тобто відновлювати потрібно в іншу папку.

Запускаємо оснащення **Windows Server Backup** і в списку **Actions** вибираємо **Recover** (відновлення). Майстер відновлення уточнює, який сервер буде відновлюватися, після чого представить перелік наявних резервних копій (рис. 10).

У наступнім вікні запитується, що саме відновлюється. Нас цікавить окрема папка, тому вибираємо варіант **Files and folders** (рис. 11). Інші варіанти відновлення зареєстрованих додатків і відновлення диска цілком.

У наступному вікні майстра в випадаючому меню можливо знайти й виділити обрану для відновлення папку. Якщо відновити потрібно кілька об'єктів, їх виділяють спільно, утримуючи клавішу **Ctrl** (або **Shift** для виділення діапазону). Після цього вибирається шлях для відновлення й задаються параметри. У нашім прикладі, ми прагнемо відновити обрану папку з файлами в знову створену папку **restored** (рис. 12).

Крім шляху (вихідний або альтернативний), вибирається варіант дій при збігу імен файлів і папок. Це особливо актуально, якщо відновлювати файли у вихідну папку. Варіантів три – створювати копії, перезаписувати наявні об'єкти відновлюваними, залишити наявні об'єкти.

Останній з обираних у цьому вікні параметрів указує на те, чи відновлювати налагодження безпеки (тобто списки доступу до файлів).

Після вибору всіх параметрів буде запитане підтвердження й почнеться відновлення.

2. Хід роботи

1. На навчальному сервері (або віртуальній машині) виберіть розділ для резервного копіювання.
2. З урахуванням розглянутих обмежень і обсягу розділу, який буде копіюватися, виберіть місце для розміщення копії. Визначите, від імені якого облікового запису буде проводитися ця операція.
3. Виконайте однократне резервне копіювання обраного розділу.
4. Виберіть із архіву, створеного в попередній частині роботи, групу файлів для відновлення. Відновіть їх у перший раз за вихідним шляхом зі збереженням копій, у другий раз – за альтернативним шляхом.
5. Розробіть і реалізуйте план щоденного резервного копіювання диска з операційною системою.
6. Використовуючи опцію **Backup Schedule** оснащення **Windows Server Backup**, вилучіть заплановане завдання на резервне копіювання.

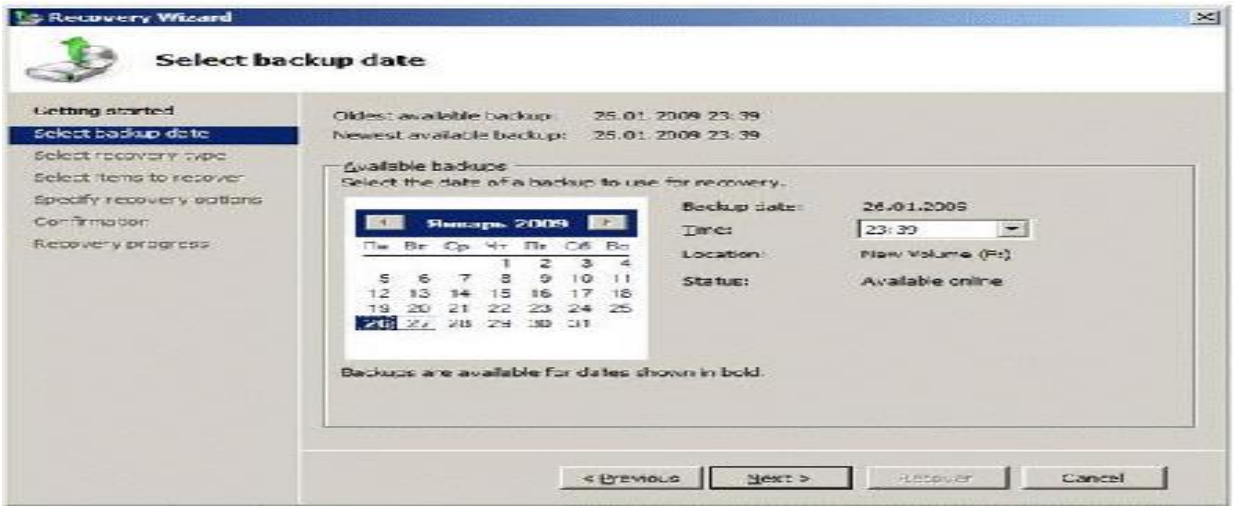


Рис. 10. Перелік доступних резервних копій для обраного сервера

Рис. 11. Вибір типу відновлення

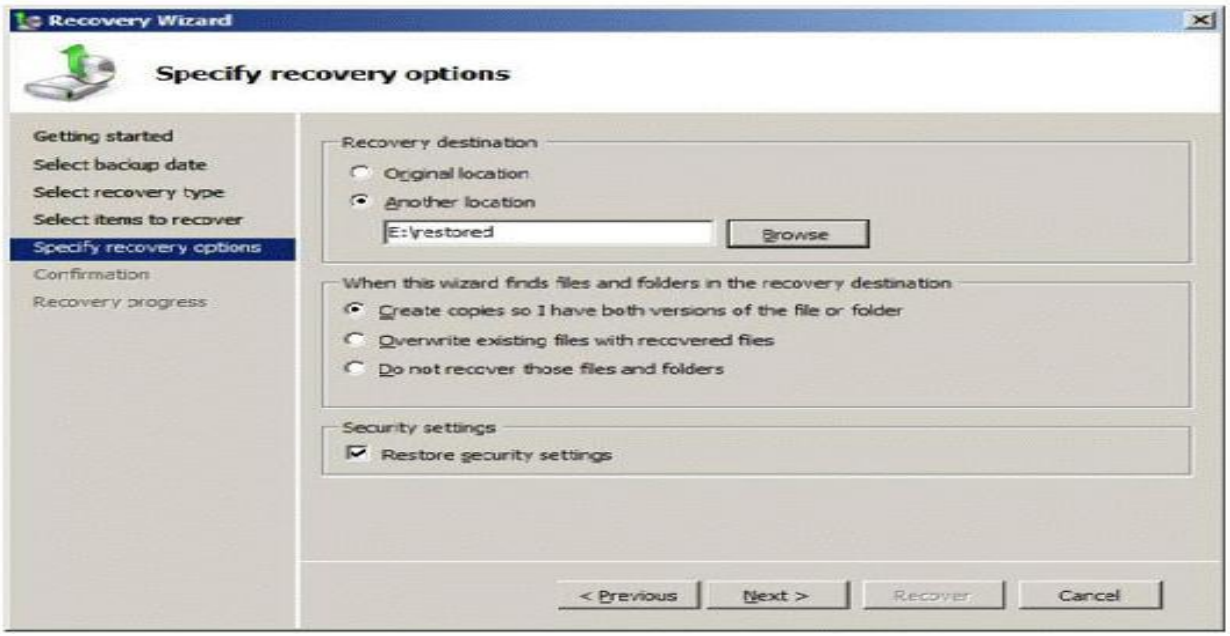


Рис. 12. Параметри відновлення

3. Контрольні питання

1 Який порядок виконання резервного копіювання?
2 Які особливості організації резервного копіювання за розкладом?
3 Який порядок відновлення даних?

ЛАБОРАТОРНА РОБОТА 17. УСТАНОВКА НОВОГО ЯДРА LINUX

Мета роботи: навчитись установлювати нове ядро Linux.

Зміст

1. Теорія
1.1. Вступ
1.2. Загальні відомості
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Вступ

Лабораторне завдання виконується в локальній мережі на робочій станції з операційною системою Linux 7 або більш пізньою версією. У лабораторіях кафедри операційна система Linux працює на комп'ютерах під керуванням програмного пакета Vmware. Цей пакет дозволяє створювати так звані «віртуальні машини» – уявний комп'ютер, що не залежить від операційної системи (ОС) на даному комп'ютері Для запуску ОС Linux необхідно запустити Vmware на робочій станції, вибрати зі списку необхідну операційну систему й натиснути кнопку «Power ON». Після закінчення завантаження, для входу в систему необхідно використовувати ім'я користувача **root.**

1.2. Загальні відомості

Ядро Unix виступає як посередник між прикладною програмою й устаткуванням, установленим у комп'ютері. Спочатку ядро підготовляється до обслуговування/розподілу пам'яті комп'ютера для всіх запущених програм (процесів), і переконується, що всі вони чесно (або нечесно, якщо ви цього бажаєте) розділяють час процесора. У додавання до цього ядро забезпечує інтерфейс для спілкування програм з устаткуванням.

Звичайно, ядро виконує більше функцій, але ці основні функції необхідно знати. Більш нові версії Unix у загальному підтримують більшу кількість типів устаткування (вони мають більше драйверів пристроїв), вони можуть мати поліпшене керування процесами, вони можуть виконуватися швидше, ніж більш старі версії, вони можуть бути більш стабільними. Більшість адміністраторів обновляють ядро, для того щоб можна було використовувати нові драйвери пристроїв і виправити помилки.

модуль, що завантажується, – це фрагмент коду ядра, який не включений прямо в ядро. модулі, що завантажуються, компілюються окремо й потім можуть вставлятися у запущенім ядрі. Багато популярних драйверів пристроїв, таких як драйвера PCMCIA, є модулями, що завантажуються.

Одержання вихідних текстів

Вихідні тексти ядра можна одержати за допомогою анонімного *ftp* з *ftp.funet.fi* у директорії */pub/Linux/PEOPLE/Linus*, з його "дзеркала", або з іншого сервера. Вони звичайно позначені як *linux-x.y.z.tar.gz,* де *x.y.z* номер версії (рис. 1). Більш нові (кращі?) версії й «заплатки» (*patches*) звичайно перебувають у піддиректоріях, таких як *`v1.1'* і *`v1.2'*. Найбільший номер має остання версія й звичайно є *`` тестовою версією''*.

Нижче наведений короткий список серверів і серверів-дзеркал:

USA: sunsite.unc.edu:/pub/Linux/kernel
USA: tsx-11.mit.edu:/pub/linux/sources/system
UK: sunsite.doc.ic.ac.uk:/pub/unix/Linux/sunsite.unc-mirror/kernel
Austria: ftp.univie.ac.at:/systems/linux/sunsite/kernel
Germany: ftp.Germany.EU.net:/pub/os/Linux/Local.Eunet/Kernel/Linus
Germany: sunsite.informatik.rwth-aachen.de:/pub/Linux/PEOPLE/Linus
France: ftp.ibp.fr:/pub/linux/sources/system/patches
Australia: sunsite.anu.edu.au:/pub/linux/kernel

Загальну інформацію про Linux і його дистрибутиви, можна подивитися на http://www.linux.org.

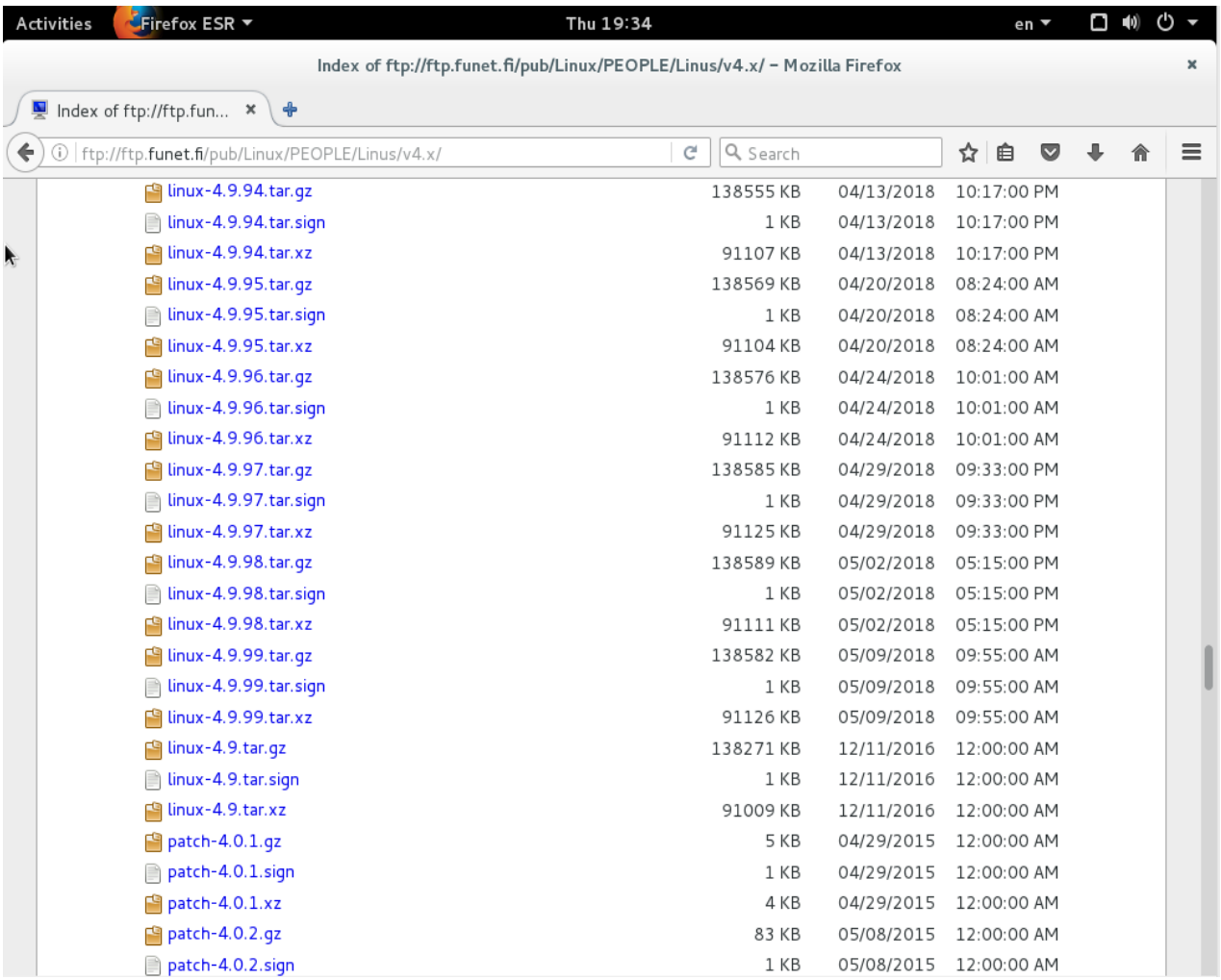


Рис. 1. Вихідні тексти ядра

Розпакування вихідних текстів

Увійдіть у систему як адміністратор або виконаєте команду *su*, і перейдіть у директорію */usr/src*. Якщо ви встановлювали вихідні тексти ядра при установці linux (як робить більшість), то там у вас уже є директорія названа *linux*, яка містить повне дерево застарілих вихідних текстів. Якщо у вас є вільний дисковий простір, то ви можете зберегти цю директорію. Необхідно визначити, яка версія ядра запущена й, відповідно перейменувати директорію. Команда *`uname -r'* видає номер поточної версії ядра. Тому, якщо команда *`uname -r'* видала *`1.0.9'*, те ви повинні перейменувати (за допомогою *`mv'*) *`linux'* в *`linux-1.0.9'*. Можна просто вилучити всю директорію. У кожному разі переконайтеся, що директорії *`linux'* в */usr/src* до розпакування повного вихідного коду ядра немає.

Тепер розпакуйте в */usr/src* вихідні тексти, користуючись командою *`tar zxpvf linux-x.y.z.tar.gz'* (рис. 2) (якщо ви одержали просто файл.*tar* без розширення *.gz* на кінці, то працює команда *`tar xpvf linux-x.y.z.tar'*). Уміст архіву буде розпакований. У процесі розпакування буде відкрита нова директорія *`linux'* в */usr/src*. Перейдіть у директорію *'linux'* і прочитайте файл README (рис.3). Там буде розділ із заголовком *`INSTALLING the kernel (Установка ядра)'*. Виконайте відповідні інструкції (символічні посилання повинні бути на своєму місці), видаліть старі **.o* файли й т.п.

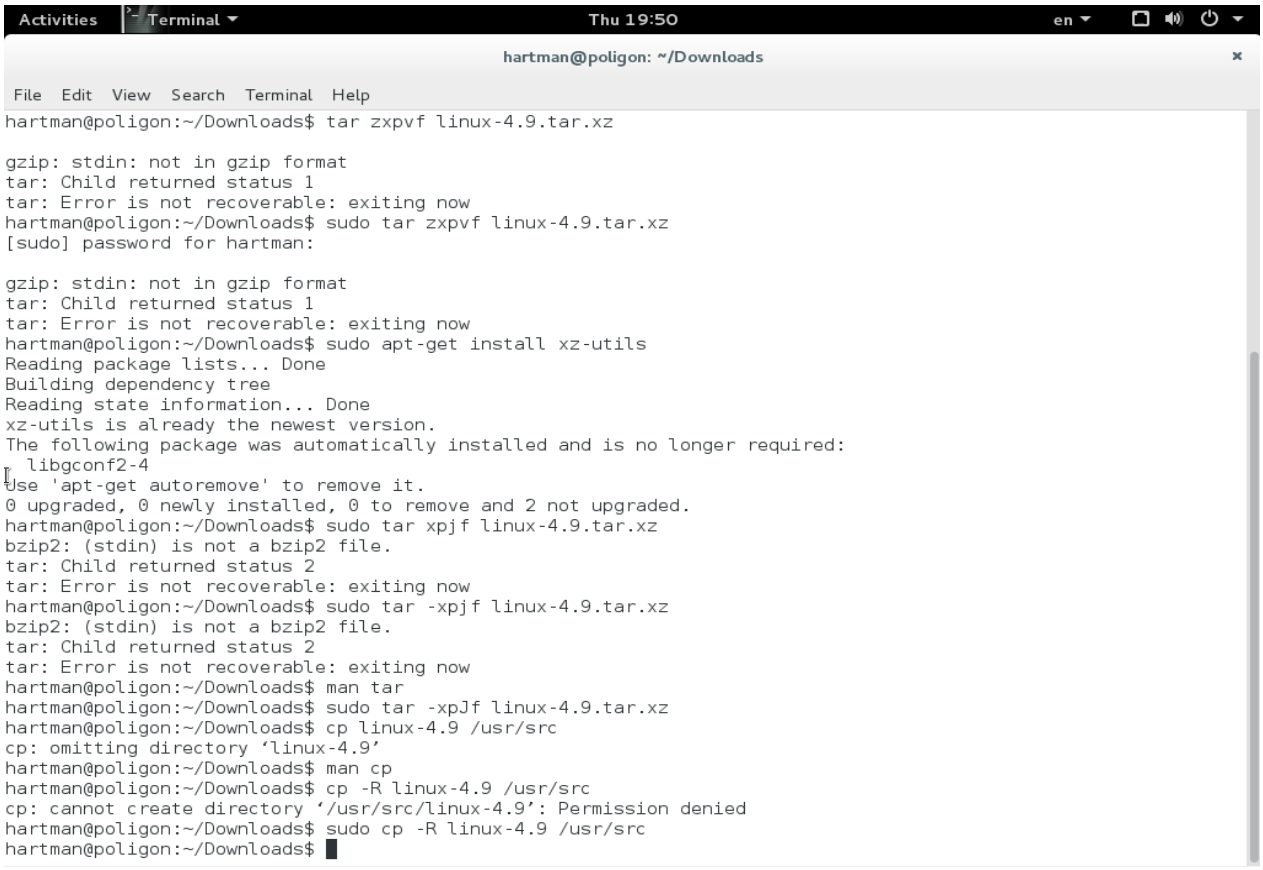


Рис. 2. Розпакування архіву

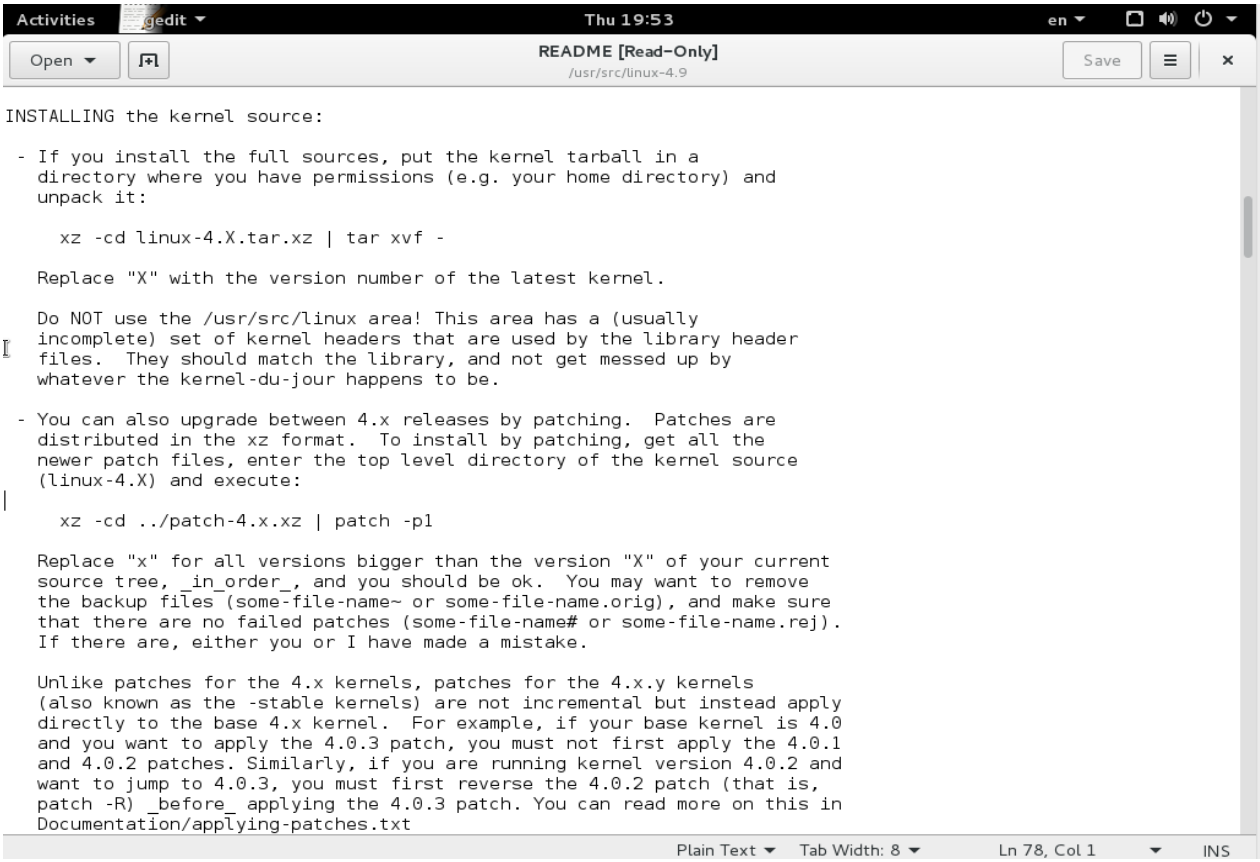


Рис. 3. Вміст файлу README

Налаштування ядра

Команда `*make config'* виконана в */usr/src/linux* запускає скрипт налагодження (рис. 4), який задасть вам багато питань. Скрипт вимагає наявності *bash*, так що перевірте, щоб *bash* перебував у директорії */bin/bash*, */bin/sh*, або *$BASH*.

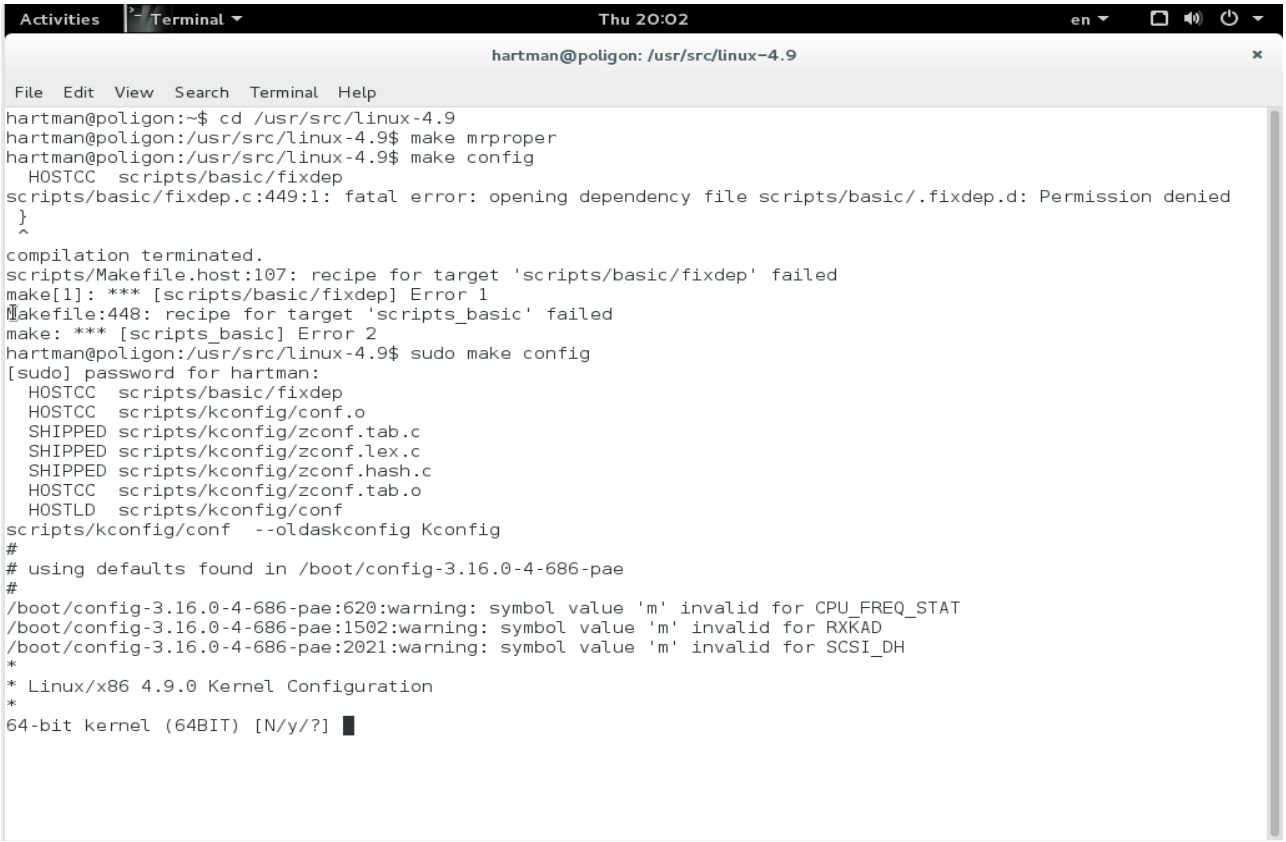


Рис. 4. Запуск скрипту налагодження

Існують деякі альтернативи команді `*make config'* і ви можете знайти їх більш зручними й легкими для використання. Ті, хто працює в *X*, можуть спробувати `*make xconfig'*. Якщо у вас установлений *Tk (`click-o-rama')* можете спробувати *Nat*. Якщо встановлений *(n)curses* і ви віддаєте перевагу текстовим меню - `*make menuconfig'*. Ці інтерфейси мають одна явну перевагу: якщо ви зробили неправильний вибір протягом налагодження, то дуже легко повернутися й виправити її.

Тепер ви готові відповідати на запитання, відповіді на які звичайно виглядають як `*y*' (так) або `*n*' (немає) (рис. 5). Драйвери пристроїв звичайно мають опцію `*m*'. Це означає ``*module (модуль)*'' і система буде компілювати цей драйвер, але не вставить його прямо в ядро, а зробить модулем, що завантажується. Деякі більш ясні й некритичні опції тут не описані.

У версіях 2.0.x і більш пізніх, існує опція `?', яка забезпечує короткий опис параметра налагодження.

Нижче описуються питання, що задаються скриптом і можливі відповіді на них. У більшості випадків питання задаються англійською мовою.

Емуляція ядром математичних функцій

Якщо у вас немає математичного співпроцесора, то ви повинні відповісти `*y*'. Якщо у вас є співпроцесор і ви однаково відповіли `*y*', то не турбуйтеся – співпроцесор усе рівно буде використовуватися, а емуляція буде зігнорована. Єдиний наслідок такої відповіді в тому, що ядро буде більш використовувати ОЗУ.

Підтримка звичайних (MFM/RLL) дисків і дисків /cdrom IDE

Вам імовірно необхідна така підтримка. Це означає, що ядро буде підтримувати стандартні жорсткі диски PC, які є в більшості комп'ютерів. Цей драйвер не включає підтримку SCSI дисків – їх вибір іде далі в налагодженні.

Потім у вас запитають про драйвери ``*old disk-only (тільки старих дисків)*" і "*new IDE (нових IDE)*". Вам необхідно вибрати один з них. Основна відмінність полягає в тому, що старі стандарти підтримували тільки два диски на одному інтерфейсі, а нові підтримують вторинний (*secondary*) інтерфейс і накопичувачі *IDE/ATAPI cdrom*. Новий драйвер на 4 Кб більше старого й також ``поліпшений", він може поліпшити продуктивність вашого диска, особливо якщо у вас нове обладнання (типу EIDE).

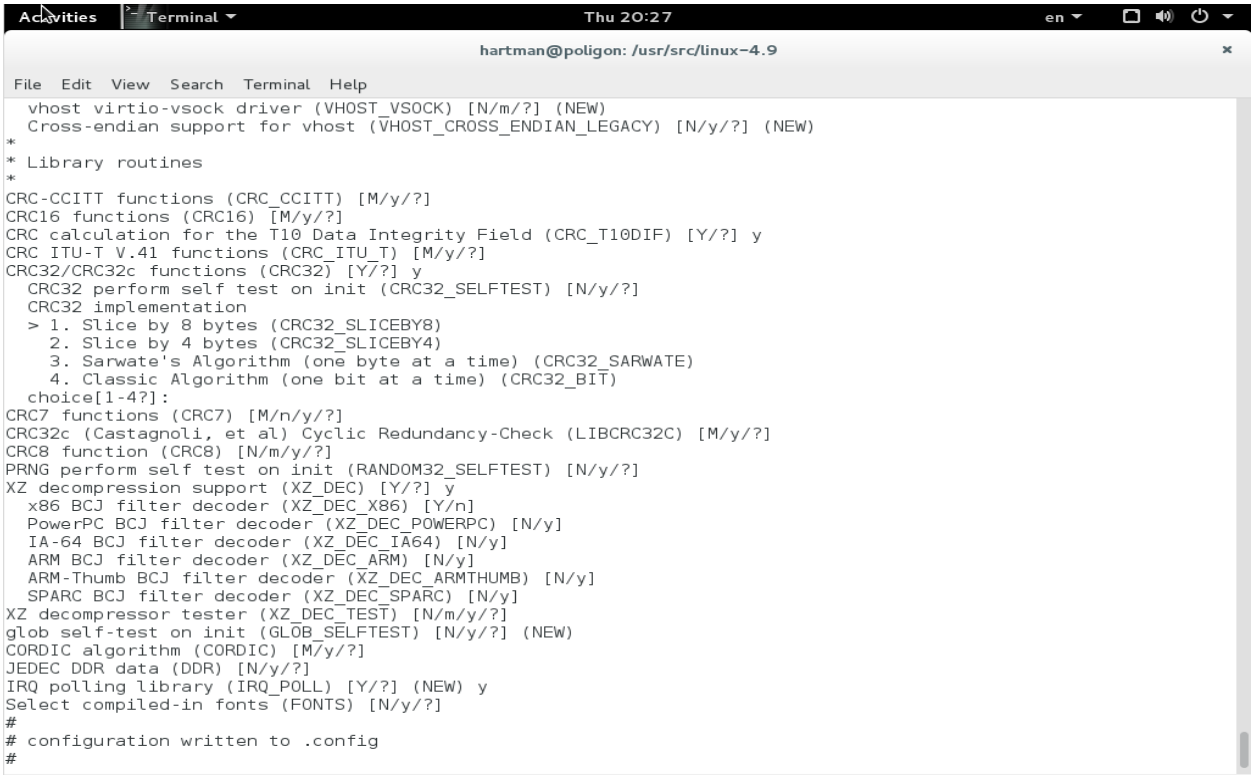


Рис. 5. Відповіді на запитання

Підтримка мережі

У принципі ви повинні відповісти `*y*', якщо ваша машина підключена до мережі, такої як *internet*, або ви прагнете використовувати *SLIP*, *PPP*, *term* і т.п. для *dial up* доступу до *internet*. Однак багато пакетів (таких як віконна система *X*) вимагає підтримку мережі, навіть якщо ви не підключені ні до якої мережі, тому ви повинні відповісти `*y*'. На запитання чи встановлювати підтримку TCP/IP необхідно відповісти `*y*'.

System V IPC

IPC (*Interprocess Communication, Міжпроцесорні Повідомлення*) використовується Perl-*Програмами* для того, щоб дозволити одному процесу спілкуватися з іншими процесами. На це питання можна відповісти `*y*'.

Тип процесора (386, 486, Pentium, Ppro)

Правильний вибір типу процесора оптимізує скомпільоване ядро системи з погляду підвищення його продуктивності. Ви повинні вказати процесор, для якого ви компілюєте ядро. Ядро для ``*386*" буде працювати на всіх машинах.

Підтримка SCSI

Якщо у вас є пристрою SCSI, то відповідайте `*y*'. Можливо знадобиться введення додаткової інформації, такої як підтримка CD-ROM, дисків, і типу наявного адаптера SCSI.

Підтримка мережевих пристроїв

Якщо у вас є мережева карта, або ви прагнете використовувати *SLIP*, *PPP*, або адаптер паралельного порту для підключення до *Internet*, то відповідайте `*y*'. Скрипт налагодження запросить у вас тип карти й типи протоколів.

Файлові системи

Потім налагоджувальний скрипт запросить у вас інформацію про підтримку файлових систем, установлюваних у вашій системі. Підтримуються наступні системи:

стандартна (*minix*). Більш нові дистрибутиви не створюють файлові системи *minix*. Деякі програми з "*дисками для відновлення (rescue disk)*" використовують цю систему, крім того деякі гнучкі диски можуть її використовувати.

extended fs – це перша версія розширеної файлової системи, яка зараз широко не використовується.

Second extended – ця файлова система широко використовується в нових дистрибутивах. Швидше за все саме цю систему вам потрібно зупиняти.

xiafs – файлова система дуже рідко використовувана.

msdos – якщо ви прагнете використовувати розділи вашого жорсткого диска з MS-DOS, або монтувати гнучкі диски, відформатовані під MS-DOS, те відповідайте `*y*'.

umsdos – ця файлова система розширює можливості файлової системи MS-DOS звичайними Unix-Подібними можливостями, такими як довгі імена.

proc – ця система не створює файлову систему *proc* на диску - вона є інтерфейсом у вигляді файлової системи до ядра й процесів. Багато програм, що видають список процесів (таких як `*ps*'), використовують її. Спробуйте виконати `*cat /proc/meminfo'* або `*cat /proc/devices'*. Деякі командні процесори ( зокрема *rc*) *використовують /proc/self/fd* (відомий як */dev/fd* в інших системах) для введення/виводу. Ви повинні майже завжди відповісти `*y*' на це питання тому що багато важливих утиліт для Linux залежать від цього вибору.

NFS – якщо ваша машина працює в мережі й ви прагнете використовувати файлові системи, що перебувають на інших машинах за допомогою NFS, те відповідайте `*y*'.

ISO9660 – є на більшості CD-ROM. Якщо у вас є привод CD-ROM і ви прагнете використовувати його в Linux, то відповідайте `*y*'.

OS/2 HPFS – працює як файлова система тільки для читання в OS/2 HPFS.

System V і Coherent – для розділів машин з System V і Coherent (це інші варіанти Unix для PC).

Символьні пристрої

Вибір драйверів для вашого принтера (паралельного принтера), шинної миші, миші для PS/2 (багато *notebook* використовують протокол миші PS/2 для своїх вбудованих трекболів), деякі стрічкові накопичувачі й інші такі ж ``символьні" пристрою. Відповідайте `*y'* де необхідно.

Зауваження 1: *Selection* це програма, яка дозволяє вам використовувати мишу поза системою *X-Window* для вирізання й вставки між віртуальними консолями. Вона працює досить добре, якщо у вас миша для послідовного порту, тому що вона добре працює з *X*, але вам необхідно виконати деякі дії, для того щоб працювали інші типи мишей. Підтримка *Selection* деякий час була опцією налагодження, але зараз вона є стандартом.

Зауваження 2: Зараз *Selection* уважається застарілою. Ім'я нової програми ``*gpm*". Вона може робити трансляцію протоколу миші, працювати з декількома мишами й ін.

Звукові карти

Якщо у вас установлена звукова карта, то відповідайте `*y*'. Далі інша програма налагодження буде скомпільована й буде задавати вам питання про вашу звукову карту. (*Примітка про налагодження звукової карти*: коли програма запитає у вас чи встановлювати повну версію драйвера, то відповідайте `*n*' і збережете деяку кількість пам'яті в ядрі вибором тільки необхідних можливостей драйвера).

Інші опції налагодження

Не всі опції налагодження перераховані тут, тому що вони занадто часто міняються або є очевидними (наприклад, підтримка *3Com 3C509* для компіляції драйвера для даної карти *ethernet*). Існує досить повний список усіх опцій (плюс спосіб помістити їх у скрипт *Configure*), який зібраний Axel Boldt (axel@uni-paderborn.de) за наступною адресою:

http://math-www.uni-paderborn.de/~axel/config_help.html

або через анонімний FTP за адресою:

ftp://sunsite.unc.edu/pub/Linux/kernel/config/krnl_cnfg_hlp.x.yz.tgz

де: x.yz – номер версії.

Для останніх версій (2.0.x і більш пізніх), цей список був інтегрований у дерево вихідних текстів.

Робота над ядром (Kernel hacking)

Дія опції налагодження ``*kernel hacking*'' звичайно проявляється в більш великому й/або повільнім ядрі й може навіть зробити ядро менш стабільним через налагодження деяких підпрограм на аналіз некоректних ситуацій у системнім ядрі *(kmalloc()).* Таким чином, вам швидше за все треба відповісти `*n*' на це питання для ``*production*'' ядер.

Компіляція ядра

Очищення й створення залежностей

Коли налагоджувальний скрипт закінчить свою роботу, він також повідомить вас, що необхідно виконати `*make dep*' і (імовірно) `*clean*' (рис.6). Тому виконаєте `*make dep*'. Він забезпечить, щоб усі залежності, такі як файли заголовків, перебували на місці. Ця процедура не триває довго, якщо у вас не повільний комп'ютер. Для більш старих версій ядер, при закінченні ви повинні виконати `*make clean*'. Ця процедура видаляє всі об'єктні файли й деякі інші компоненти, що залишилися від попередньої компіляції. *У кожному разі, не забувайте виконати цей крок до початку перекомпіляції ядра.*

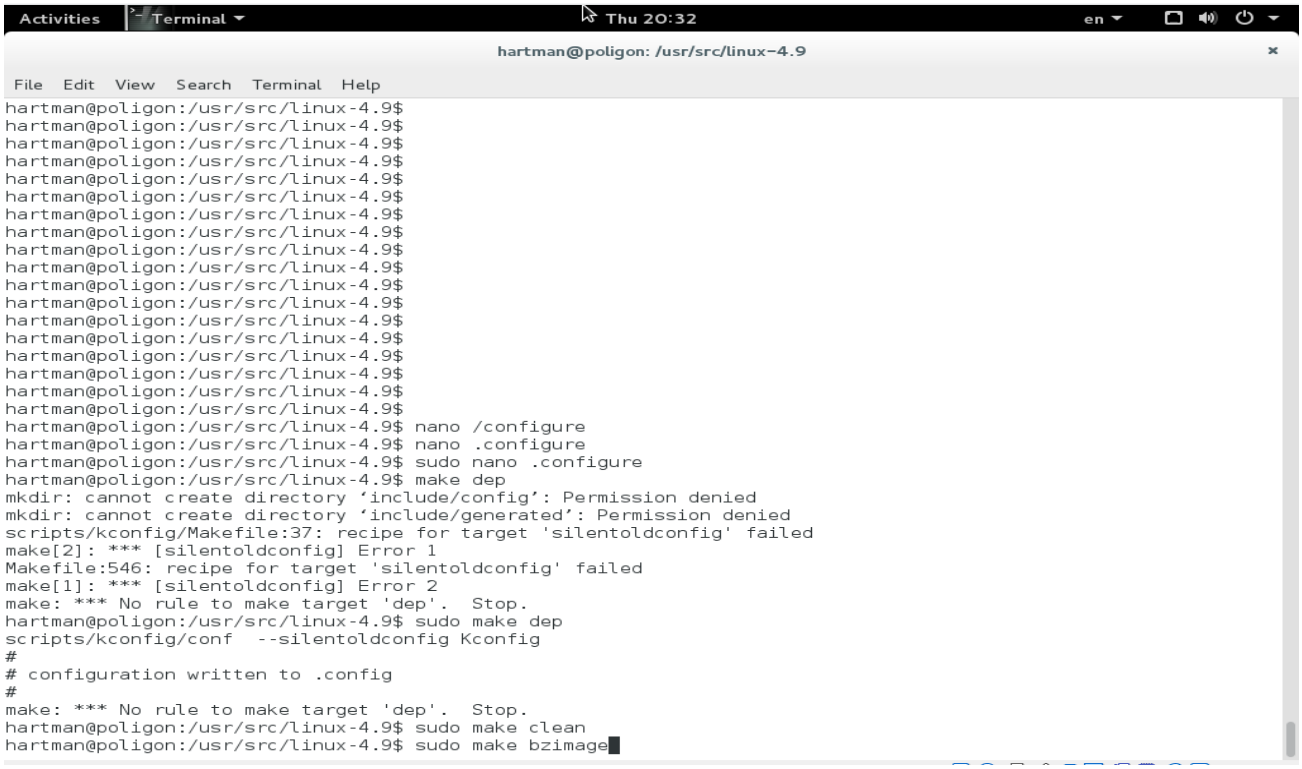


Рис. 6. Налагоджувальний скрипт

Процес компіляції

Після виконання *dep* і *clean*, ви можете виконувати `*make bzimage*' або `*make zdisk*' (ця частина процесу забирає тривалий час). `*make bzimage*' скомпілює ядро й залишить у директорії *arch/i386/boot* файл, з іменем `*zimage*'. Це нове стисле ядро. `*make zdisk*' робить теж

саме, але додатково поміщає новий файл *zimage* на гнучкий диск, який ви повинні вставити в пристрій ``*A:*''. `*zdisk*' є досить зручним для тестування нових ядер – якщо воно не завантажується (або просто працює неправильно), то просто витягніть дискету з дисководу й завантажтеся зі старим ядром. Це може бути також зручним у тому випадку, якщо ви випадково вилучили ядро (або зробили що-небудь подібне за свожю руйнівною дією). Ви також можете використовувати його для установки нових систем, у тому випадку, коли ви просто робите дамп із одного диска на іншій.

Усі, навіть порівняно недавні ядра є стислими, тому вони мають букву `*z*' на початку імені. Стисле ядро автоматично розтискається при виконанні.

Команда ``make'' (рис. 7).

`*make mrproper*' виконає більш інтенсивне очищення дерева вихідних текстів. Іноді вона є необхідною. Ви можете виконувати цю команду після кожного накладення заплаток. `*make mrproper*' також вилучить ваші файли конфігурації, так що ви можете захотіти зберегти резервну копію вашого файлу (*.config*), якщо ви вважаєте його потрібним.

`*make oldconfig*' спробує налагодити ваше ядро, використовуючи старий файл налагодження - він проробить шлях в процесі конфігурації `*make config*' замість вас. Якщо у вас немає скомпільованого ядра або у вас немає старого файлу налагодження, то вам швидше за все не треба робити цієї операції, оскільки ви ймовірно захочете змінити налагодження за замовчуванням.

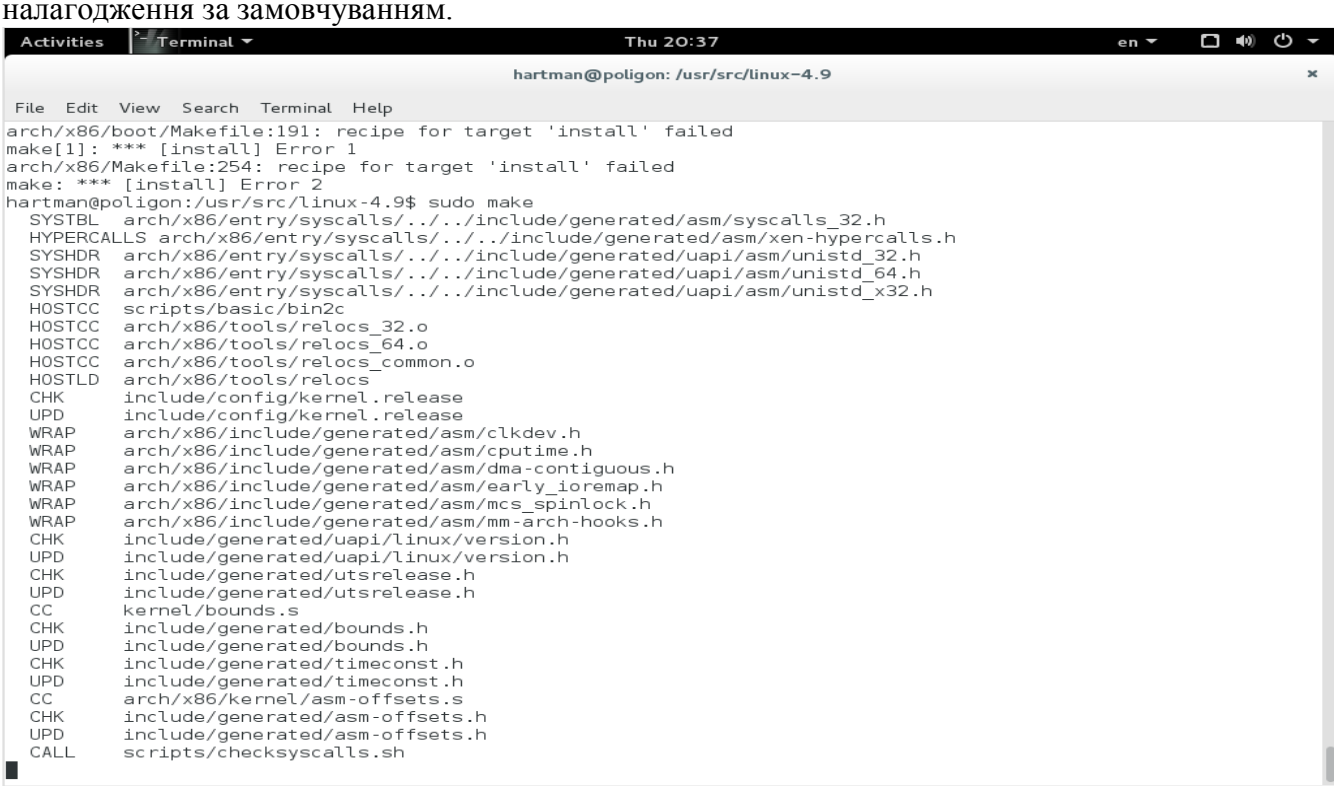


Рис. 7. Команда ``make''

Дивіться розділ про модулі для опису операції `*make modules*' (рис. 8).

Установка ядра

Після того як ви встановили, що нове ядро працює так як що вам треба, наступає час його установки. У більшості випадків для цього використовується LILO (завантажник Linux). Команда `*make install*' (рис. 9) установить нове ядро, запустить для нього LILO, і все буде готове до перезавантаження, ***але тільки*** якщо LILO налагоджене правильно у вашій системі: ядро розташовується у файлі */vmlinuz*, LILO перебуває в директорії */sbin*, і ваш конфігураційний файл LILO (*/etc/lilo.conf*) відбиває ці умови. Інакше вам доведеться використовувати LILO безпосередньо. Це досить легкий в установці й у роботі пакет, але він має тенденцію вводити в замішання своїм конфігураційним файлом. Подивитеся

конфігураційний файл (або */etc/lilo/config* для старих версій або */etc/lilo.conf* для більш нових версій), і подивитеся поточні налагодження. Конфігураційний файл виглядає приблизно так:

```
image = /vmlinuz
   label = Linux
   root = /dev/hda1
   ...
```

`image ='* указує на встановлене в цей час ядро. Часто використовується */vmlinuz*. *`label' використовується для визначення того, яке ядро або операційна система буде завантажуватися, і *`root'* – це кореневий розділ окремої операційної системи. Зробіть резервну копію вашого ядра й скопіюйте тільки що зроблене ядро на його місце (ви повинні виконати команду *`cp zimage /vmlinuz'* якщо ви використовуєте *`/vmlinuz'*). Потім запустите знову LILO – на більш нових системах ви можете просто запустити *`lilo'*.

Модулі

Модулі, що завантажуються, ядра можуть зберегти пам'ять і спростити налагодження. Область застосування модулів включає файлові системи, драйвери карт *ethernet*, драйвери стрічкових накопичувачів і т.п.

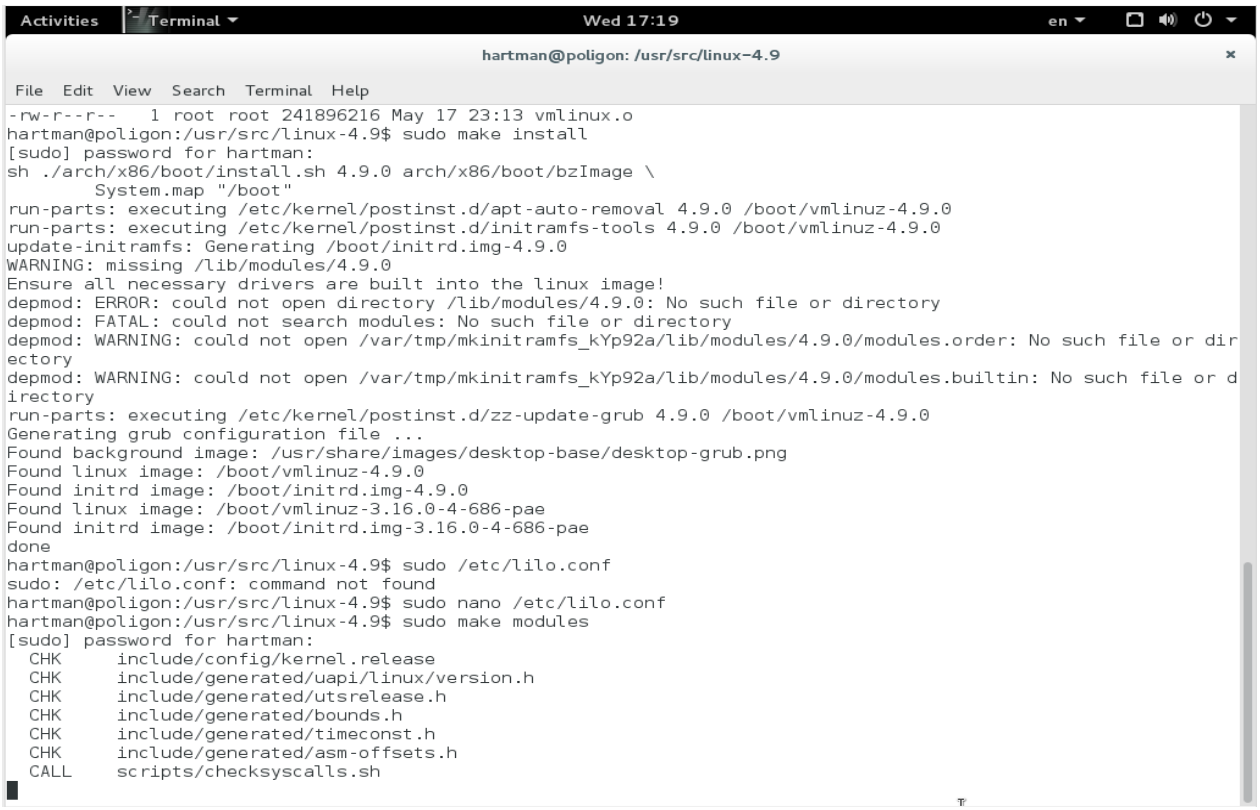


Рис. 8. Команда *`make modules'*

Установка утиліт для роботи з модулями

Утиліти для роботи з модулями перебувають там же, де було ядро. Вони називаються *modules-x.y.z.tar.gz*. Виберіть найбільший номер *x.y.z*, який рівний або нижче номеру вашого поточного ядра. Розпакуйте їх за допомогою команди *`tar zxvf modules-x.y.z.tar.gz'*, перейдіть у директорію, яку ця команда створила (*modules-x.y.z*), подивіться файл README, і виконайте наведені в ньому інструкції з установки (які звичайно є дуже простими, такими як *make install*). Ви повинні тепер одержати програми *insmod*, *rmmod*, *ksyms*, *lsmod*, *genksyms*, *modprobe* і *depmod* у директорії */sbin*. Якщо прагнете, протестуйте отримані програми за допомогою демонстраційного драйвера *``hw''* в *insmod*. Для більш детальної інформації дивіться файл INSTALL, який перебуває в директорії з вихідними текстами.

Команда *insmod* вставляє модуль у працююче ядро. Модулі звичайно мають розширення **.o*; приклад драйвера, згаданого вище називається *drv_hello.o*, так для того щоб вставити його, ви повинні виконати `*insmod drv_hello.o*'. Для того щоб побачити список завантажених модулів використовуйте команду *lsmod*. Її вивід виглядає приблизно так:

```
blah# lsmod
Module:      #pages:  Used by:
drv_hello       1
```

де: `*drv_hello'* – це ім'я модуля, він використовує 1 сторінку оперативної пам'яті (4 Кб), і ні які модулі ядра не залежать від нього на теперішній момент. Для видалення цього модуля використовуйте команду `*rmmod drv_hello'*. Помітимо, що *rmmod* вимагає *ім'я модуля,* а не ім'я *файлу*. Ви можете одержати його зі списку видаваного *lsmod*. Призначення інших утиліт для роботи з модулями описане в їхніх довідкових сторінках.

Модулі, розповсюджувані з ядром

У версії 2.0.30, майже всі модулі, доступні. Для їхнього використання спочатку переконайтеся, що ви не налагодили їх як «вкомпільованими» у ядро, тобто ви не відповіли '*y*' у процесі виконання `*make config'*. Скомпілюйте нове ядро й завантажитеся з ним. Потім знову перейдіть в */usr/src/linux*, і виконайте `*make modules'*. Це скомпілює всі модулі, які ви не вказали при налагодженні ядра, і помістить посилання на них в */usr/src/linux/modules*. Ви можете використовувати їх прямо із цієї директорії, або виконаєте команду `*make modules_install'*, яка встановить модулі в директорію */lib/modules/x.y.z*, де: *x.y.z* - це версія ядра.

Рис. 9. Команда `*make install'*

Це може бути особливо корисним у використанні файлових систем. Ви можете нечасто використовувати файлові системи *minix* або *msdos*. Наприклад, для операцій із гнучким диском з *msdos*, потрібно зробити *insmod /usr/src/linux/modules/msdos.o*, і потім – *rmmod msdos*, коли все закінчене. Ця процедура зберігає приблизно 50 Кб ОЗУ в ядрі протягом нормальної роботи. *Маленьке зауваження для використання файлової системи minix*: ви повинні ***завжди*** налагодити його прямо в ядро для використання в ``відбудовні (rescue)" дисках.

2. Хід роботи

У ході лабораторної роботи необхідно зробити установку й налагодження ядра 2.4.22, продемонструвати його працездатність.

Ядро перебуває на ftp://ais.khstu.ru/pub/kernel/

Скомпільоване ядро повинне забезпечувати роботу в мережі й підтримувати firewall, а також підтримку SCSI.

Зміст звіту

1. Список команд, що використовувалися при роботі.
2. Виводи за роботою.

3. Контрольні питання

1. Що таке модуль, що завантажується?
2. Яка послідовність установки нового ядра?
3. Як скомпілювати нове ядро?

ЛАБОРАТОРНА РОБОТА 18. ПОБУДОВА МЕРЕЖІ В ОС «LINUX»

Мета роботи: навчитися будувати мережу в ОС LINUX та розбивати на різні складові, виходити в зовнішню мережу, налагоджувати параметри захисту.

Зміст

1. Побудова мережі
1.1. Вивчення vlan.
I.2. Будуємо мережу між vm1, vm2 в одному vlan.
1.3. Розбиваємо vm1 vm2 на різні vlan. Набудовуємо intervlan routing за допомогою R1.
2. Хід роботи
3. Контрольні питання

1. Побудова мережі

Дано: локальна мережа (рис. 1), що складається з VM1,VM2. Роутер R1 (теж віртуальна машина), Web сервер S1. Скачати готову віртуальну програму (рис. 2) для цієї лабораторної роботи можна з Яндекс.

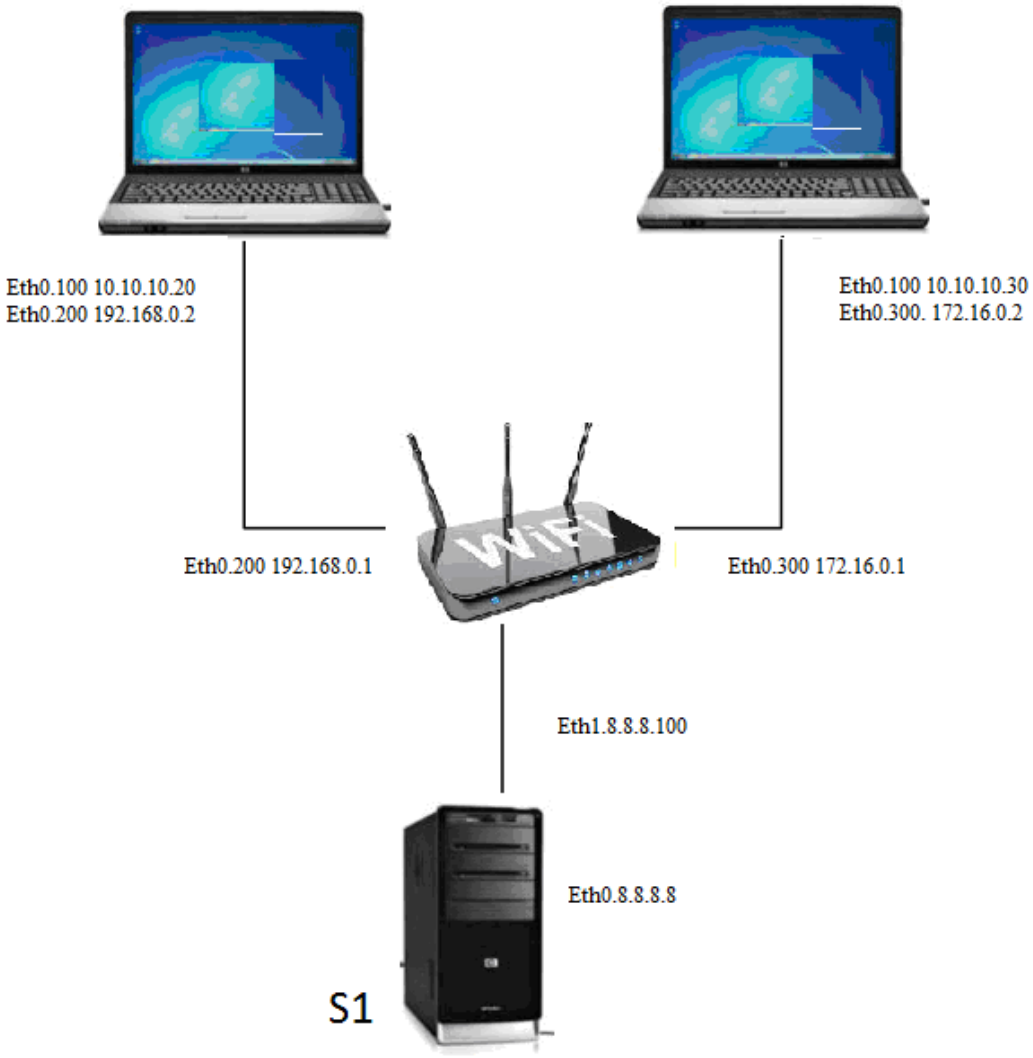


Рис. 1. Схема мережі

1.1. Вивчення vlan.

Розбиваємо vm1 vm2 на різні vlan.

Налагодження для VM1 – підключаємо як bridge до інтерфейсу. Інтерфейс можна вибрати будь-який і забриджувати усе на нього. Для повноти відповідності схемі зроблено у системі 2 bridge адаптера (br0,br1) (рис. 3) і підключено vm1,vm2,r1(адаптером 1) до br0, а s1,r1(адаптером 2) до br2.

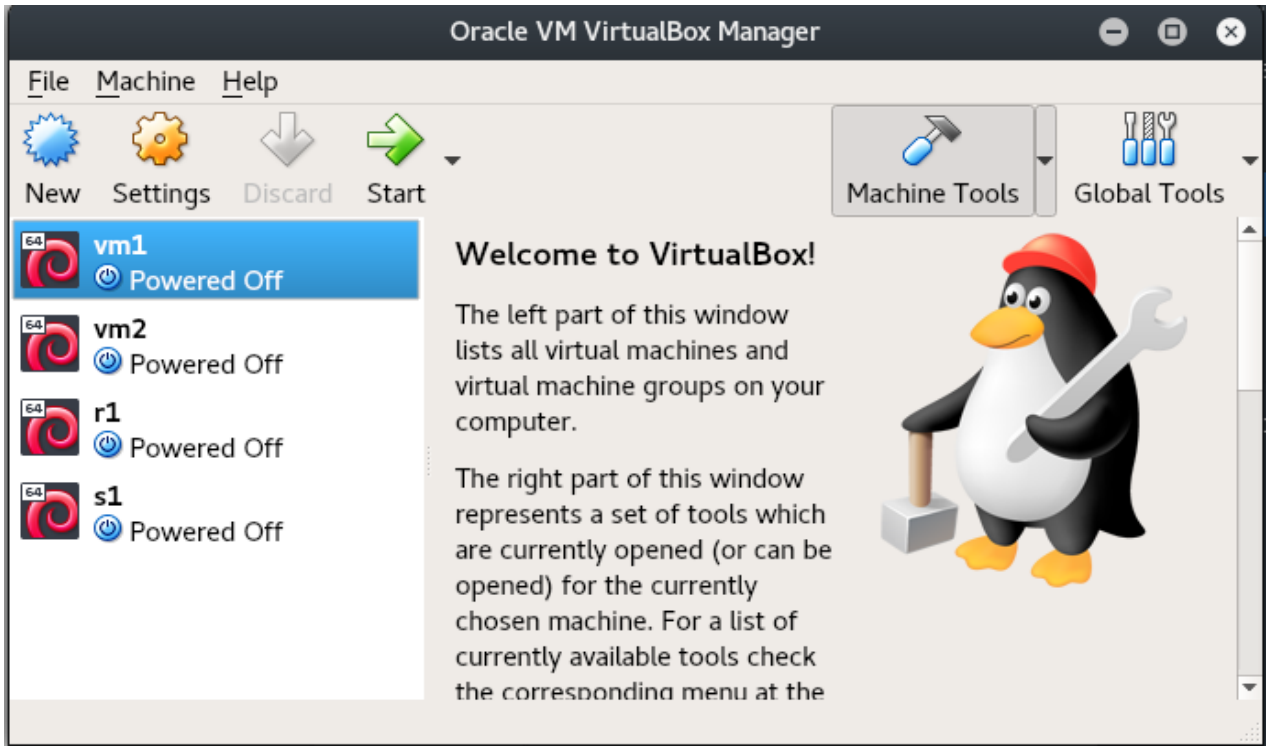


Рис. 2. Приклад віртуальних машин

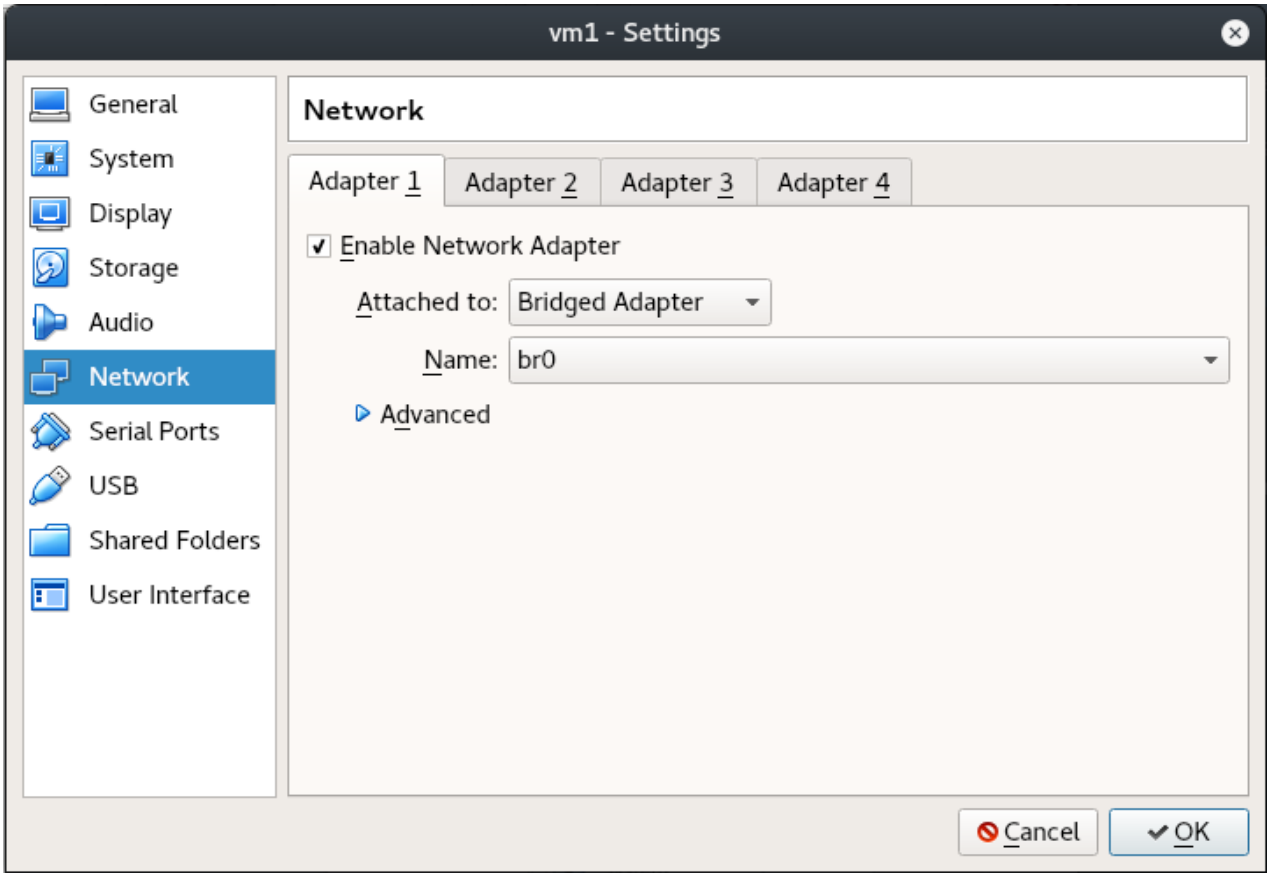


Рис. 3. Приклад налагодження адаптера

Для інших 3-х адаптерів налагодження аналогічні.

I.2. Будуємо мережу між vm1, vm2 в одному vlan.

Запускаємо vm1 і vm2 і дивимося інтерфейси в нашій системі командою ip addr (рис. 4), (скорочено ip a)

Додаємо новий пристрій, який буде називатися eth0.100 і являти собою тегований інтерфейс із id=100.

```
ip link add - добавити устрій
link eth0 - з'єднати з фізичним  адаптером eth0
name eth0.100 - ім'я устрою в списку.
type vlan - тип інтерфейса, що створюється. Він працює з
8021q - тип vlan
id 100 - власне сам id vlan
```

Тепер привласнимо цьому інтерфейсу ip адресу (рис. 5).

ip addr add 10.10.10.10/24 dev eth0.100

короткий вид запису:

ip a a 10.10.10.10/24 dev eth0.100 (рис. 6).

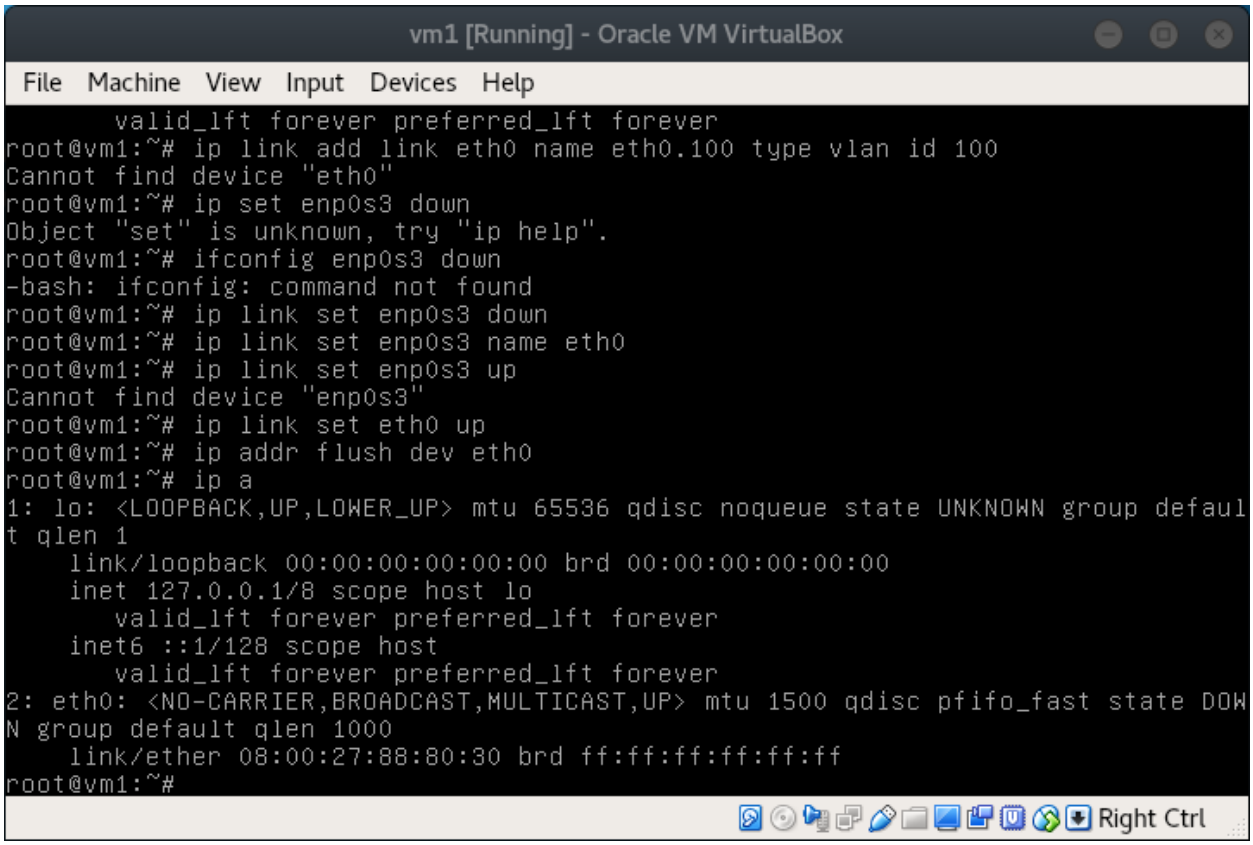


Рис. 4. Запуск vm1 і vm2 Перегляд налаштувань адаптерів

Звертаємо увагу на наступні речі: no-carrier і DOWN це значить що в нас до інтерфейсу не підключений мережевий кабель, а сам інтерфейс перебуває в DOWN.

Підключаємо кабель і одержуємо такі результати (рис. 7):

Виконаємо включення інтерфейсу командою (рис. 8):

ip link set dev eth0.100 up

У такий спосіб ми створили інтерфейс, який буде одержувати теговані пакети з vlan id = 100 і відповідно добавляти на пакети тег 100 при випуску пакета в мережу через цей інтерфейс. і призначили йому ip адресу 10.10.10.20/24 робимо те ж саме на VM2 (рис. 9), призначаємо адресу 10.10.10.30/34/

Перевіряємо з'єднання між VM1 і VM2: виконаємо ping 10.10.10.20 з VM2 (рис. 10).

Підіб'ємо підсумок: ми створили на двох машинах в одній локальній мережі 2 тегованих інтерфейси в 100-тому vlan-е й перевірили з'єднання між ними.

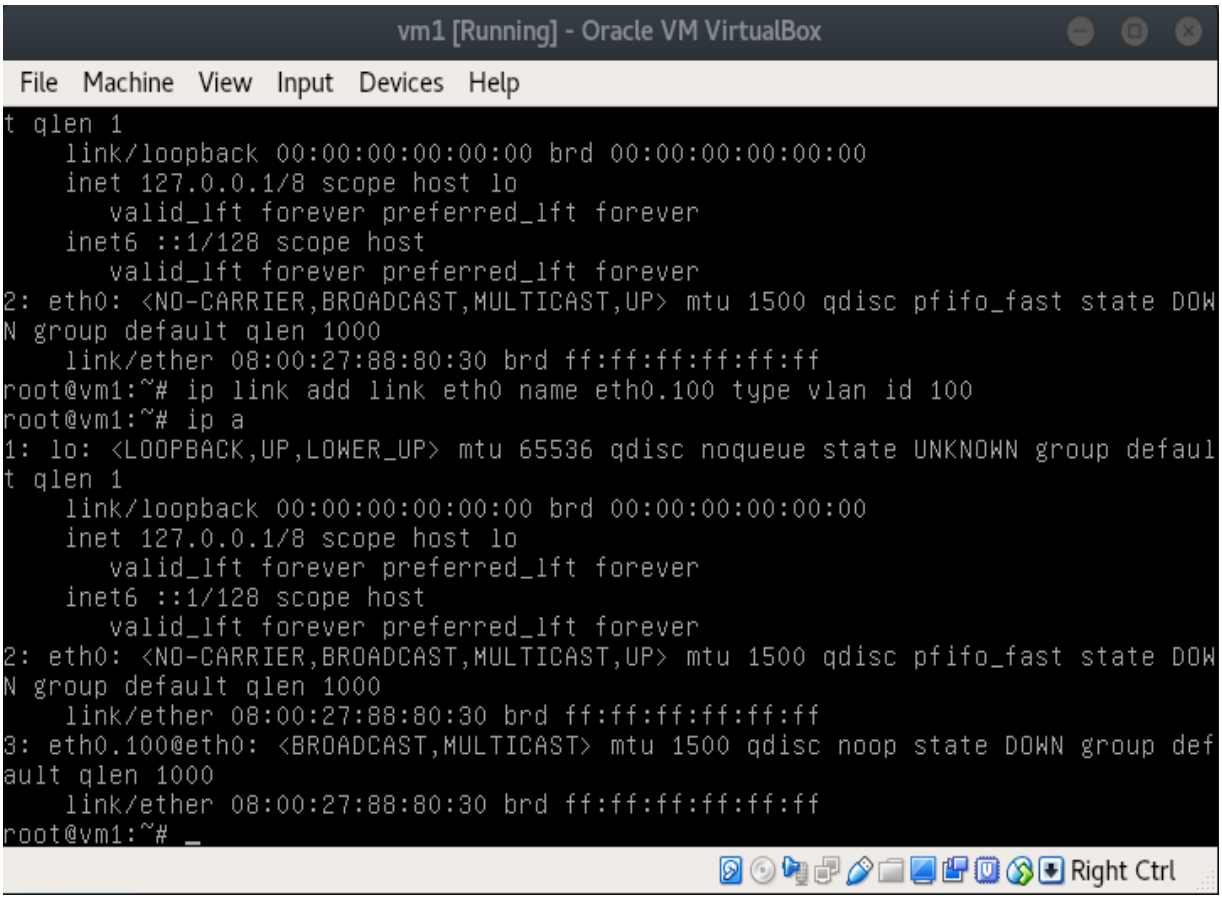


Рис. 5. Створення нового адаптеру інтерфейсу

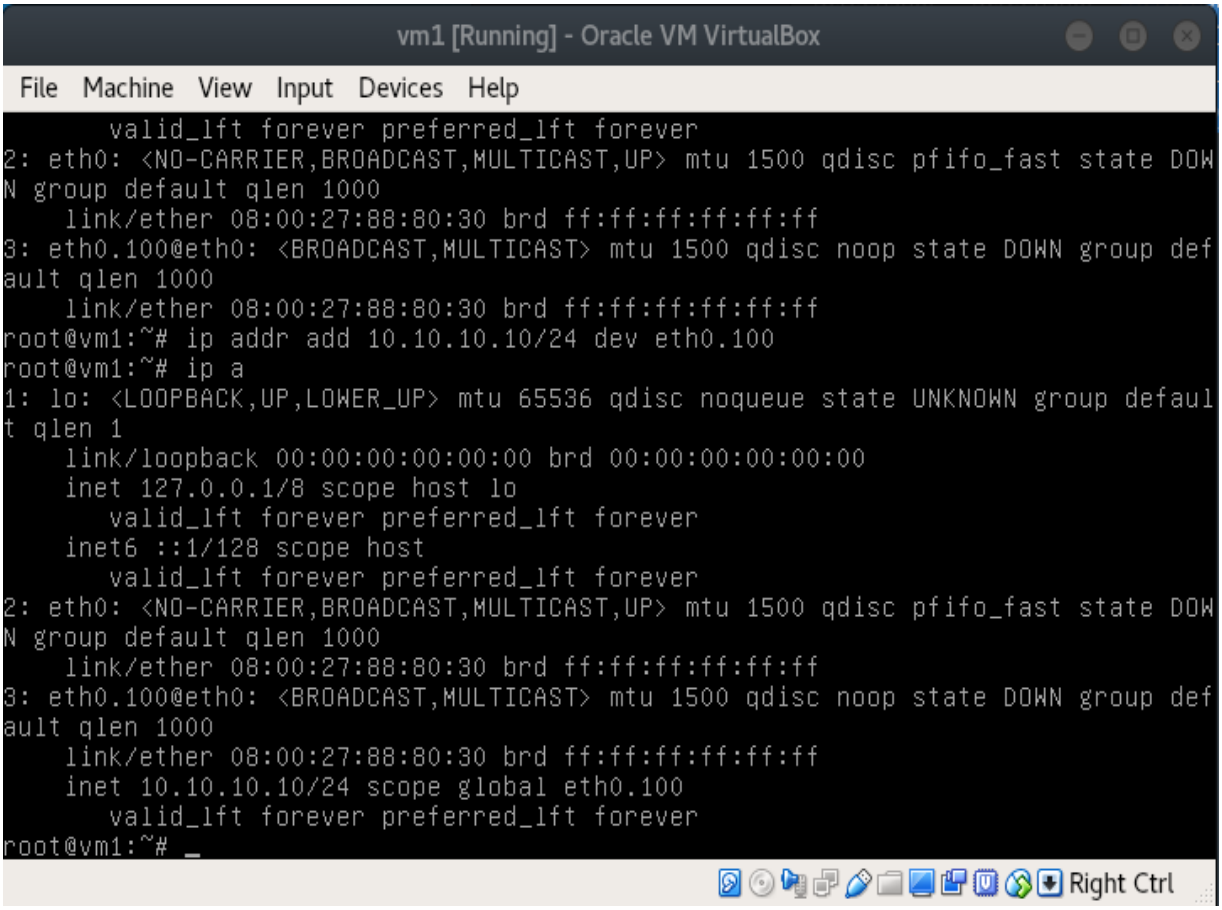


Рис. 6. Призначення адреси нового адаптеру

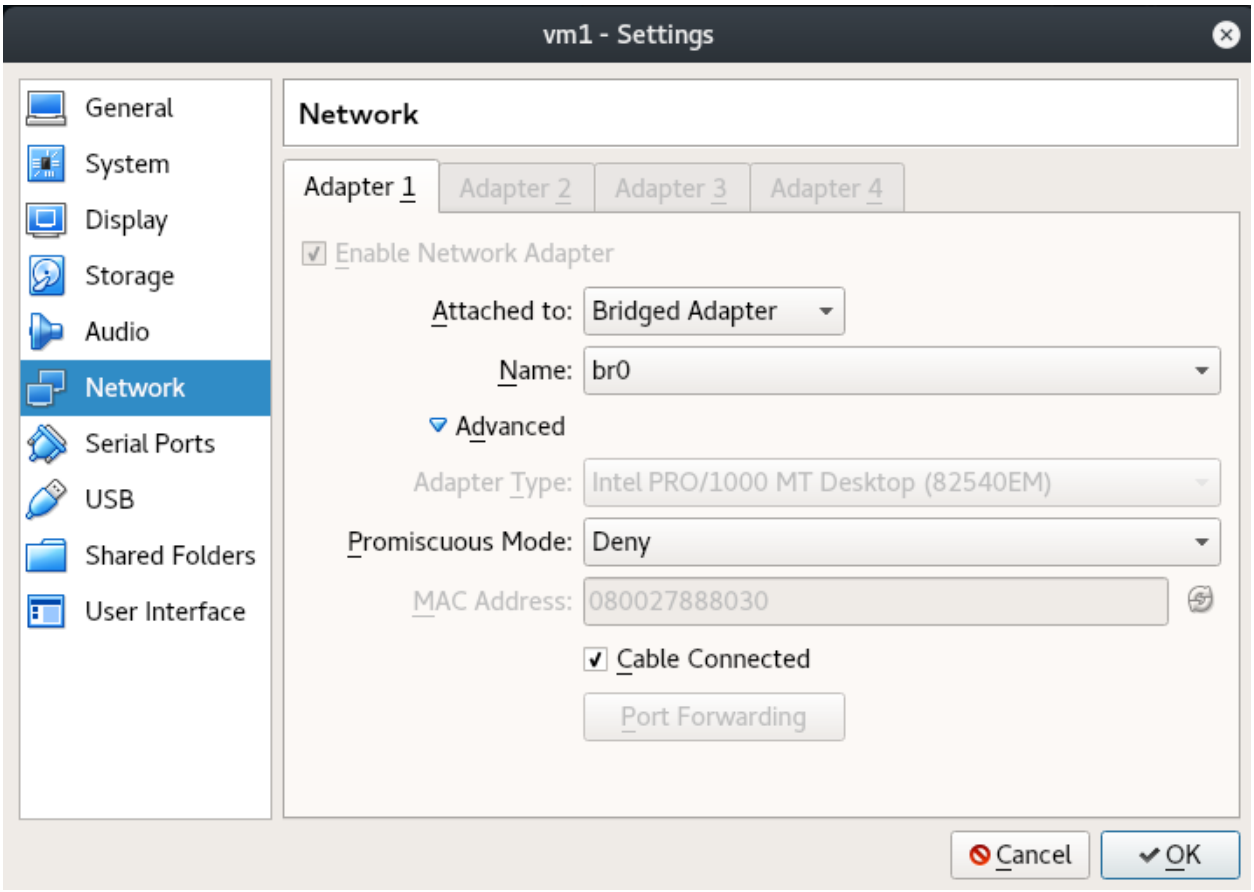


Рис. 7. Підключення кабелю

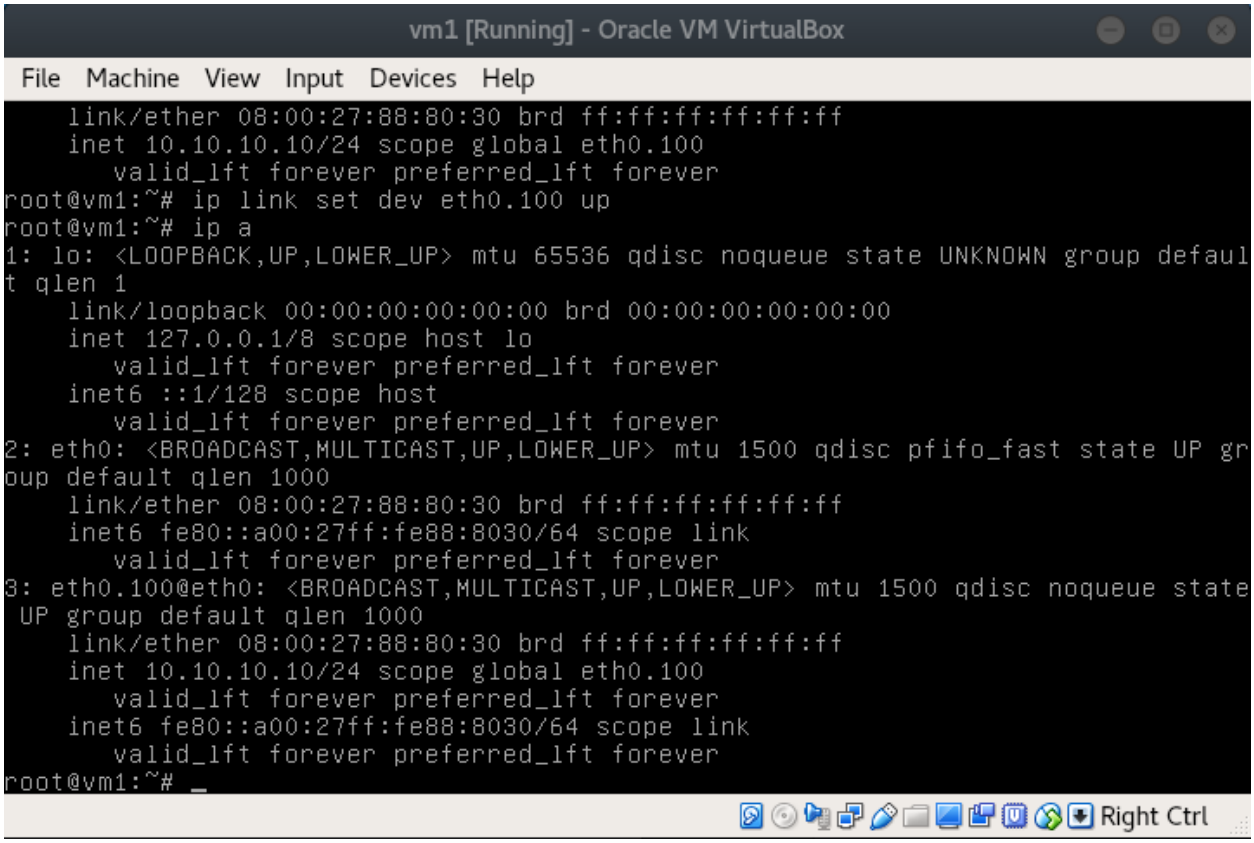


Рис. 8. Кабель підключено, інтерфейс активний

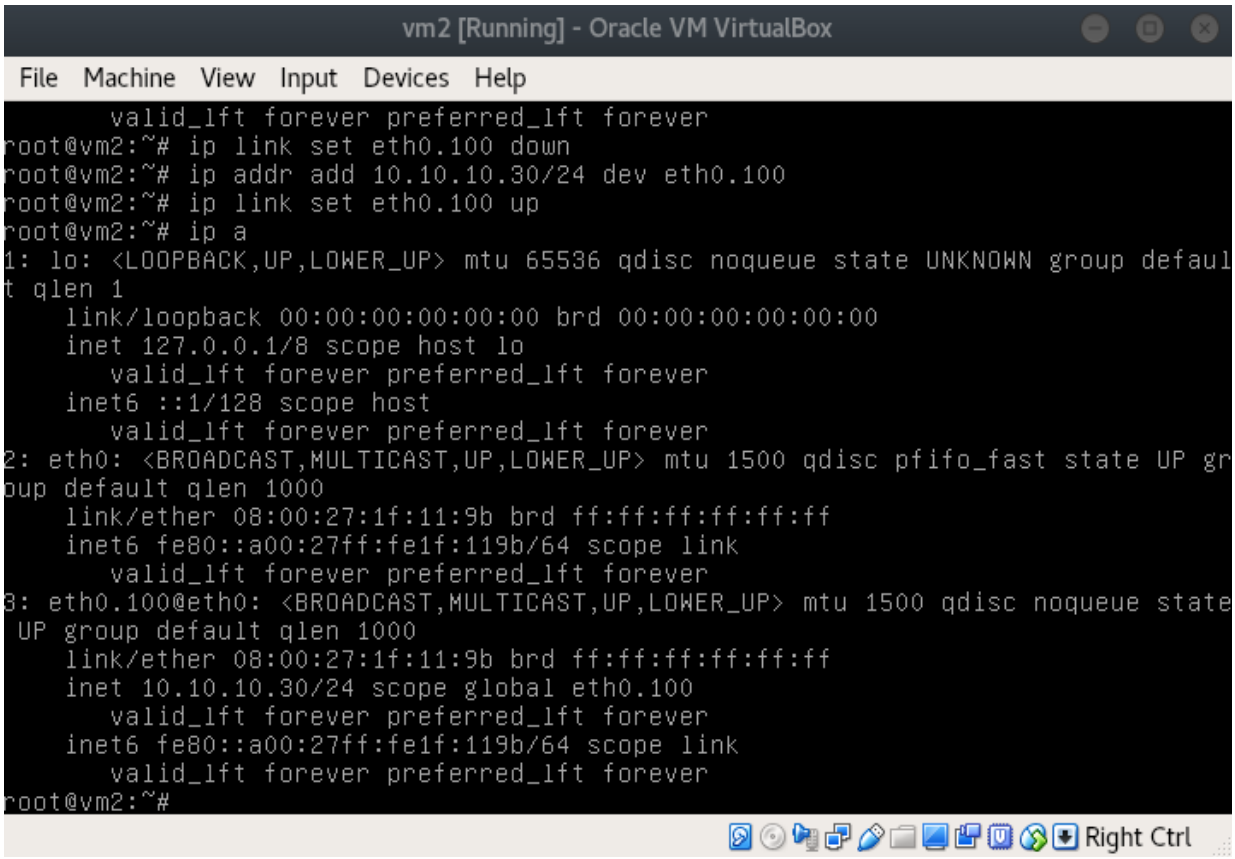


Рис. 9. Включення інтерфейсу та призначення адреси на другій машині

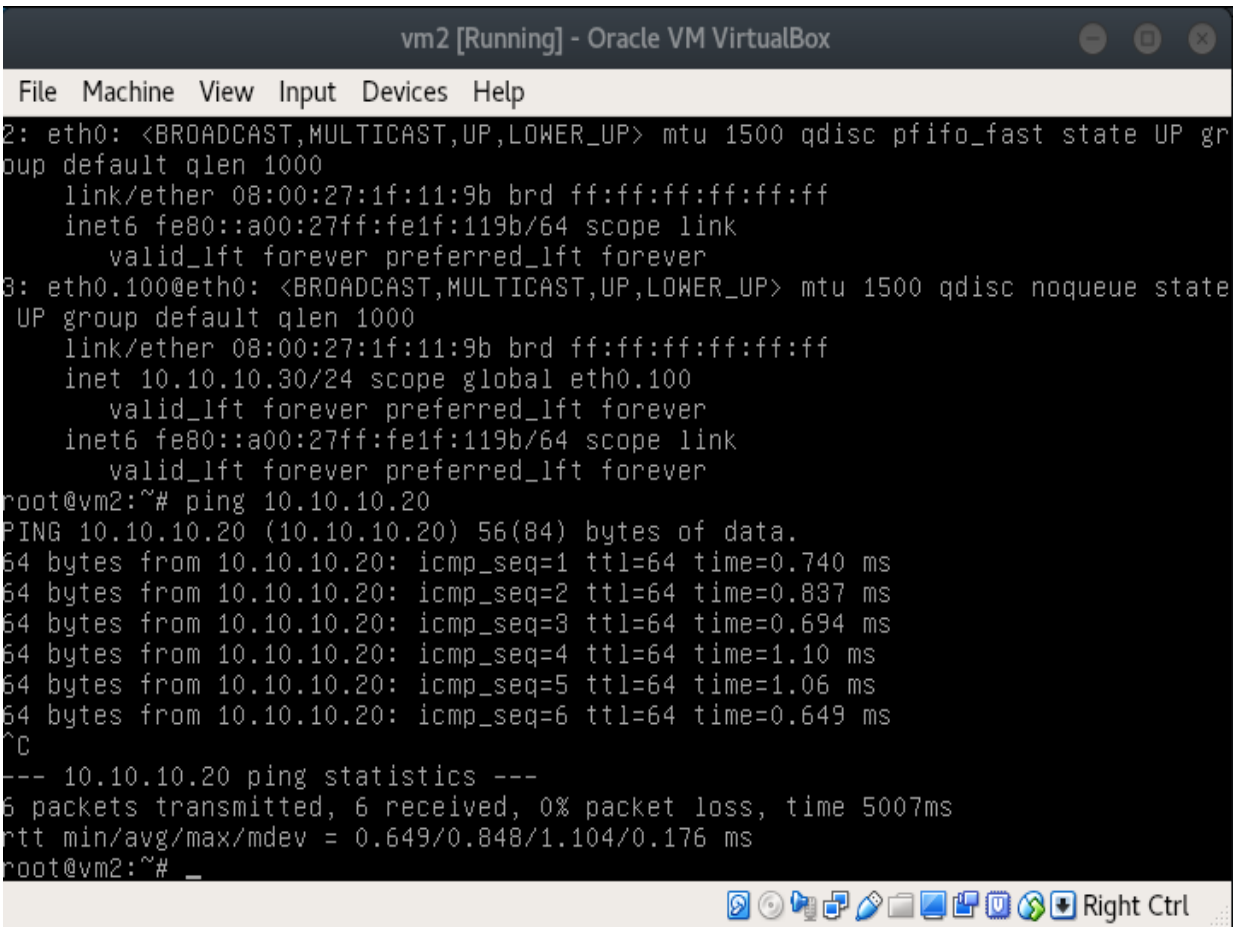


Рис. 10. Перевірка з’єднання

1.3. Розбиваємо vm1 vm2 на різні vlan. Набудовуємо intervlan routing за допомогою R1.

Тепер переходимо до пункту №2 – розіб'ємо ці дві віртуалки на різні vlan і налагодимо роутер. На VM1: додати інтерфейс eth0.200 с тегом 200 і привласнити йому адресу 192.168.0.2 (рис. 10); на VM2: додати інтерфейс eth0.300 с тегом 300 і привласнити йому адреса 172.16.0.2 (рис. 11) (Зробити самостійно)

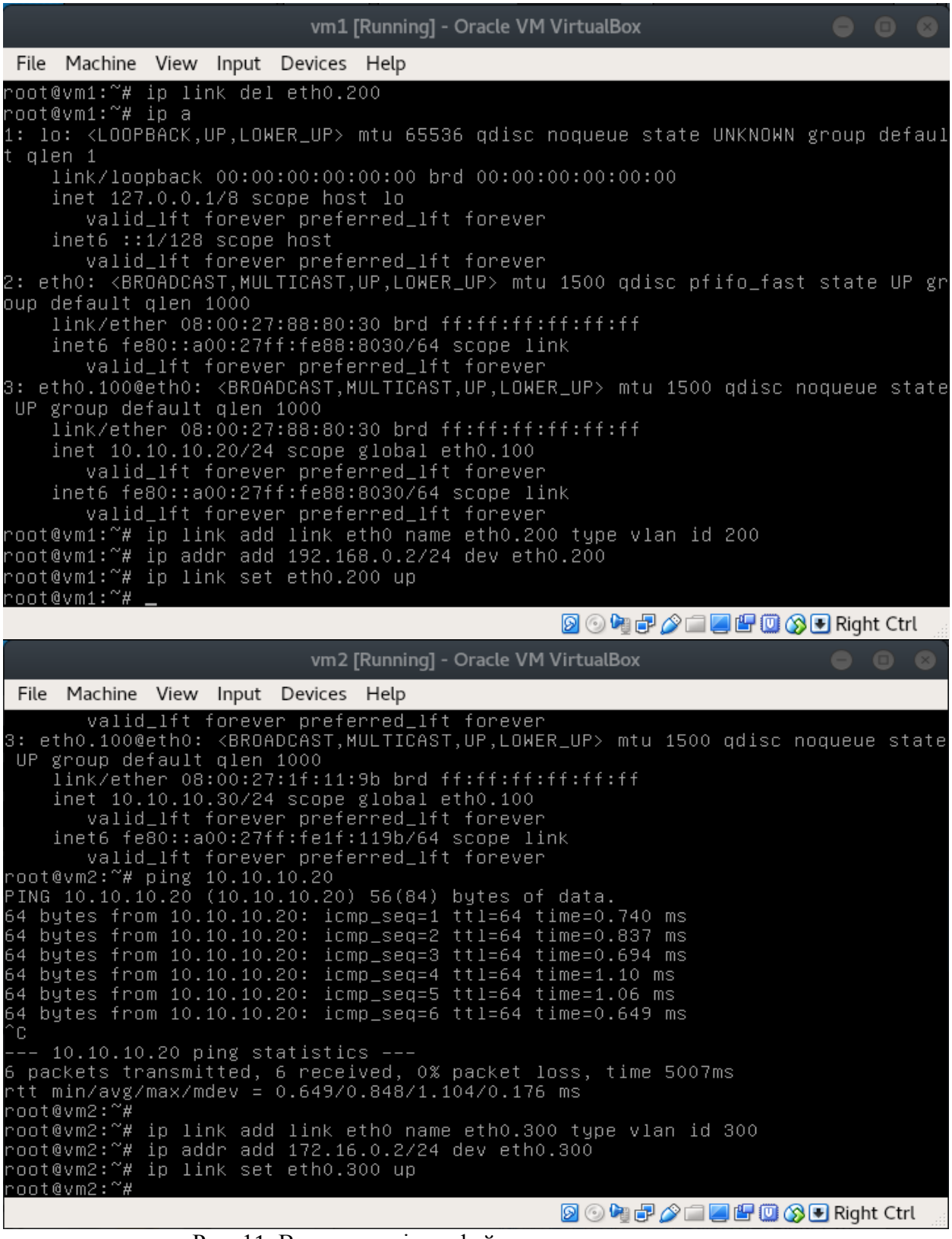


Рис. 11. Включення інтерфейсу та призначення адреси

Включимо й налагодимо роутер R1 (рис. 12). На роутері на відміну від VM1, VM2 потрібно створити інтерфейс і в vlan 200 і в vlan 300 – цей інтерфейс буде шлюзом у даних мережах. Привласнимо їм адреси 192.168.0.1, 172.16.0.1.

Перевіряємо з'єднання. Пінгуєм з роутера 192.168.0.2 і 172.16.0.2.

Отже, ми одержали з'єднання між VM1, R1 і VM2, R1. Спробуємо з'єднання VM1,VM2 через R1. Для того щоб наш Router одержав можливість посилати пакети між інтерфейсам потрібно дозволити йому це (рис. 13). Необхідно розкоментувати директиву **net.ipv4.ip_forward = 1** у файлі **/etc/sysctl.conf** і застосувати зміни командою **sysctl -p**.

```
# nano /etc/sysctl.conf
# sysctl -p
net.ipv4.ip_forward = 1
```

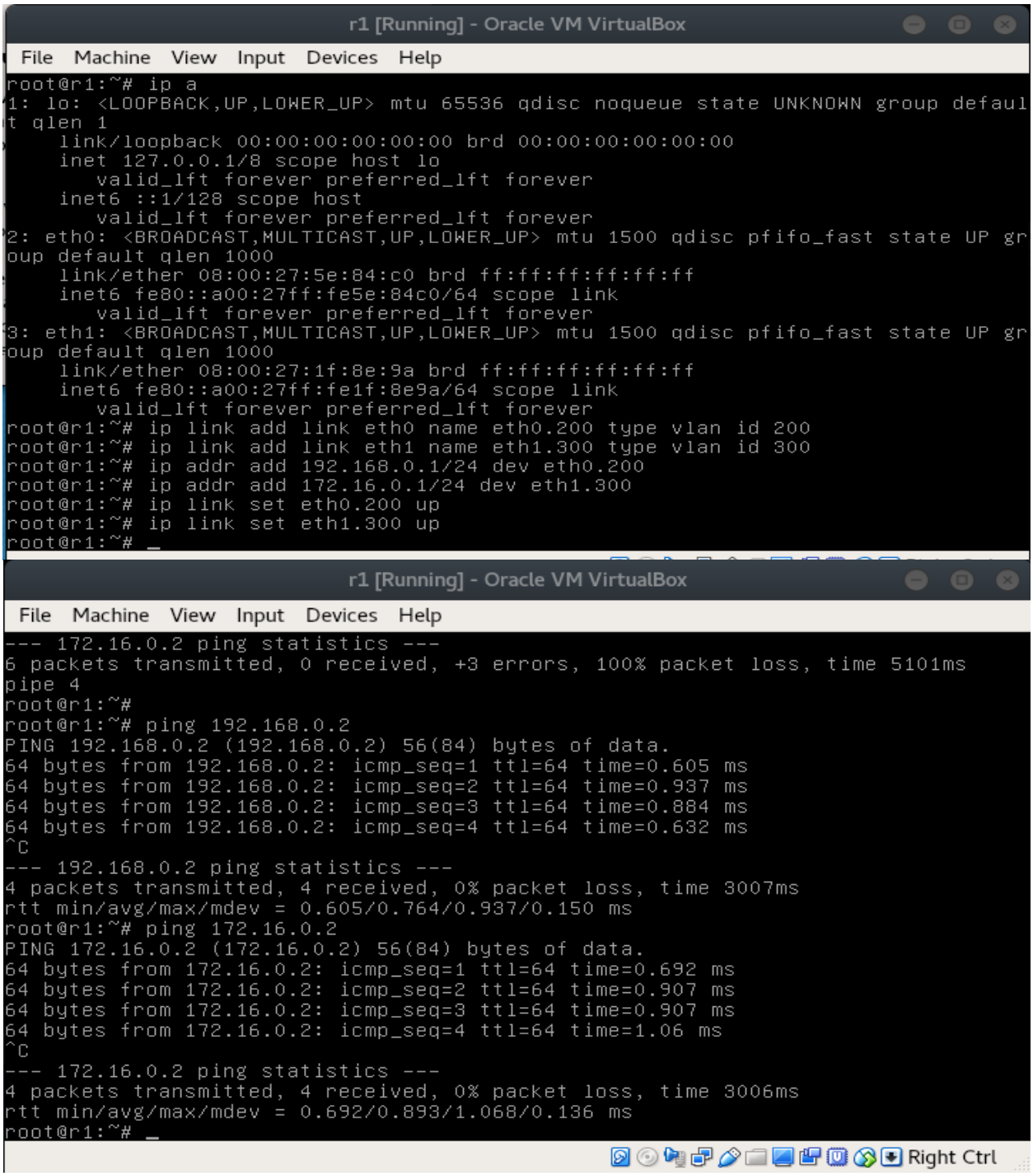
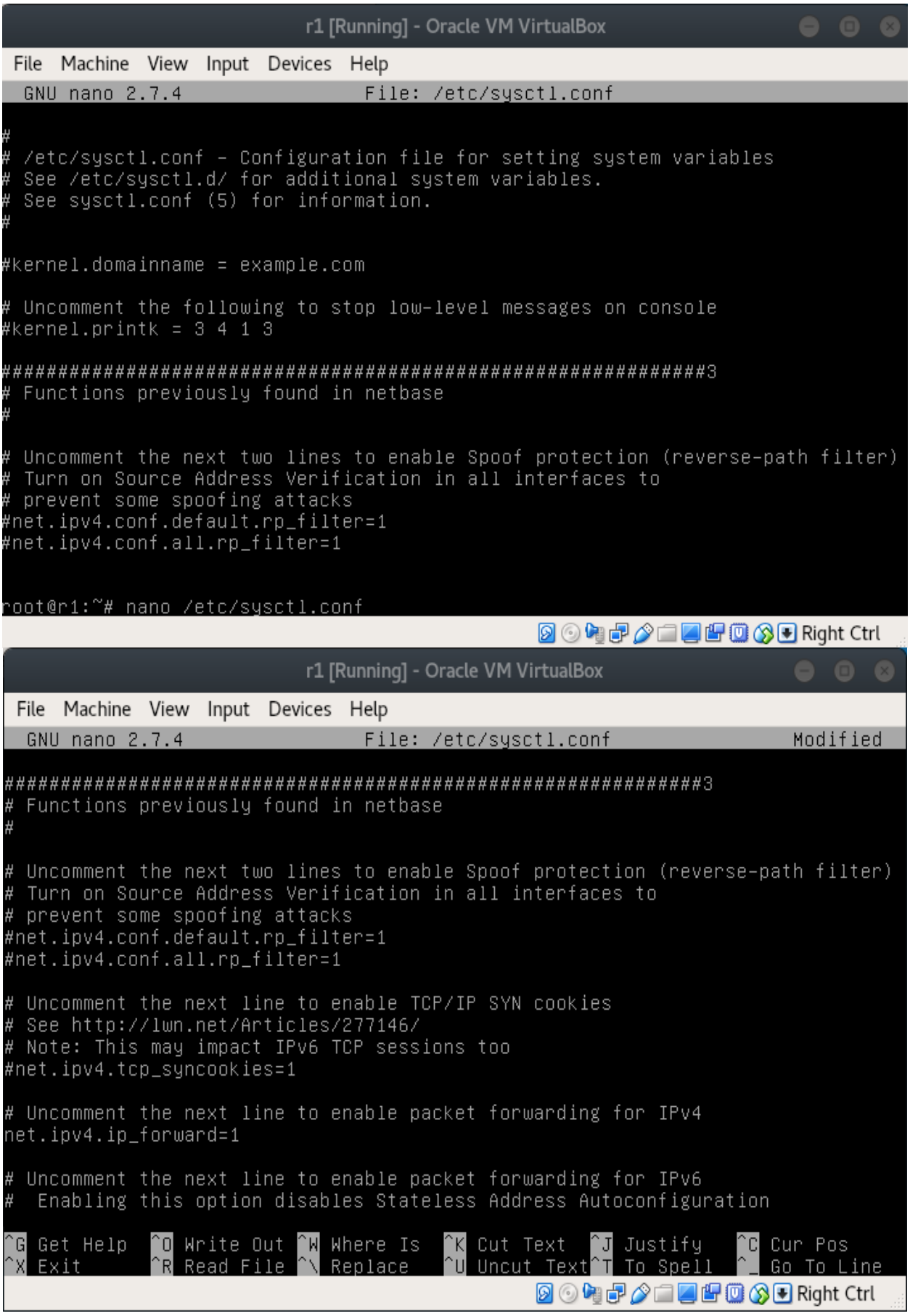


Рис. 12. Налагодження роутера R1


r1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.7.4 File: /etc/sysctl.conf
#
/etc/sysctl.conf - Configuration file for setting system variables
See /etc/sysctl.d/ for additional system variables.
See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
##3
Functions previously found in netbase
#
Uncomment the next two lines to enable Spoof protection (reverse-path filter)
Turn on Source Address Verification in all interfaces to
prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
root@r1:~# nano /etc/sysctl.conf
Right Ctrl
r1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.7.4 File: /etc/sysctl.conf Modified
##3
Functions previously found in netbase
#
Uncomment the next two lines to enable Spoof protection (reverse-path filter)
Turn on Source Address Verification in all interfaces to
prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
Uncomment the next line to enable TCP/IP SYN cookies
See http://lwn.net/Articles/277146/
Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
Right Ctrl

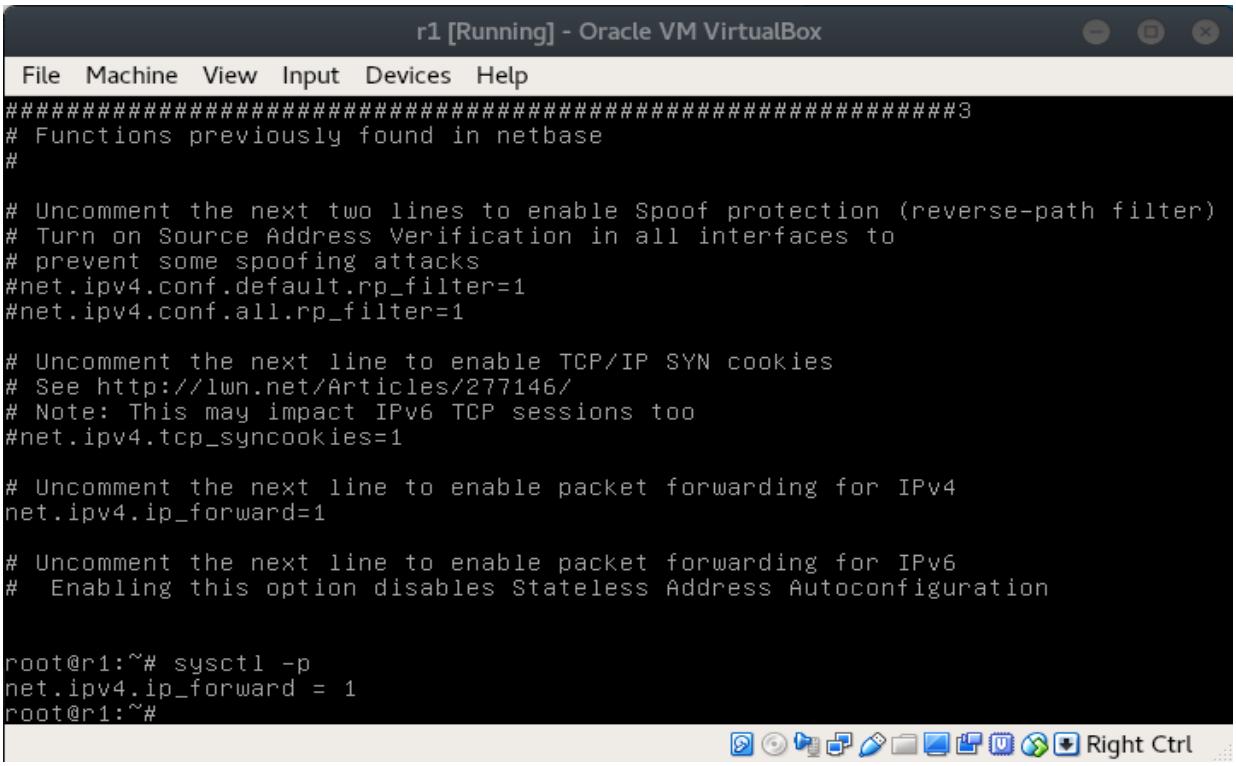


Рис. 13. Дозвіл роутеру на пересилання пакетів

Потрібно налагодити маршрутизацію. Є три розповсюджених способів це зробити:

1. Указати маршрут за замовчуванням, тобто ми не знаємо де в нас перебуває destination ip, тому всі пакети не приналежні локальної мережі передаємо на роутер.

2. Указати шлюз для конкретної підмережі. Це потрібно робити якщо мережі доступні за різними маршрутизаторами.

3. Указати інтерфейс, за яким перебуває той хто прийме пакет

Така ситуація може виникнути, наприклад при необхідності змаршрутизувати підмережу.

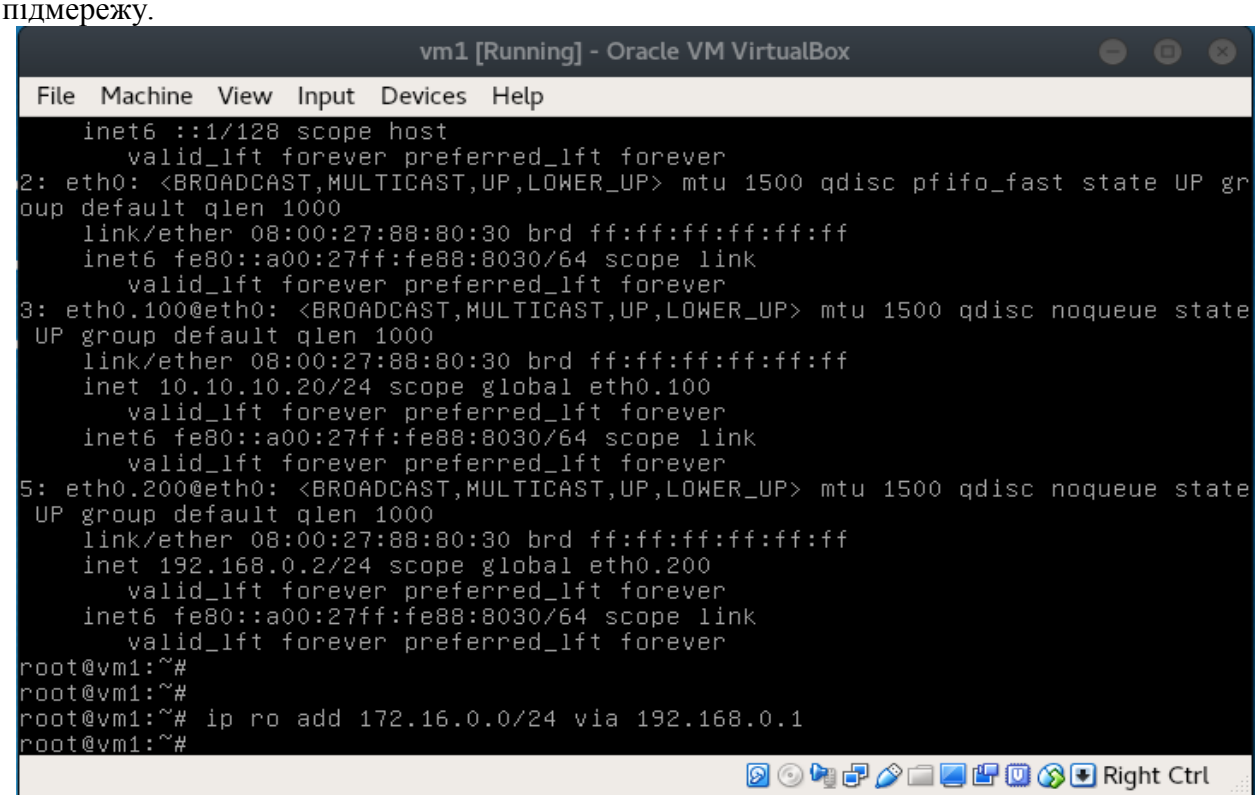


Рис. 14. Встановлення шляху для мережі

Наша віртуалка знає всього про дві підмережі: 10.10.10.0/24 & 192.168.0.0/24. Про хост 172.16.0.2 нічого не сказано, тому якщо спробувати пропінгувати нічого не вийде.

додамо маршрут до підмережі 172.16.0.0/24:

ip ro add 172.16.0.0/24 via 192.168.0.1 (рис. 14).

via — значить через кого, тобто відправляємо пакети хосту 192.168.0.1, він розбереться з пересиланням.

Переглядаючи таблицю маршрутизації ухвалюється наступний розв'язок:

1. Кому призначений даний пакет? хосту 172.16.0.2
2. Кому відправити пакет 172.16.0.2? хосту 192.168.0.1
3. Що ми знаємо про хост 192.168.0.1? він directly connected. Це підмережа. Формуємо на канальному рівні mac адресу джерела, mac адреса хосту 192.168.0.1, ip джерела — 192.168.0.2, ip адреса призначення 172.16.0.2, і відправляємо через інтерфейс eth0.200. Спробуємо пропінгувати шлюз сусіднього vlan:

ping 172.16.0.1 (рис. 15).

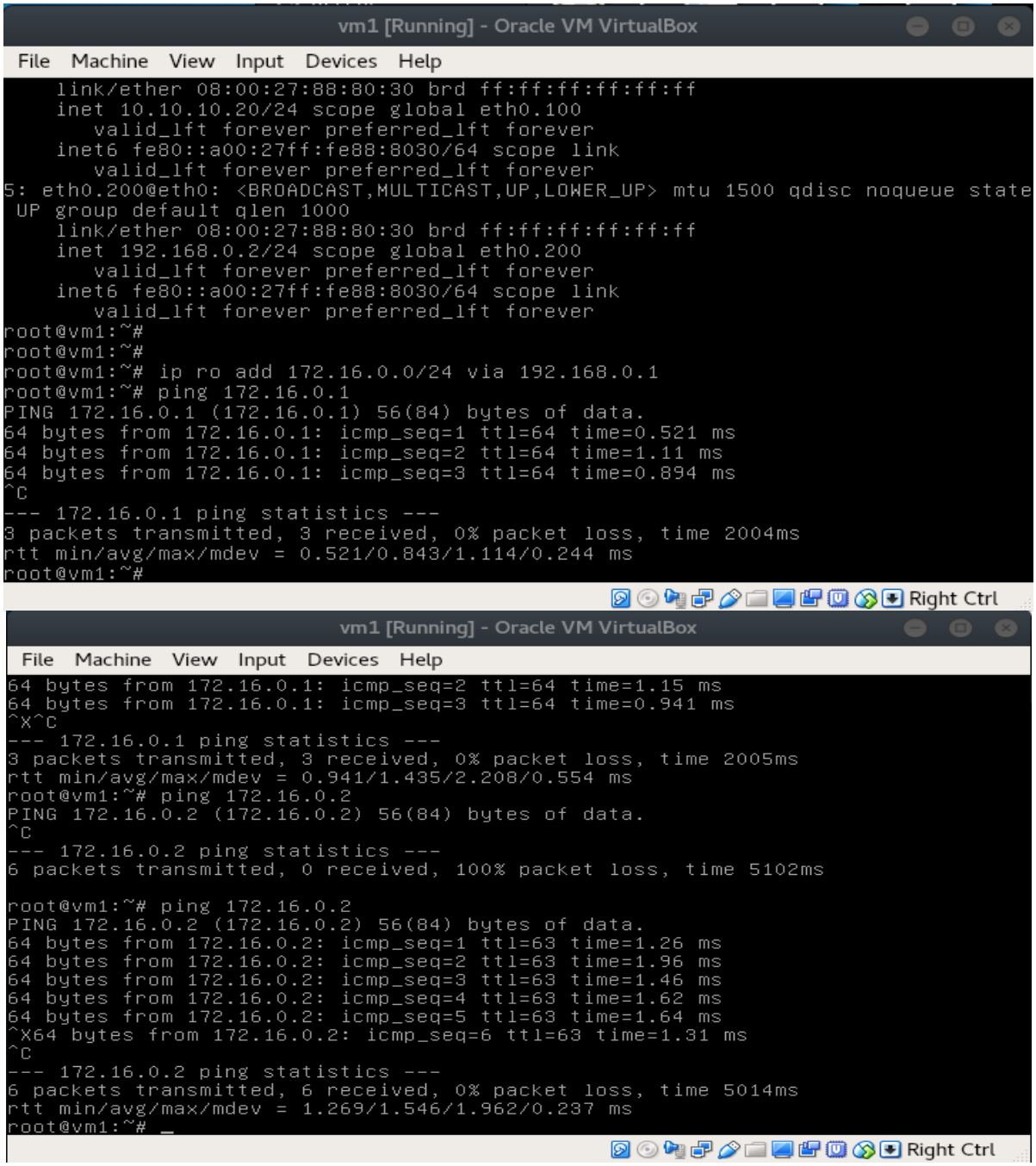


Рис. 15. Перевірка з’єднання

Працює! Але що буде якщо пінгувати 172.16.0.2? Працювати не буде, тому що немає зворотного маршруту. Пакет дійде до хосту VM2, а от назад VM2 відправити його вже не зможе, тому що не знає куди. Спробуємо додати маршрут назад на VM2. Додамо маршрут за-умовчанням для VM2. Зробити це можна вказавши підмережу і маску (0.0.0.0/0 – тобто під неї попадають абсолютно всі адреси) або використовуючи ключове слово default.

Підіб'ємо підсумок: Ми навчилися виконувати маршрутизацію між двома vlan за допомогою linux-роутера.

2. Хід роботи

Виконати дії, що прописані в розділі 1.

3. Контрольні питання

1. Для чого використовується віртуальна машина?
2. Як налагодити адаптер?
3. Якою командою додаються нові інтерфейси?
4. Як додати новий пристрій?
5. Як привласнити адресу інтерфейсу?
6. Як провести включення інтерфейсу?
7. Якою командою перевіряється з’єднання?
8. Який порядок розбивання віртуалок на різні vlan?
9. Як налагодити шлюз на роутері?
10. Які способи створення маршрутизації існують?

ЛАБОРАТОРНА РОБОТА 19.
МЕТОДИКА РОЗРАХУНКУ КОНФІГУРАЦІЇ МЕРЕЖІ ETHERNET

Мета роботи: отримати практичні навички в розрахунку параметрів різних типів мереж

1. Теорія
1.1. Розрахунок мереж Ethernet
1.2. Розрахунок PDV
1.3. Розрахунок PW
1.4. Розрахунок мережі Fast Ethernet.
2. Хід роботи
3. Контрольні питання

1. Теорія
1.1. Розрахунок мереж Ethernet

Дотримання численних обмежень, установлених для різних стандартів фізичного рівня мереж Ethernet, гарантує коректну роботу мережі (природно, при справному стані всіх елементів фізичного рівня).

Найбільше часто приходиться перевіряти обмеження, зв'язані з довжиною окремого сегмента кабелю, а також кількістю повторювачів і загальною довжиною мережі.

Правила «5-4-3» для коаксіальних мереж, створених на основі коаксіальних кабелів (рис. 1), і «4 хабів» для мереж на основі крученої пари (рис. 2) й оптоволокна не тільки дають гарантії працездатності мережі, але і залишають великий «запас міцності» мережі. Наприклад, якщо порахувати час подвійного обороту в мережі, що складається з 4 повторювачів 10Base-5 і 5 сегментів максимальної довжини 500 м, то виявиться, що воно складає 537 бітових інтервалів.

Рис. 1. Коаксіальний кабель

Рис. 2. Кабель типу “Кручена пара”

А так як час передачі кадру мінімальної довжини, разом із преамбулою, яка складає 72 байти, дорівнює 575 бітовим інтервалам, то видно, що розроблювачі стандарту Ethernet залишили 38 бітових інтервалів, як запас для забезпечення надійності. Проте в документах комітету 802.3 затверджується, що і 4 додаткових бітових інтервали створюють достатній запас надійності.

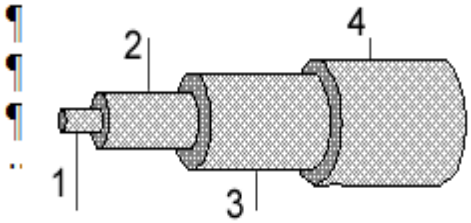


Рис. 3. Оптоволоконний кабель

Примітка. На рис. позначено: 1 – сердечник; 2 – оболонка, що відображає; 3 – покриття первинного буфера; 4 – покриття вторинного буфера

Комітет IEEE 802.3 наводить вихідні дані про затримки, які вносяться повторювачами і різними середовищами передачі даних, для тих фахівців, які хочуть самостійно розраховувати максимальну кількість повторювачів і максимальну загальну довжину мережі, не задовольняючись тими значеннями, які приведені в правилах «5-4-3» і «4 хабів». Особливо такі розрахунки корисні для мереж, що складаються зі змішаних кабельних систем, наприклад, коаксіалу й оптоволокна (рис. 4), на які правила про кількість повторювачів не розраховані. При цьому максимальна довжина кожного окремого фізичного сегмента повинна суворо відповідати стандартові, тобто 500 м для «товстого» коаксиала, 100 м для крученої пари і т.д.

Щоб мережа Ethernet, яка складається із сегментів різної фізичної природи, працювала коректно, необхідне виконання чотирьох основних умов:

- кількість станцій у мережі – не більш 1024;
- максимальна довжина кожного фізичного сегмента — не більш величини, яка визначена у відповідному стандарті фізичного рівня;
- час подвійного обороту сигналу (Path Delay Value, PDV) між двома найбільш віддаленими одна від іншої станціями мережі – не більш 575 бітових інтервалів;
- скорочення міжкадрового інтервалу IPG (Path Variability Value, PVV) при проходженні послідовності кадрів через усі повторювачі – не більше, ніж 49 бітових інтервалів (тому що при відправленні кадрів кінцеві вузли забезпечують початкову міжкадрову відстань у 96 бітових інтервали. Після проходження повторювача воно повинно бути не менше, ніж 96 - 49 = 47 бітових інтервали).

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування, що визначають

Максимальна кількість повторювачів і загальну довжину мережі в 2500 м.

1.2. Розрахунок PDV

Для спрощення розрахунків, звичайно, використовуються довідкові дані IEEE, які містять значення затримок поширення сигналів у повторювачах, приймально-передаючих пристроях і різних фізичних середовищах.

Таблиця 1

Дані для розрахунку значення PDV

Тип сегмента	База лівого сегмента, bt	База проміжного сегмента, bt	База правого сегмента, bt	Затримка середовища на 1м, bt	Максимальна довжина сегменту, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	--	24,0	--	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI9 > 2m	0	0	0	0,1026	2+48

Позначення: bt –бітові інтервали.

У табл. 1 наведені дані, необхідні для розрахунку значення PDV для усіх фізичних стандартів мереж Ethernet. Бітовий інтервал позначений як bt.

Комітет 802.3 намагався максимально спростити виконання розрахунків, тому дані, приведені в таблиці, включають відразу кілька етапів проходження сигналу. Наприклад, затримки, внесені повторювачем, складаються із затримки вхідного трансивера, затримки блоку повторення й затримки вихідного трансивера. Проте в таблиці всі ці затримки представлені одною величиною, названою базою сегмента.

Щоб не потрібно було два рази складати затримки, внесені кабелем, у таблиці даються подвоєні величини затримок для кожного типу кабелю.

У таблиці використовуються також такі поняття, як лівий сегмент, правий сегмент і проміжний сегмент. Пояснимо ці терміни па прикладі мережі, яка наведена на рис. 5.

Лівим сегментом називається сегмент, у якому починається шлях сигналу від виходу передавача (вихід Tx на рис. 5) кінцевого вузла. На прикладі – це сегмент 1. Потім сигнал проходить через проміжні сегменти 2-5 і доходить до приймача (вхід Rx на рис. 5) найбільш віддаленого вузла найбільш віддаленого сегмента 6, який називається правим. Саме тут у гіршому випадку відбувається зіткнення кадрів і виникає колізія.

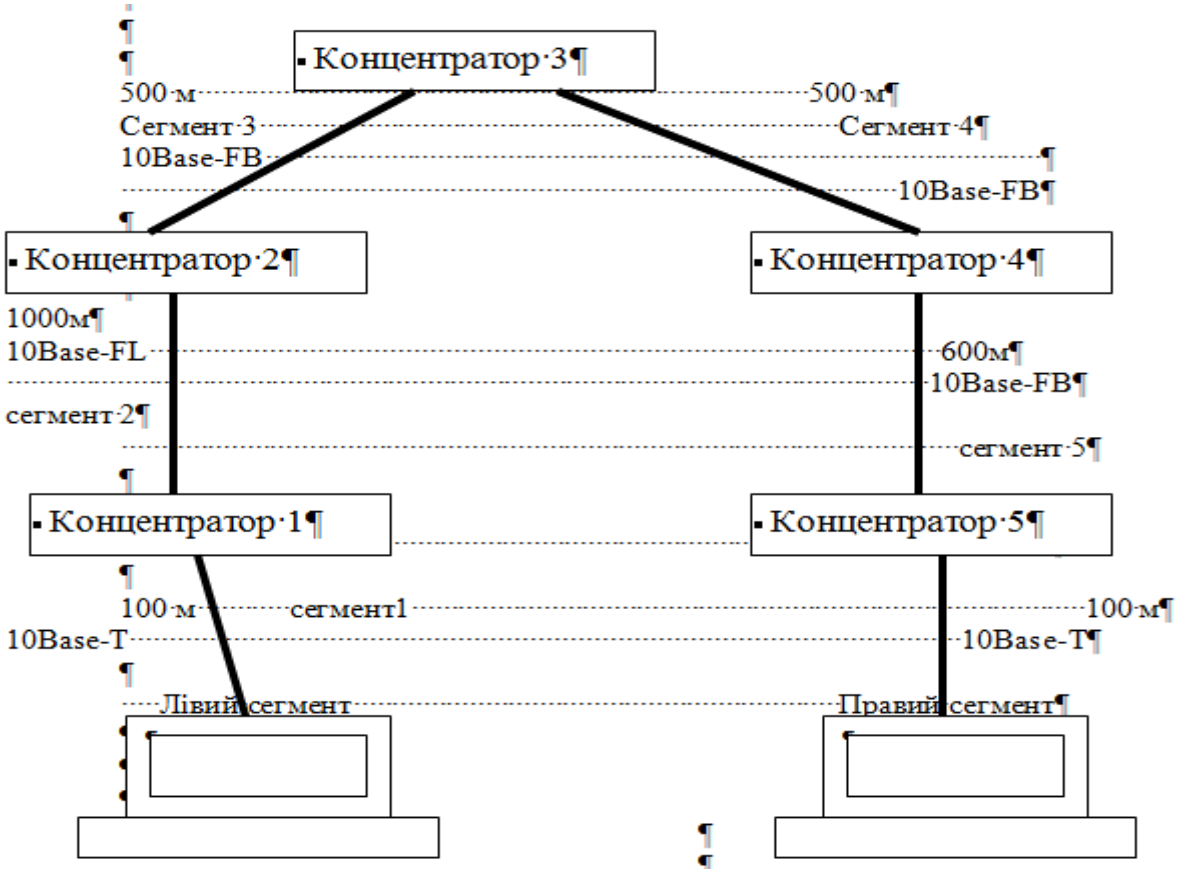


Рис. 4. Приклад мережі Ethernet

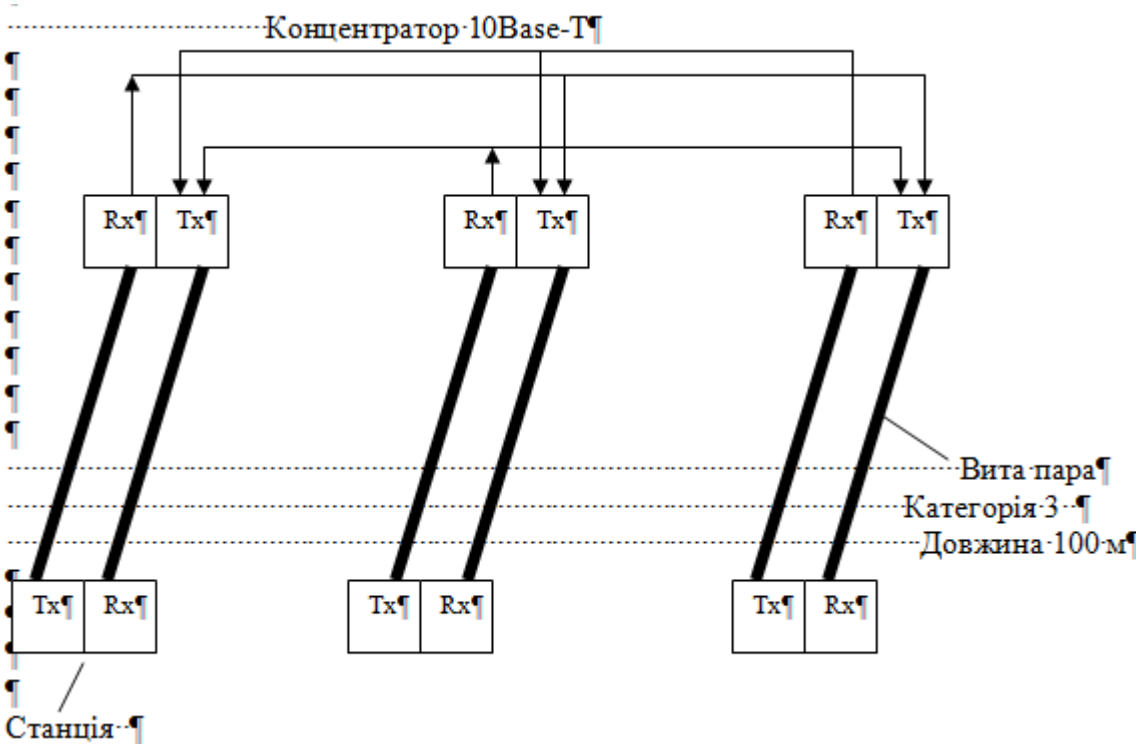


Рис. 5. Мережа стандарту 10Base-T
Позначення: Tx-- передавач, Rx-- приймач

З кожним сегментом зв'язана постійна затримка, названа базою, що за лежить тільки від типу сегмента і від положення сегмента на шляху сигналу (лівий, проміжний або правий). База правого сегмента, у якому виникає колізія, набагато перевищує базу лівого й проміжних сегментів.

Крім цього, із кожним сегментом зв'язана затримка поширення сигналу уздовж кабелю сегмента, що залежить від довжини сегмента й обчислюється шляхом множення часу поширення сигналу за одним метром кабелю (у бітових інтервалах) на довжину кабелю – в метрах.

Розрахунок полягає в обчисленні затримок, внесених кожним відрізком кабелю (приведена в таблиці затримка сигналу на 1 м кабелю множиться на довжину сегмента), а потім підсумовування цих затримок із базами лівого, проміжних і правого сегментів. Загальне значення PDV не повинне перевищувати 575.

Так як лівий і правий сегменти мають різні величини базової затримки, то у випадку різних типів сегментів на віддалених краях мережі необхідно виконувати розрахунки двічі: один раз прийняти як лівий сегмент, сегмент одного типу, а в другий – сегмент іншого типу. Результатом можна вважати максимальне значення PDV. У нашому прикладі крайні сегменти мережі належать до одного типу – стандартові 10Base-T, тому подвійний розрахунок не вимагається, але якби вони були сегментами різного типу, то в першому випадку потрібно було б прийняти в якості лівий сегмент між станцією й концентратором 1, а в другому вважати лівим сегмент між станцією й концентратором 5.

Приведена на малюнку мережа відповідно до правила 4 хабів не являється коректною – у мережі між вузлами сегментів 1 і 6 мається 5 хабів, хоча не всі сегменти є сегментами 10Base-FB. Крім того, загальна довжина мережі – 2800 м, що порушує правило 2500 м. Розрахуємо значення PDV для нашого прикладу.

- Лівий сегмент 1:
- 15,3 (база) + 100 x 0,113 = 26,6.
- Проміжний сегмент 2:
  - 33,5 + 1000 x 0,1 = 133,5.
- Проміжний сегмент 3:

- 24 + 500 x 0,1 = 74,0.
- Проміжний сегмент 4:
  - 24 + 500 x 0,1 = 74,0
- Проміжний сегмент 5:
  - + 600 x 0,1 = 84,0.
- Правий сегмент 6:
- 165 + 100x0,113 = 176,3.

Сума всіх складових дає значення PDV --568,4.

Тому що значення PDV менше максимально припустимої величини 575, то ця мережа проходить за критерієм часу подвійного обороту сигналу незважаючи на те, що її загальна довжина перевищує 2500 м, а кількість повторювачів більше 4.

1.3. Розрахунок PW

Щоб визнати конфігурацію мережі коректною, потрібно розрахувати також зменшення міжкадрового інтервалу повторювачами, тобто величину PVV.

Для розрахунку PVV також можна скористатися значеннями максимальних величин зменшення міжкадрового інтервалу при проходженні повторювачів різних фізичних середовищ, рекомендованими IEEE і приведеними в табл. 2.

Таблиця 2

Зменшення міжкадрового інтервалу повторювачами

Тип сегмента	Передаючий сегмент, bt	Проміжний сегмент, bt
10Base-5, або 10Base-2	16	11
10Base-FB	--	2
10Base-FL	10,5	8
10Base-T	10,5	8

Відповідно до цих даних розрахуємо значення PVV для нашого прикладу.

- Лівий сегмент 1 10Base-T: скорочення в 10,5 bt.
- Проміжний сегмент 2 10Base-FL -- 8 bt.
- Проміжний сегмент 3 10Base-FB -- 2 bt.
- Проміжний сегмент 4 10Base-FB -- 2 bt.
- Проміжний сегмент 5 10Base-FB –2 bt.

Сума цих величин дає значення PVV, рівне 24,5, що менше граничного значення в 49 бітових інтервалів.

У результаті приведена в прикладі мережа відповідає стандартам Ethernet за всіма параметрами, зв'язаних і з довжинами сегментів, і з кількістю повторювачів.

1.4. Розрахунок мережі Fast Ethernet

Порядок розрахунку коректності конфігурації мережі Fast Ethernet трохи відрізняється від розрахунку мережі Ethernet, як за параметрами, так і за схемою розрахунку. Стандарт Fast Ethernet не підтримує коаксіальний кабель і мережа будується винятково за топологією зірка. Обмеження на довжину кабелю комп'ютер-повторювач, комп'ютер-комп'ютер приведені нижче (табл. 3):

Таблиця 3

Обмеження на довжину кабелю в стандарті Fast Ethernet.

Тип кабелю	Стандарт	До повторювача підключений	Максимальна довжина кабелю, м
Кручена пара категорії 5	100Base-TX	—	100
Кручена пара категорії 3, 4	100Base-T4	—	100

Багатомодове оптоволокно 62,5/125 мкм	100Base-FX	тільки оптоволоконний кабель	412 (напівдуплекс) 2000 (повний дуплекс)
		один оптоволоконний кабель і кілька кабелів кручена пара	160
		трохи оптоволоконних кабелів і кілька кабелів кручена пара	136

Обмеження на кількість повторювачів

Повторювачі Fast Ethernet поділяються на два класи. Повторювачі класу 1 мають порти всіх типів (стандарт 100Base-TX, 100Base-FX і 100Base-T4). Повторювачі класу 2 мають або всі порти 100Base-T4, або порти 100Base-TX і 100Base-FX. Між будь-якими двома комп'ютерами в мережі може бути не більш двох повторювачів класу 2 або тільки один повторювач класу 1. Між собою повторювачі класу 1 повинні поєднуватися за допомогою комутаторів, мостів, маршрутизаторів. Приведених правил побудови мережі цілком достатньо для визначення коректності конфігурації мережі, тому що ці правила обрані з мінімальним "запасом міцності". Однак, при бажанні, можна провести і розрахунок PDV, виходячи з наступних підходів. Максимально припустима величина PDV = 512 бітових інтервалу. При розрахунку сегменти не поділяються на правий і лівий. Для розрахунку беруться затримки, що вносять дві взаємодіючих через повторювач мережеві карти комп'ютерів (або мережна карта комп'ютера й порт комутатора). Також враховується затримка сигналу в повторювачі й затримка, внесена кабелем. Вихідні дані для розрахунку приведені в табл. 4.

Таблиця 4

Розрахунок затримок поширення сигналу

Затримка, внесена кабелем		Затримка, внесена мережевими картами		Затримка, внесена повторювачем, мережевими картами	
Тип кабелю	Подвоєна затримка, bt на 1 м	Тип мережевих карт, які взаємодіють через повторювач	Подвоєна затримка, bt	Клас повторювача	Подвоєна затримка, bt
UTP Cat 3	l,14bt	Два адаптери TX/FX	114bt (100 м)	1	140
UTPCat4	l,14bt	Два адаптери T4	114 bt (100 м)	2	138
UTP Cat 5	l,112bt	Один адаптер TX/FX і один -- T4	111,2 bt (100 м)		128
Оптоволокно	1,0 bt	Два адаптери TX/FX	412 bt (412 м)		100

Підрахуємо, для прикладу, PDV між двома комп'ютерами, підключеними до повторювача 1 класу, розташованому в правій частині Рис. 6. Припускаємо, що використовується кручена пари 5-ої категорії (TX). PDV=100*1,112 (кабель, кручена пара) + 136*1,0 (оптокабель) + 100 (мережеві карти) + 140 (повторювач) = 487,2 < 512 Розраховане значення PDV менше граничного значення в 512 бітових інтервалів, відповідно розрахунки поки не виявили некоректність конфігурації мережі.

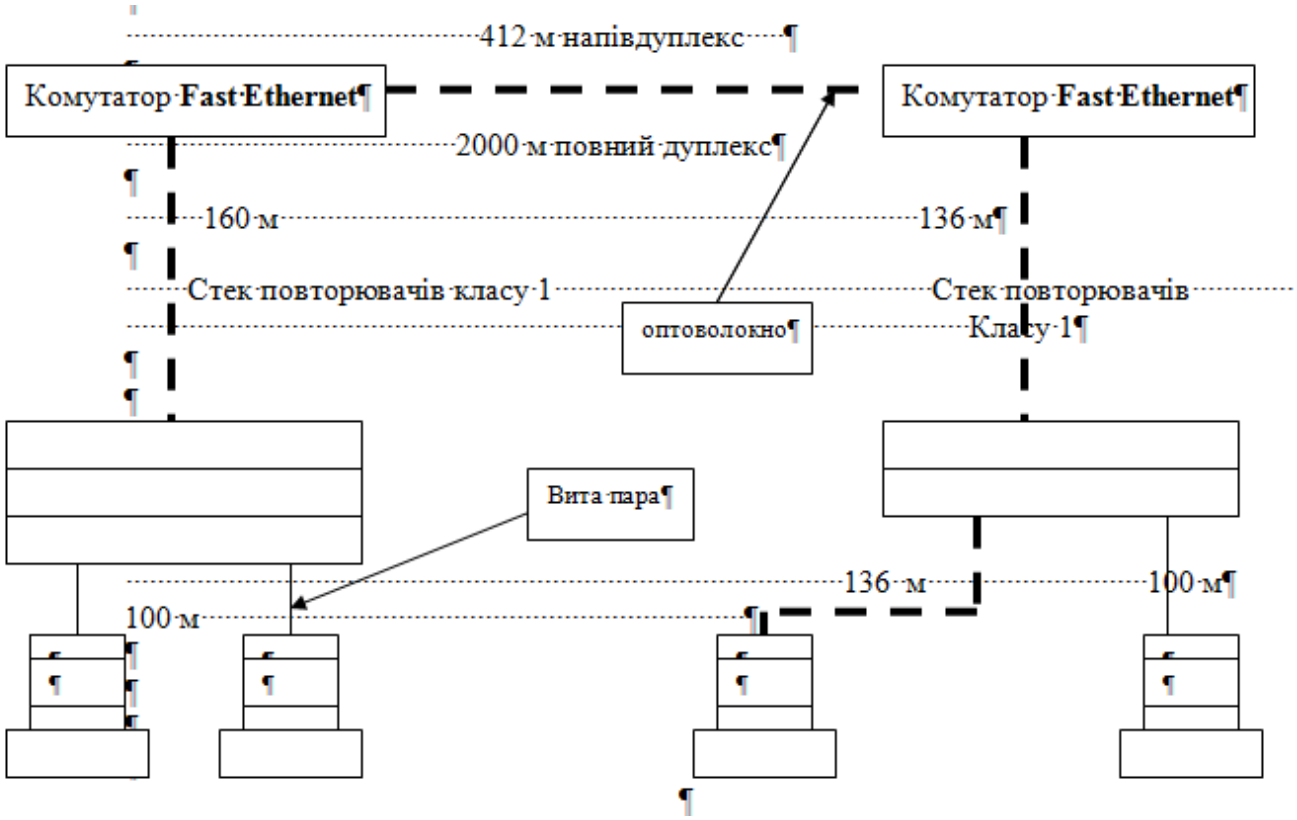
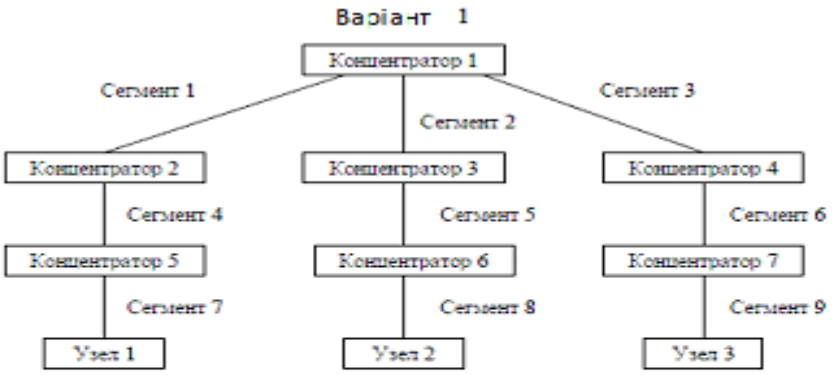


Рис. 6. Фрагмент мережі типу Fast Ethernet

2. Хід роботи

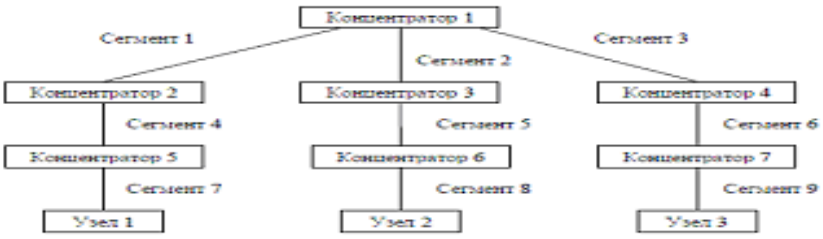
1. Ознайомитися з теоретичним матеріалом.

2. Зробити оцінку конфігурації мережі відповідно до варіанта (варіант відповідає порядковому номеру в списку групи):



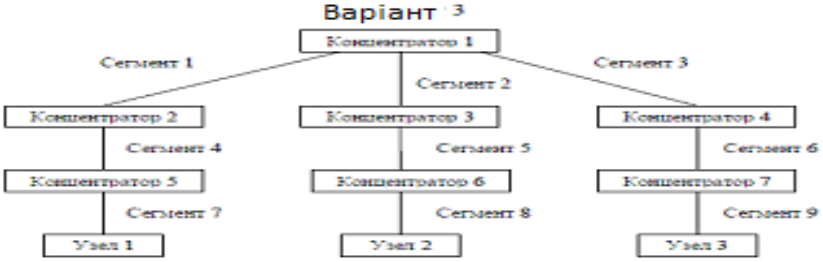
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 2	+			300
Сегмент 3	+			400
Сегмент 4		+		1000
Сегмент 5		+		300
Сегмент 6		+		400
Сегмент 7			+	100
Сегмент 8			+	50
Сегмент 9			+	100

Варіант 2



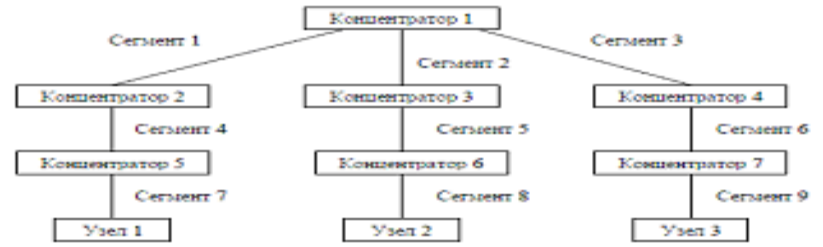
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		700
Сегмент 2	+			400
Сегмент 3	+			400
Сегмент 4		+		700
Сегмент 5		+		200
Сегмент 6	+			500
Сегмент 7			+	80
Сегмент 8			+	100
Сегмент 9			+	80

Варіант 3



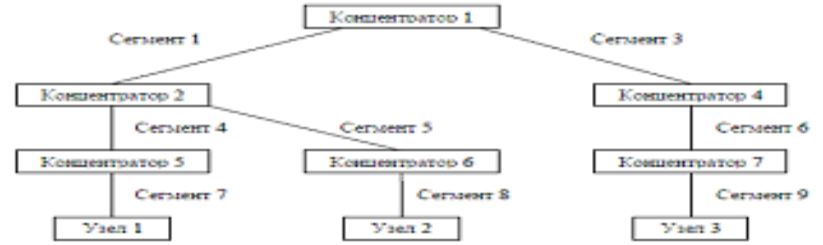
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			1000
Сегмент 2		+		200
Сегмент 3		+		200
Сегмент 4		+		400
Сегмент 5	+			300
Сегмент 6		+		200
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	40

Варіант 4



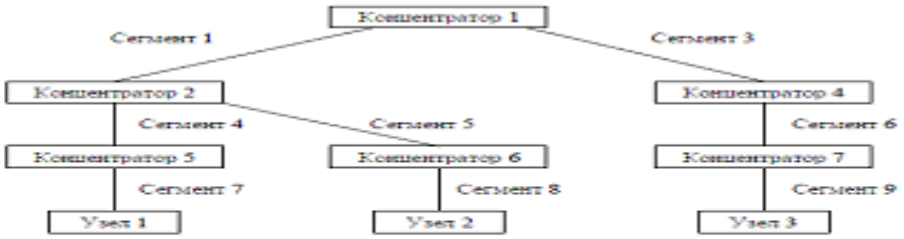
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		600
Сегмент 2		+		400
Сегмент 3		+		200
Сегмент 4	+			800
Сегмент 5	+			500
Сегмент 6	+			800
Сегмент 7			+	50
Сегмент 8			+	100
Сегмент 9			+	50

Варіант 5



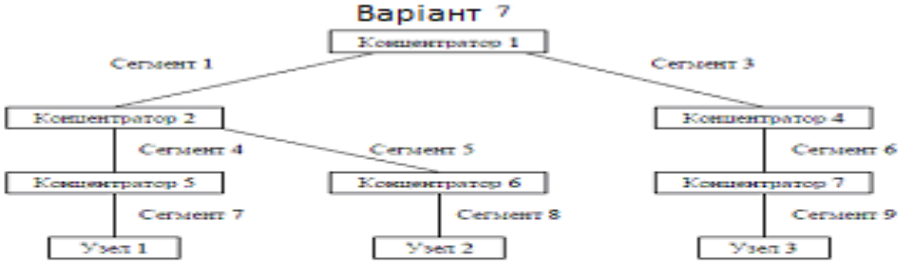
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			400
Сегмент 3	+			500
Сегмент 4		+		1100
Сегмент 5		+		1100
Сегмент 6		+		600
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	100

Варіант 6



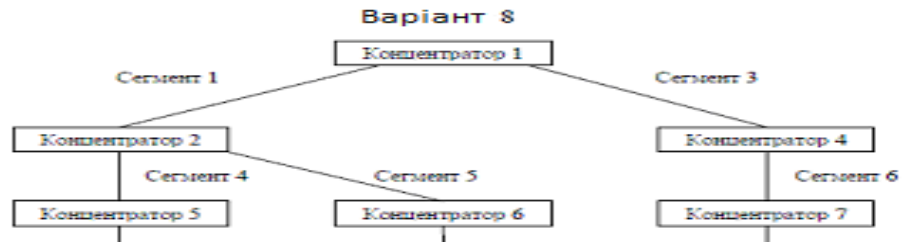
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 3		+		500
Сегмент 4	+			1000
Сегмент 5	+			1000
Сегмент 6		+		500
Сегмент 7			+	80
Сегмент 8			+	80
Сегмент 9			+	100

Варіант 7



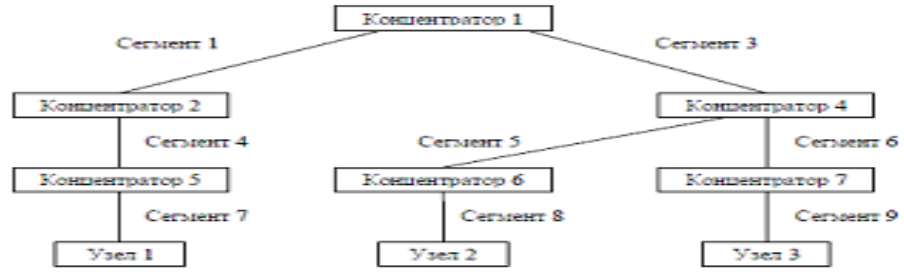
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		1000
Сегмент 3	+			1000
Сегмент 4		+		600
Сегмент 5		+		600
Сегмент 6	+			400
Сегмент 7			+	60
Сегмент 8			+	60
Сегмент 9			+	90

Варіант 8



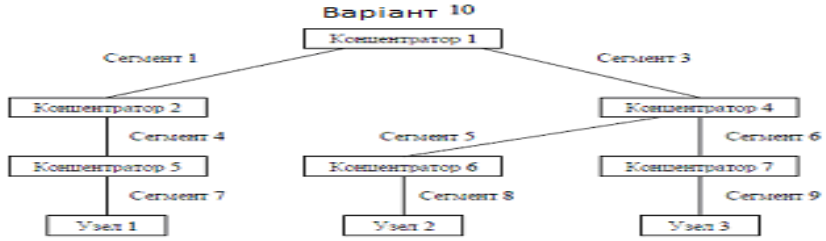
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		900
Сегмент 3		+		900
Сегмент 4	+			700
Сегмент 5	+			700
Сегмент 6	+			500
Сегмент 7			+	70
Сегмент 8			+	70
Сегмент 9			+	100

Варіант 9



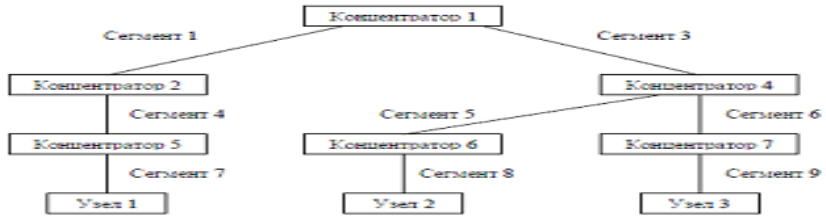
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			400
Сегмент 3	+			500
Сегмент 4		+		1100
Сегмент 5		+		1100
Сегмент 6		+		600
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	100

Варіант 10



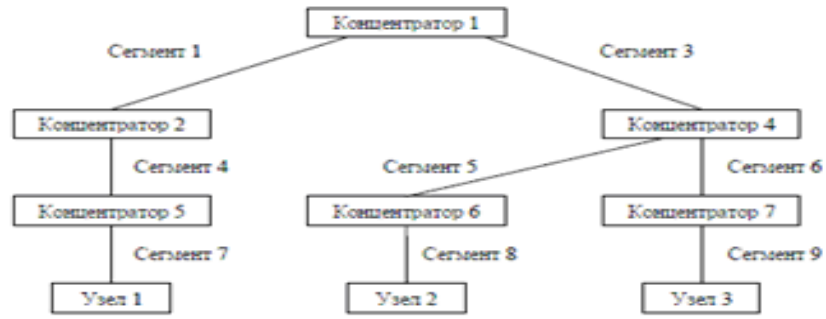
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 3		+		500
Сегмент 4	+			1000
Сегмент 5	+			1000
Сегмент 6		+		500
Сегмент 7			+	80
Сегмент 8			+	80
Сегмент 9			+	100

Варіант 11



	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		1000
Сегмент 3	+			1000
Сегмент 4		+		600
Сегмент 5		+		600
Сегмент 6	+			400
Сегмент 7			+	60
Сегмент 8			+	60
Сегмент 9			+	90

Варіант 12



	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		600
Сегмент 3		+		600
Сегмент 4	+			900
Сегмент 5	+			1000
Сегмент 6	+			500
Сегмент 7			+	70
Сегмент 8			+	80
Сегмент 9			+	90

3. Контрольні питання

1. Суть правила «5-4-3».
2. Значення максимальної довжини різних видів фізичних сегментів для мережі Ethernet.
3. Основні умови нормальної роботи мережі Ethernet, яка складається з різних видів фізичних сегментів.
4. Основні умови нормальної роботи мережі Fast Ethernet, яка складається з різних видів фізичних сегментів.
5. Значення максимальної довжини різних видів фізичних сегментів для мережі Fast Ethernet.
6. Довідкові дані IEEE.
7. Послідовність розрахунку показника PDV.
8. Послідовність розрахунку показника PW.
9. Локальна мережа. Ознаки класифікації мереж.
10. Топологія мереж. Фізичні середовища передачі даних.

ЛАБОРАТОРНА РОБОТА 20. МОДЕЛЮВАННЯ МЕРЕЖІ, ЗНАЙОМСТВО ІЗ СЕРЕДОВИЩЕМ CISCO PACKET TRACER

Мета роботи: познайомитися з інтерфейсом симулятора, вивчити режим реального часу, основні операції с обладнаннями.

Зміст

1. Хід роботи
1.1. Побудова топології мережі
1.2. Побудова топології мережі, що складається із двох підмереж
2. Контрольні питання

1. Хід роботи

1.1. Побудова топології мережі

Запускаємо середовище Cisco Packet Tracer (рис. 1).

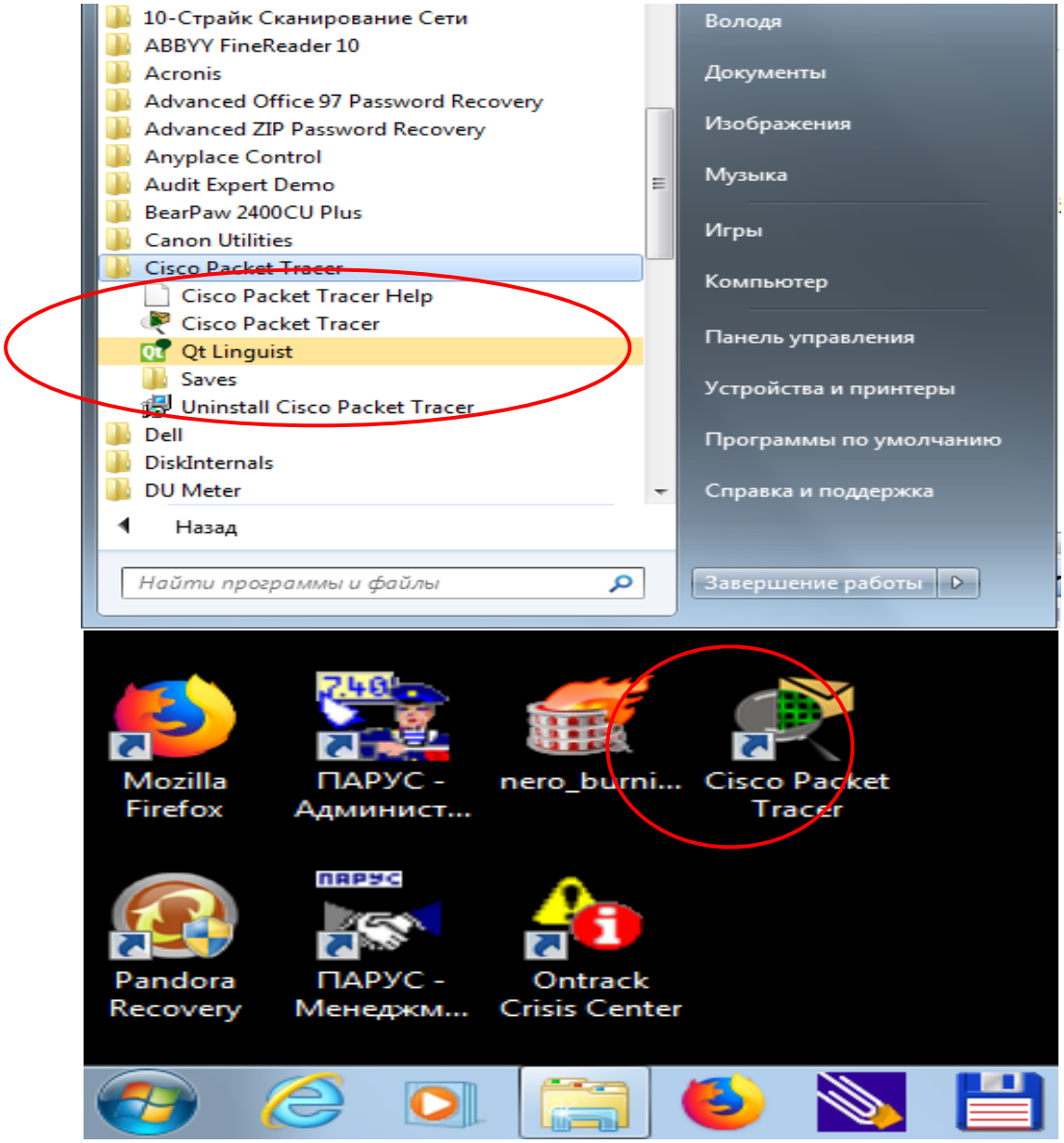


Рис. 1. Запуск програми

При запуску програми відкривається головне вікно симулятора (рис. 2).

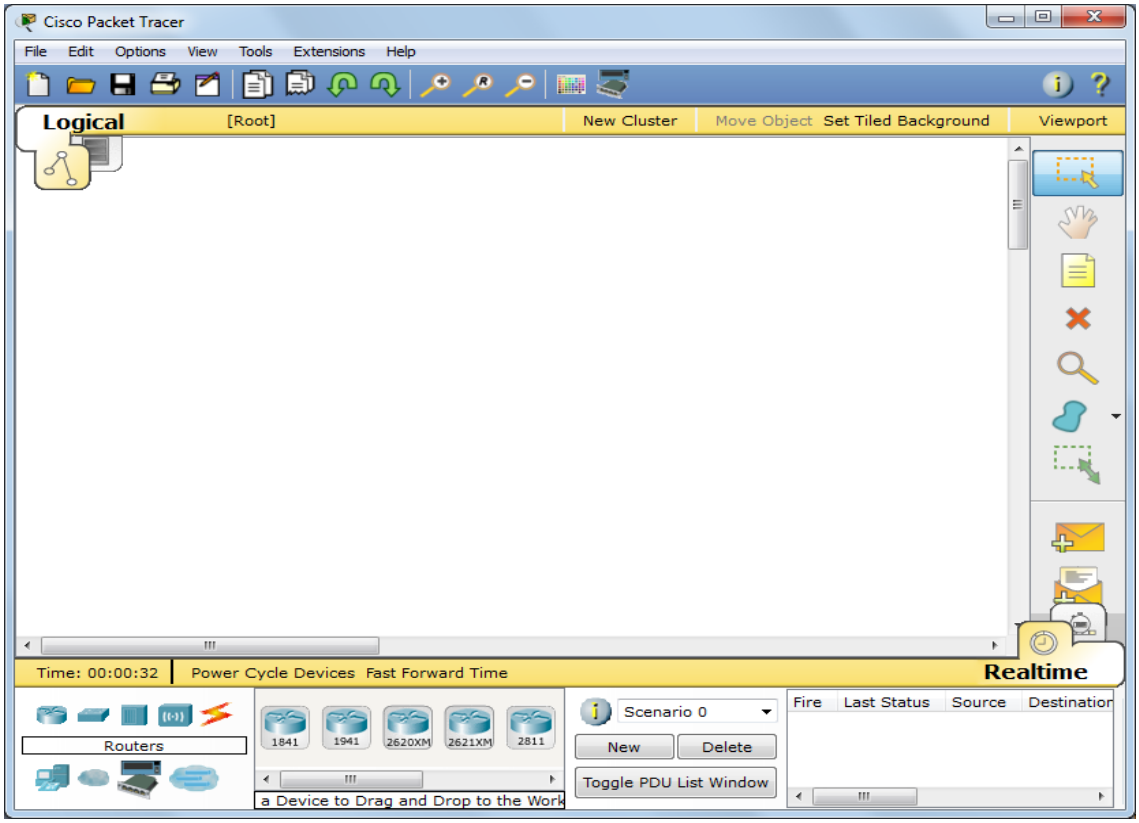


Рис. 2. Вікно програми Cisco Packet Tracer

Створюємо нову топологію мережі, вибираємо необхідні обладнання й з'єднання.

Топологія мережі може бути сконфігурирована з різних обладнань і зв'язків. У даній лабораторній роботі ми використовуємо прості мережеві обладнання: концентратор, комутатор, кінцеві обладнання (комп'ютери).

Network Component Box містить усе представлене встаткування, за допомогою якого можна побудувати мережу.

За допомогою одного клику за кожною групою обладнань і з'єднань можна відобразити різні їхні варіанти, що відрізняються між собою (рис. 3).

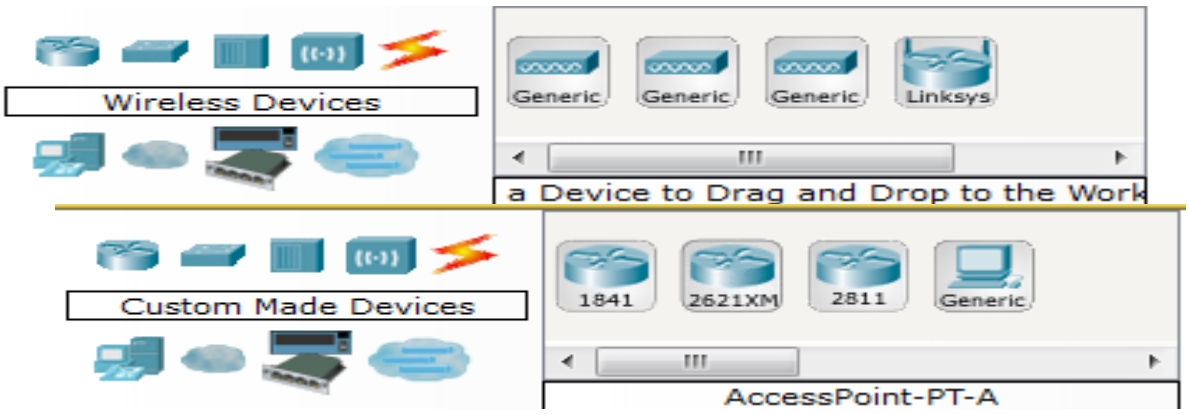


Рис. 3. Види обладнань і з'єднань

1. Побудова топології, додавання вузлів

Один клик по кінцевих обладнаннях (рис. 4,а).

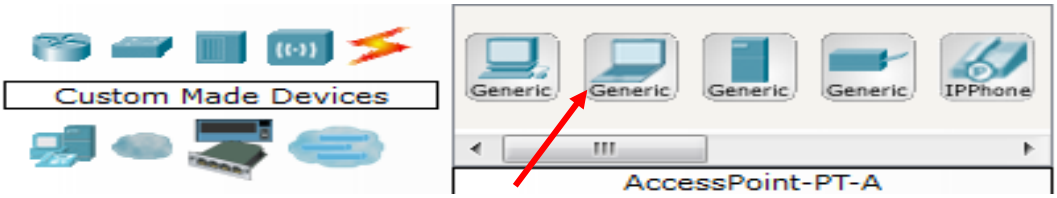


Рис. 4,а. Види кінцевих обладнань

Один клик по обранім обладнанню, для нашої роботи це PC (рис. 4,б).

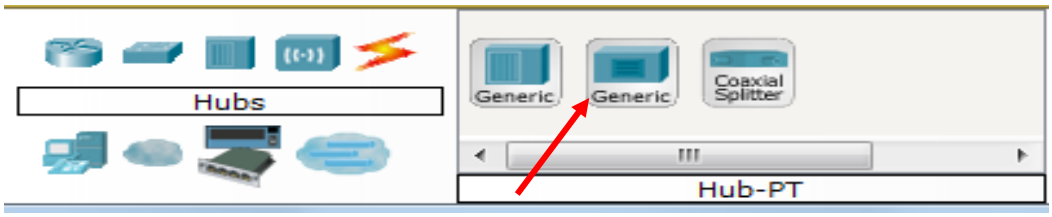


Рис. 4,б. Вибір кінцевого обладнання

Перемістіть курсор на робочу область симулятора. Курсор повинен перетворитися в знак “+”. Клацніть мишею в будь-якім місці на області й обране вами обладнання скопіюється. Проробіть цю процедуру ще п’ять разів, на робочій області у вас буде 6 PC (рис. 5).

Рис. 5. Вид робочої області

2. Підключення до вузлів концентратора й комутатора

Виберіть групу обладнань концентратори (Hubs), із цієї групи виберіть першу модель (Hub-pt). Розмістіть концентратор між PC0 і PC1 (рис. 6).

Завдання концентратора досить просте: він повторює пакет, прийнятий на одному порту на всіх інших портах.

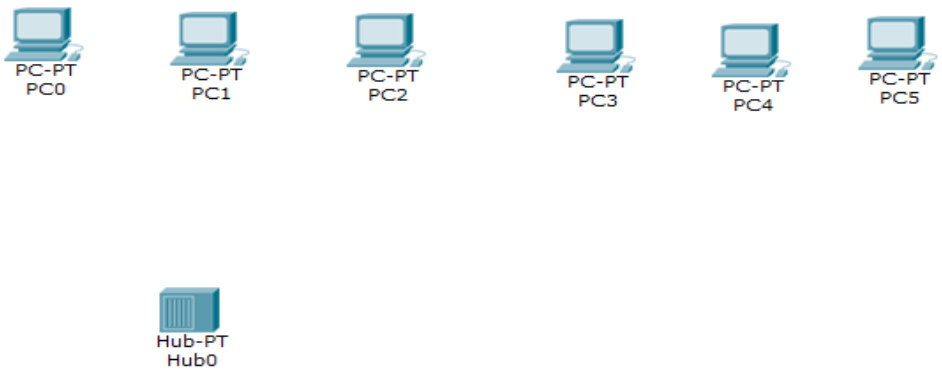


Рис. 6. Вид робочої області

Підключимо PC0 до Hub1, вибравши спочатку тип підключення. Для цього випадку підійде мідний кабель із прямим підключенням (рис. 7).

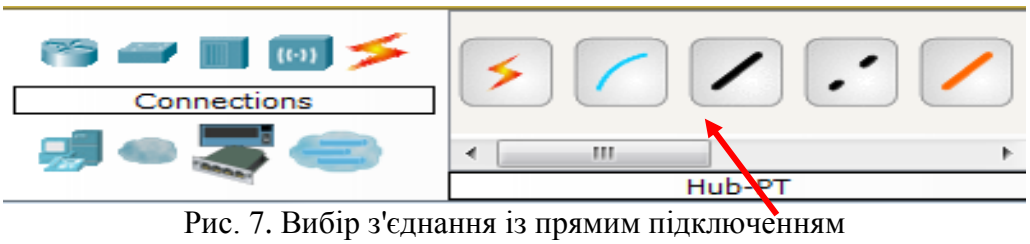


Рис. 7. Вибір з'єднання із прямим підключенням

Для підключення PC0 до Hub0 виконаєте наступну послідовність дії (рис. 8):

1) Один раз клацніть мишею на PC0
2) Виберіть тип інтерфейсу Fastethernet
3) Перемістите курсор на Hub0
4) Натисніть на Hub0 один раз і виберіть порт 0
5) Зверніть увагу на зелені індикатори двох обладнань на з'єднанні, що виходить, обоє обладнання готові до роботи.

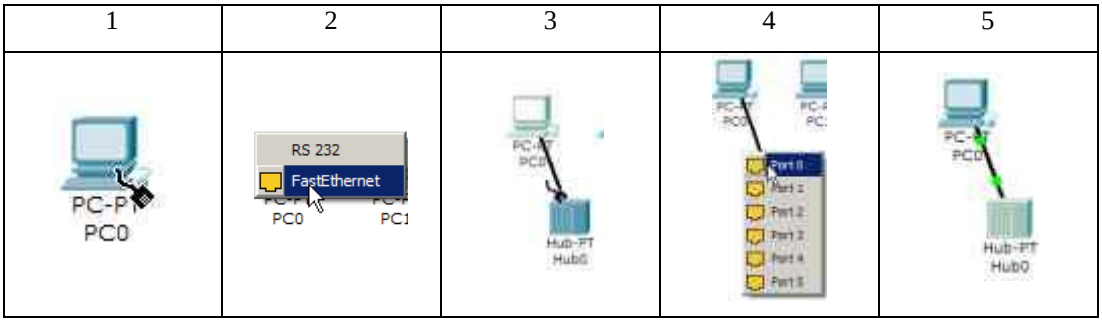


Рис. 8. Підключення PC0 до Hub0

Повторіть описані вище дії для підключення PC1 та PC2 до Hub0, вибравши на концентраторі порт 1 (рис. 9). Фактично номер порту значення не має, однак зручніше займати порти послідовно.

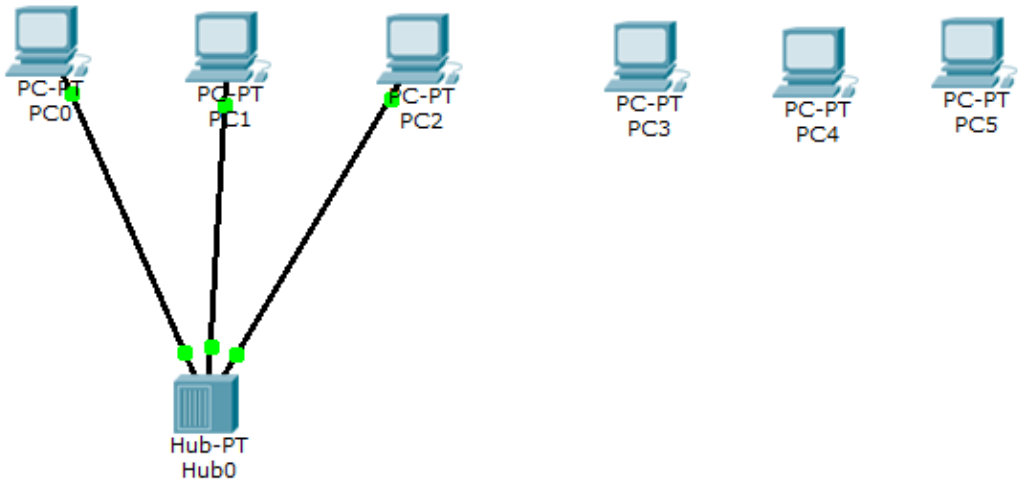


Рис. 9. Вид робочої області

Далі розміщаємо на робочій області симулятора комутатор, наприклад, модель 2950-24 (рис. 10). Опис сімейства комутаторів серії 2950 можна знайти на сайті компанії Cisco Systems. [Електронний ресурс]. URL:

http://www.cisco.com/web/RU/products/hw/switches/ps628/ps627/index.html.

Комутатори – це обладнання, що працюють на канальному рівні моделі OSI і призначені для об'єднання декількох вузлів у межах одного або декількох сегментів мережі. Комутатор передає пакети на підставі внутрішньої таблиці – таблиці комутації, отже, трафік іде тільки на той порт, якому він призначений, а не повторюється на всіх портах, на відміну від концентратора.

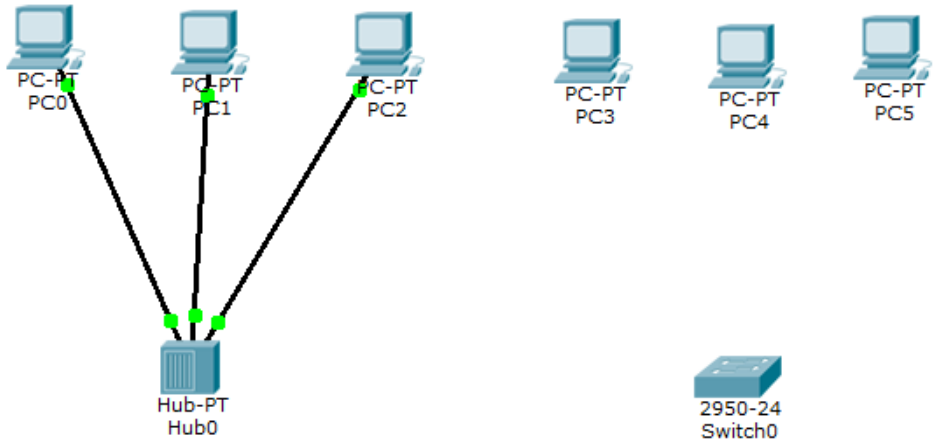


Рис. 10. Вид робочої області

Підключимо PC3 до Switch0, вибравши тип з'єднання мідний кабель із прямим підключенням.

Для підключення виконаєте наступну послідовність дії (рис. 11):

1) Клацніть мишею один раз на PC2
2) Виберіть тип інтерфейсу Fastethernet
3) Перемістіть курсор на Switch0
4) Натисніть один раз на Switch0 і виберіть Fastethernet0/1
5) Зверніть увагу, що для правильної роботи мережі обоє підключених обладнання повинні бути готові, про що свідчать зелені індикатори. На відміну від підключення до концентратора, це може зайняти якийсь час.

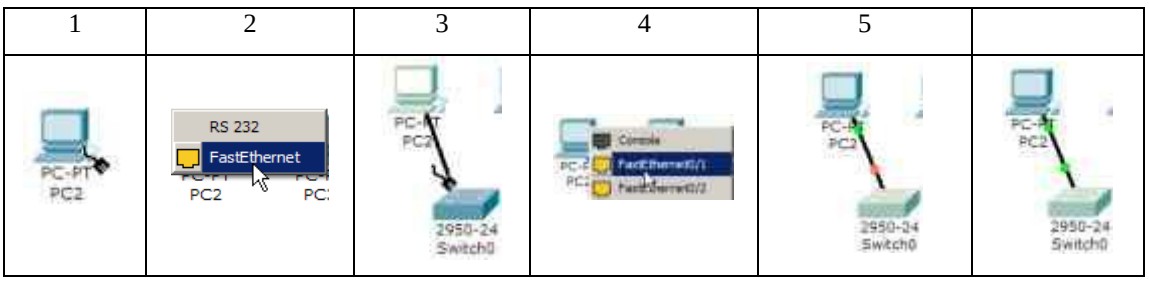


Рис. 11. Підключення PC2 до Switch0

Повторіть описані вище дії для підключення PC4 та PC5 до Switch0, вибравши один з його інтерфейсів Fastethernet0/2 (рис. 12).

Якщо навести курсор на один з індикаторів, можна подивитися, який інтерфейс задіяний при даним підключенні (рис. 13).

3. Налаштування Ip-Адреси й маски підмережі на хостах

Перш ніж ми зможемо спілкуватися між хостами за мережею, нам потрібно налаштувати Ip-адреси й маски підмережі на обладнаннях.

Клацніть мишею один раз на PC0. Відкриється вікно властивостей кінцевого вузла на вкладці Physical (рис. 14).

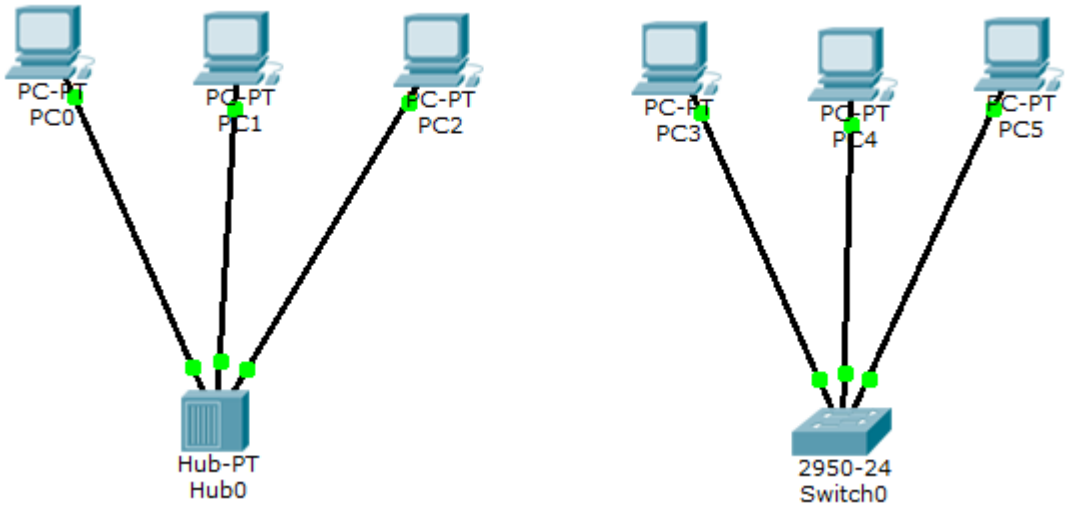


Рис. 12. Вид робочої області

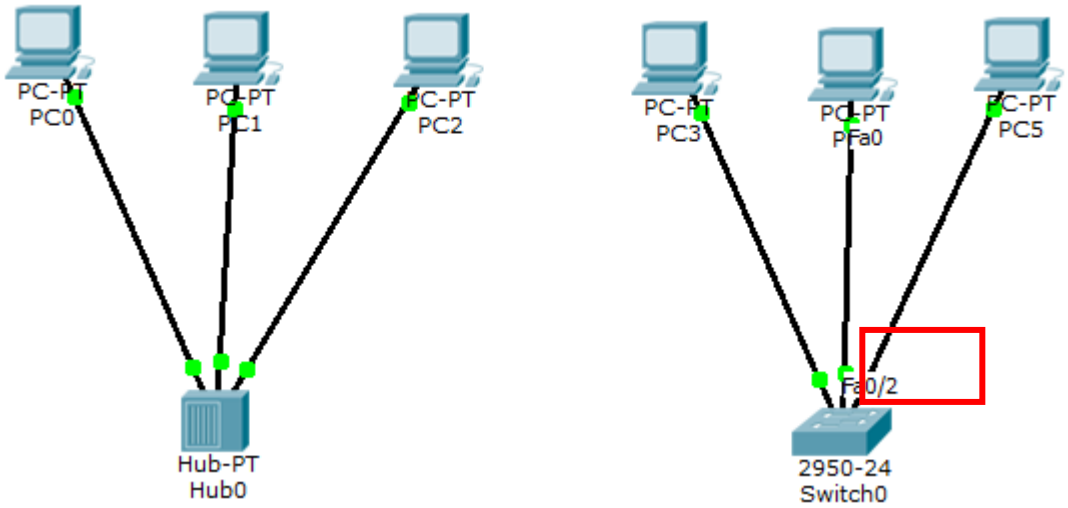


Рис. 13. Вид робочої області

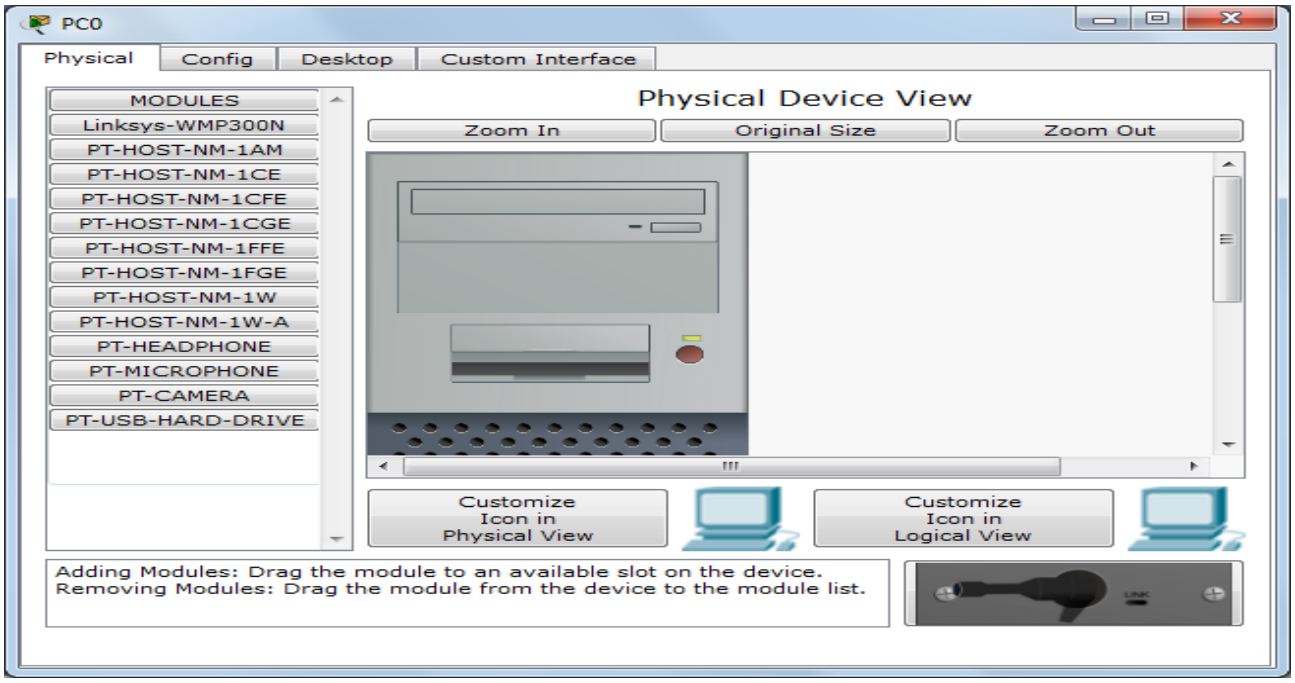


Рис. 14. Вкладка Physical кінцевого обладнання (комп'ютера)

Фізичний вид обладнання ми міняти не будемо, тому відразу переходимо до Налаштування у вкладці Config (рис. 15).

Саме тут ви можете змінити назву PC0 (наприклад, увести Ip-адресу цього комп'ютера, щоб не підглядати його щораз у налагодженнях). Крім того, тут ви можете вказати Ip-адресу шлюзу, також відомий як шлюз за замовчуванням, і Ip-адресу Dns-Сервера. Ми обговоримо це пізніше, але це буде Ip-адреса локального маршрутизатора. Якщо ви прагнете, ви можете ввести Ip-адресу шлюзу 192.168.1.1 і Ip-адреса Dns-Сервера 192.168.1.100, хоча він не буде використовуватися в цій лабораторній роботі.

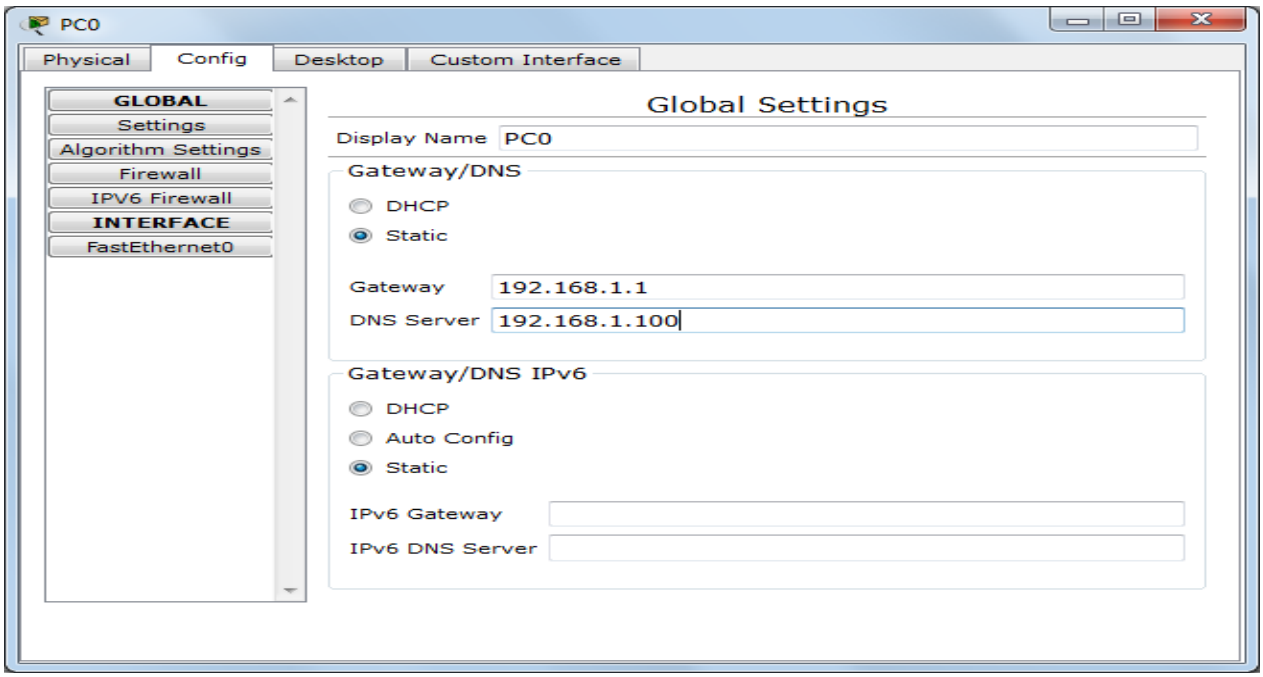


Рис. 15 Вкладка Config кінцевого обладнання (комп'ютера)

Кликніть мишею на інтерфейсі Fastethernet (рис. 16). Укажіть Ip-адресу комп'ютера 192.168.1.10. Натисніть на поле для введення маски підмережі, вона визначиться автоматично 255.255.255.0.

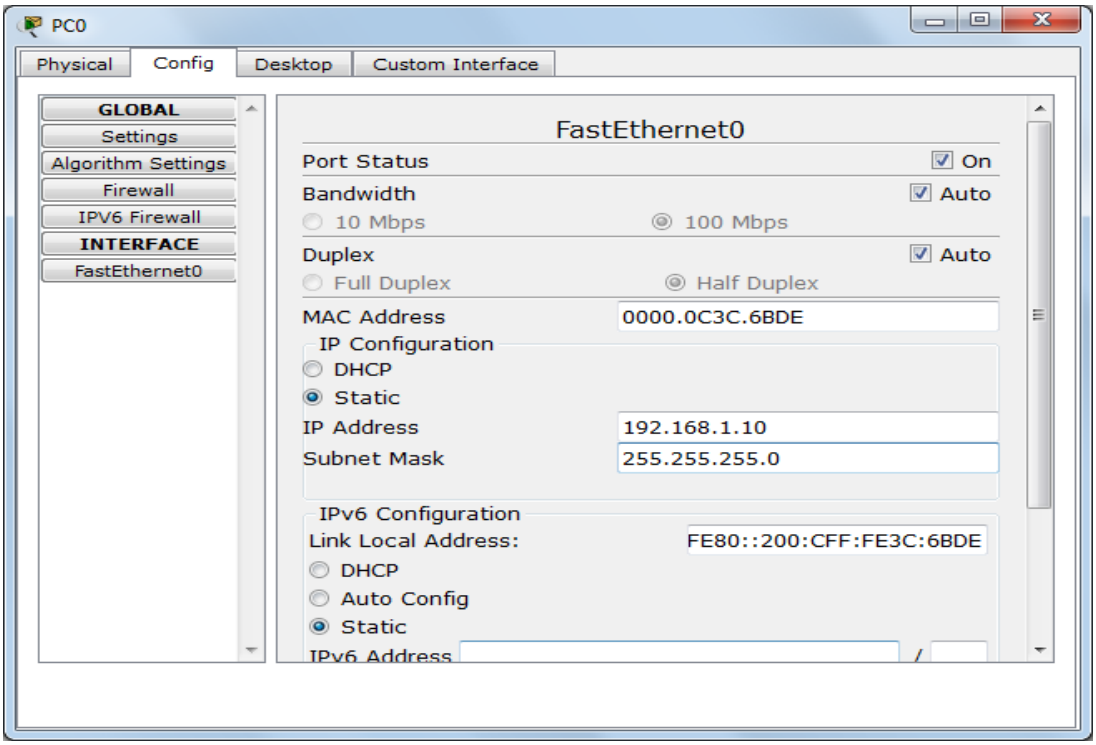


Рис. 16. Налаштування інтерфейсу кінцевого обладнання

Інформація автоматично зберігається після введення.

Закрийте вікно Налаштування PC0 і повторіть зазначені вище дії для інших вузлів мережі, використовуючи інформацію про Ip-Адреси і маски підмережі, представлену в таблиці 1.

Таблиця 1

Інформація про Ip-адреси і маски підмережі

Хост	Ip-адреса	Маска підмережі
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
PC2	192.168.1.12	255.255.255.0
PC3	192.168.1.13	255.255.255.0
PC4	192.168.1.14	255.255.255.0
PC5	192.168.1.15	255.255.255.0

Після налаштування вузлів робоча область симулятора буде виглядати в такий спосіб, якщо навести вказник мишки на один із кінцевих вузлів (рис. 17):

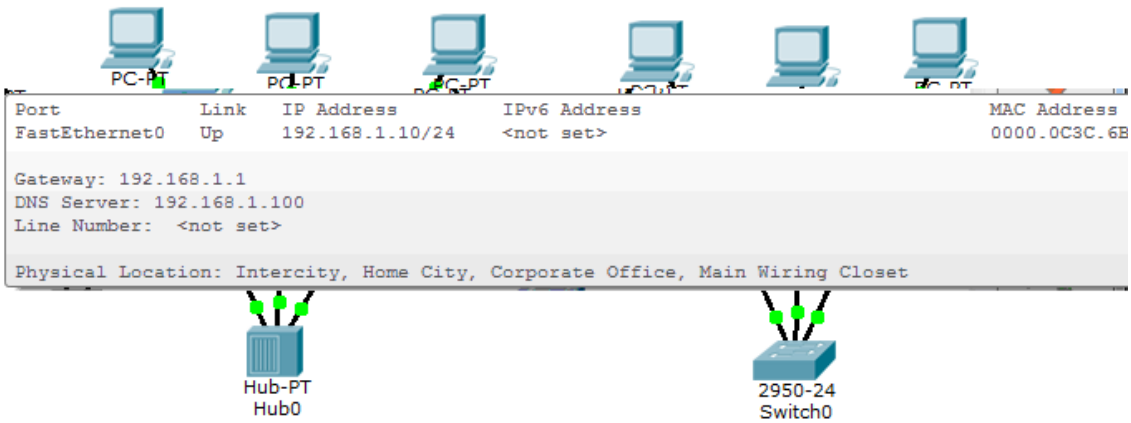


Рис. 17. Перевірка налаштувань кінцевого обладнання (комп'ютера)

Якщо при побудові мережі які-небудь обладнання або зв'язки виявилися зайвими, їх можна вилучити за допомогою інструмента Delete на бічній панелі симулятора (Common Tools Bar). Для видалення потрібно клацнути один раз на інструмент Delete, потім на елемент мережі.

4. З'єднання концентратора й комутатора

Для підключення такого типу обладнань, як комутатора й концентратора, використовується перехресний кабель (рис. 18).

Рис. 18. Вибір з'єднання

Для підключення Hub1 до Switch0 виконайте наступні дії:

1) Клацніть один раз на Hub0, виберіть порт 3 (рис. 19).

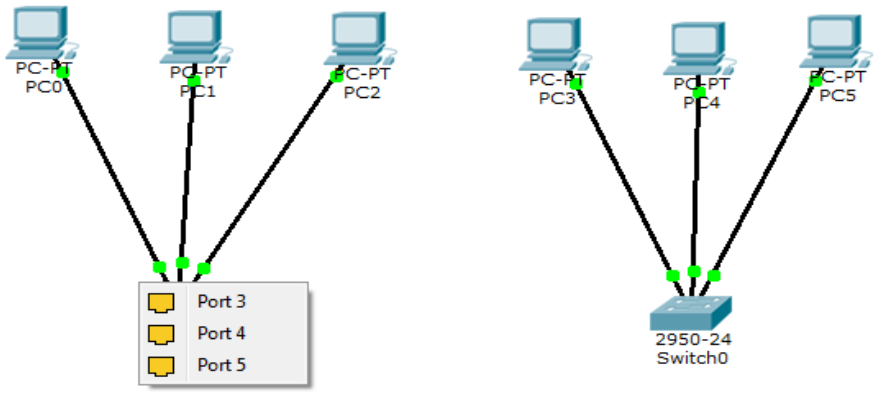


Рис. 19. Вид робочої області

2) Перемістіть курсор на Switch0, клацніть на ньому мишею й виберіть інтерфейс Fastethernet0/4 (рис. 20).

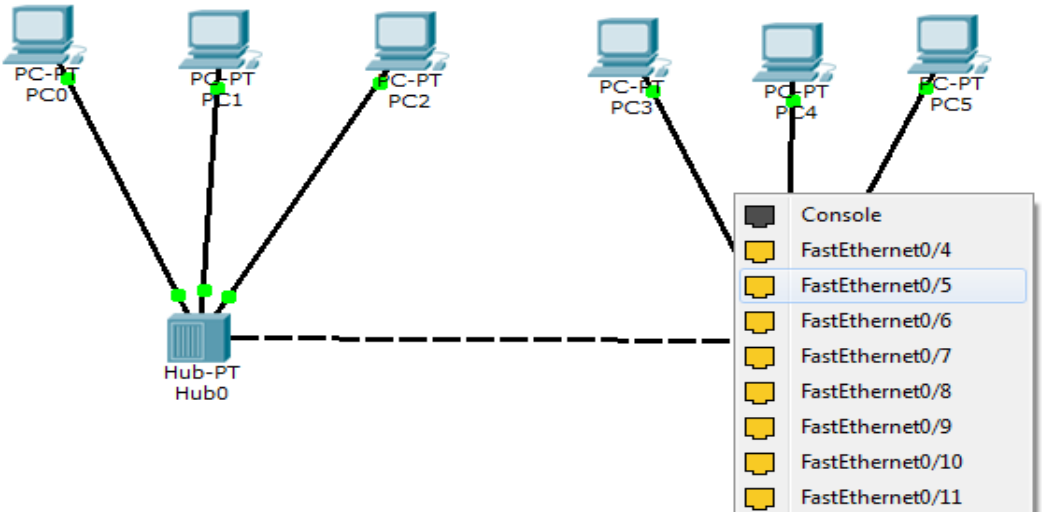


Рис. 20. Вид робочої області

3) Коли обоє обладнання будуть готові до роботи, індикатори стану стануть зеленими (рис. 21).

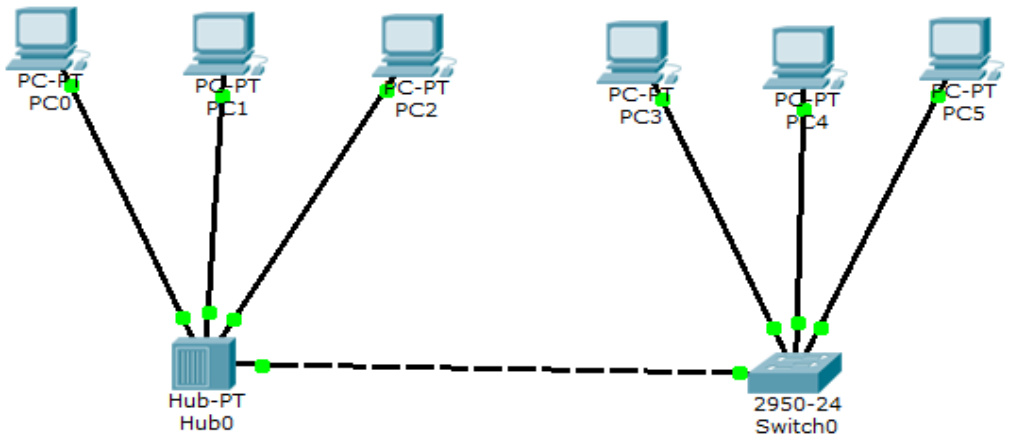


Рис. 21. Вид робочої області

Сформуємо простий пакет ping-запиту для перевірки роботи мережі, скориставшись Add Simple PDU. Натисніть один раз на Add Simple PDU (рис. 22).

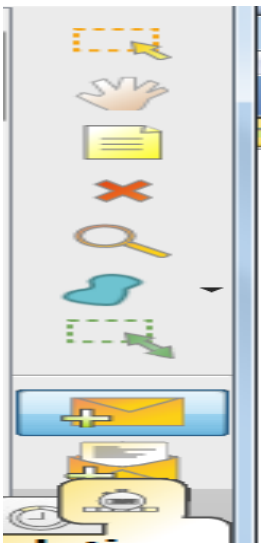


Рис. 22. Add Simple PDU

Тепер потрібно вибрати два вузли: джерело й приймач ping-запиту. Наведіть курсор на PC0 (192.168.1.10) і клацніть на ньому мишею (джерело ping-запиту), потім перемістіть курсор на PC3 (192.168.1.15) (приймач ping-запиту) і кликніть на ньому (рис. 23).

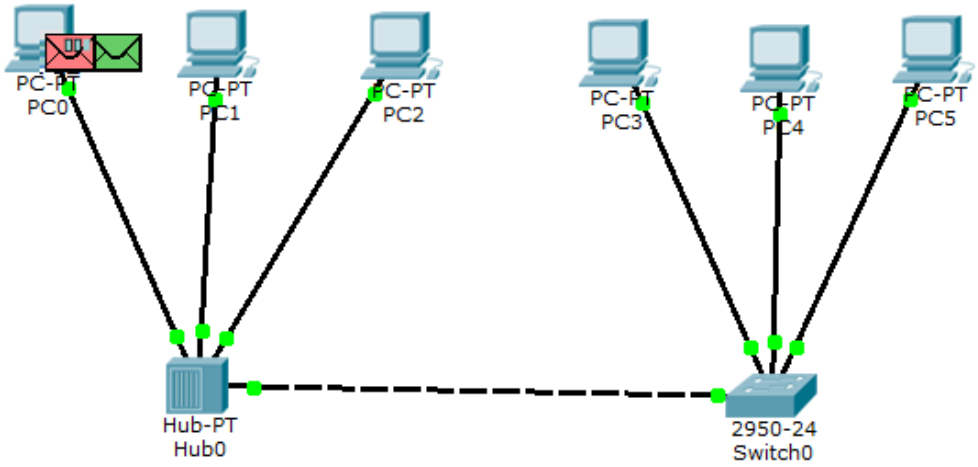


Рис. 23. Початок проходження ping-запиту

Тому що всі інтерфейси й зв'язку мережі налагоджені правильно (про що говорять зелені індикатори стану), то ping-запит повинен пройти успішно. У вікні керування пакетами User Created Packet Window з'явиться відповідний запис (рис. 24).

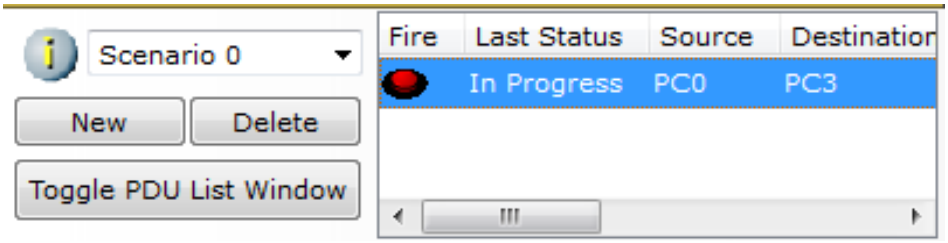


Рис. 24. Вікно керування пакетами

Важливо: змініть Ip-Адресу 192.168.1.13 вузла PC3 на Ip-Адресу 192.168.2.13, з тою ж маскою підмережі 255.255.255.0. Виконаєте ping-запит від PC0 до PC3. Який вийшов результат? Які причини?

Щоб очистити список виконаних операцій моделювання, необхідно вилучити відповідний сценарій симуляції.

Натисніть на кнопку Delete на панелі User Created Packet Window (рис. 25).

Рис. 25. Вікно керування пакетами

Усі записи сценарію видаляться.

5. Збереження створеної топології

Виберіть в Menu вкладку **File**, далі **Save as.** Виберіть відповідну директорію. Усі файли симулятора Cisco Packet Tracer мають розширення .pkt.

1.2. Побудова топології мережі, що складається із двох підмереж

У результаті першої роботи ми вивчили основні операції з обладнаннями. Самостійно побудувати мережу, яка складається з двох підмереж (рис. 26).

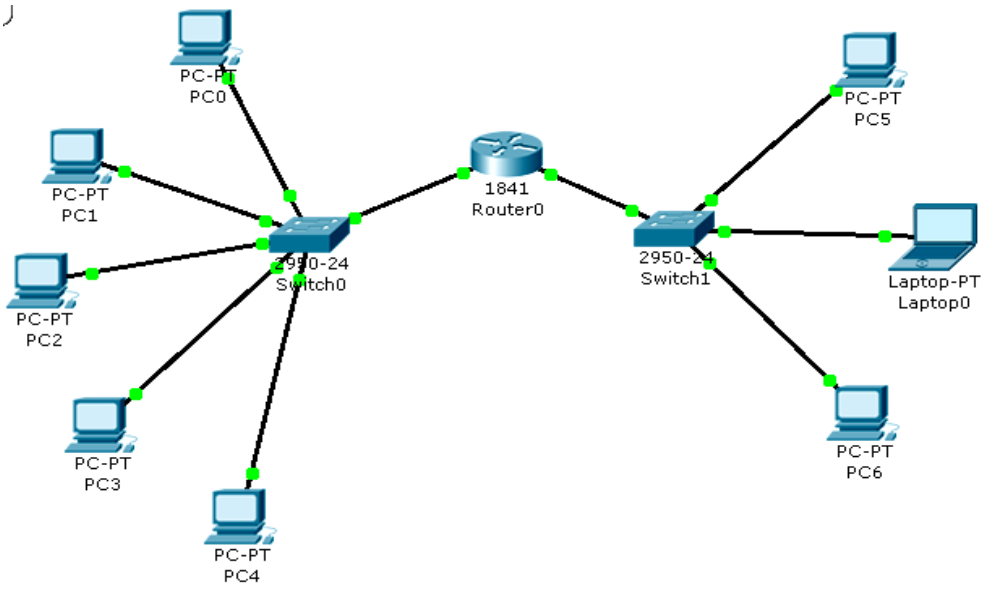


Рис. 26. Топологія мережі

Для створення такої топології потрібно додати в робочу область симулятора кінцеві вузли, два комутатори й маршрутизатор. При додаванні маршрутизатора виберіть модель 1841, тому що вона має два інтерфейси. Опис маршрутизаторів серії 1841 можна знайти на сайті компанії Cisco Systems. [Електронний ресурс]. URL: http://www.cisco.com/en/US/products/ps5875/index.html. При з'єднанні обладнань між собою скористайтеся мідним кабелем із прямим підключенням.

2. Контрольні питання

1. Які групи встаткування існують в Cisco Packet Tracer?
2. Які види обладнань і з'єднань існують в Cisco Packet Tracer?
3. Який порядок роботи з обладнанням в Cisco Packet Tracer?
4. Який порядок підключення вузлів в Cisco Packet Tracer?
5. Як налаштувати Ip-Адреси й маски підмережі на хостах?
6. Як проводиться перевірка працездатності мереж та їх складових?
7. Як проводиться збереження створеної топології?
8. Які особливості створення мереж з декількох підмереж?

ЛАБОРАТОРНА РОБОТА 21. КЛОНУВАННЯ РОБОЧИХ СТАНЦІЙ

Мета роботи: опанувати навичками створення образів жорстких дисків робочих станцій і розгортання образа в локальній або корпоративній мережі за допомогою пакета програм Ghost.

Зміст

1. Хід роботи
1.1. Установка програми GHOST на сервер
1.2. Створення завантажувальної дискети
1.3. Створення образу диска
1.4. Розгортання образу диску
2. Контрольні питання

1. Хід роботи

1.1. Установка програми GHOST на сервер

Symantec Ghost Solution Suite – це програмний продукт для створення й розгортання образів для настільних комп'ютерів, ноутбуків, планшетів і серверів. До складу Ghost Solution Suite входить консоль Deployment Solution разом з основними технологіями розгортання ОС, міграції й керування на різних платформах. У комбінації з базовими функціями Ghost Solution Suite такими як Ghost Cast Server і Deployanywhere, продукт Ghost Solution Suite прискорює й спрощує процес створення й розгортання образів.

1) З компакт-диска запустіть програму **Setup.exe** установки Symantec Ghost Solution Suite**.**

2) Перейдіть до другого вікна майстра.

3) Ознайомившись із умовами ліцензійної угоди, перейдіть до наступного вікна майстра.

4) У вікні **Choose Installation Type** укажіть опцію **Standard Tools Only**.

5) У наступнім вікні введіть ім'я користувача, організацію, поштову адресу й серійний номер. Серійний номер перебуває в каталозі з інсталяційним пакетом Ghost.

6) У вікні вибору каталогу для установки погодитеся зі значенням за замовчуванням.

7) У вікні вибору складу встановлюваних компонентів погодитеся із запропонованим списком і перейдіть до останнього вікна майстра установки.

8) Клацніть на **Install** для процесу установки.

1.2. Створення завантажувальної дискети

Завдання. Потрібно створити завантажувальну дискету, яка дозволить створити образ жорсткого диска.

1) Запустіть утиліту **Ghost Boot Wizard** програмної групи **Symantec Ghost** меню **Пуск**.

2) У першім вікні після запуску пропонується вибрати спосіб створення образа. Виберіть пункт **Network Boot Disk**.

3) У наступнім вікні відображається список уже відомих програмі драйверів мережевих карт. Натисніть клавішу **Add.** З'явиться діалогове вікно, що пропонує вибрати тип драйвера. Установіть перемикач у позицію **Packet Driver** і натисніть **OK.**

4) На вкладці **Packet Driver** клацніть на **Browse**. Укажіть драйвер внутрішньої мережевої карти, розташований у каталозі **PKT**. Привласніть параметру **Parameters** значення **0x60**, виберіть для **Multicasting Mode** режим **Receive Mode 6**. Клацніть на **OK.**

5) Змініть назву доданого елемента на **RLT100ATX**. Перейдіть до наступного вікна.

6) У наступнім вікні пропонується вибрати тип завантажувальної дискети. Виберіть опцію **Symantec Ghost**. Перейдіть до наступного вікна.

7) На наступному кроці пропонується вказати параметри мережі. Установіть перемикач **The IP settings will be statically defined** і вкажіть наступні параметри:

• **First IP address – 192.168.1.11**;

• **Subnet mask – 255.255.255.0**;
• **Gateway – 192.168.1.1;**
• **Router hops – 10**.

8) Далі пропонується вибрати дисковід і ввести кількість дискет, яка необхідно створити. Вставте дискету в дисковід і клацніть на **Далее**.

9) З'явиться інформаційне вікно в якім повідомляється про обрані параметри. Клацніть на **Далее**.

10) Проведіть форматування дискети й закрийте вікно майстра форматування дисків.

1.3. Створення образу диска

Завдання. Потрібно створити образ диска робочої станції.

1) На сервері запустіть утиліту **Multicast Server** програмної групи **Symantec Ghost** меню **Пуск**.

2) Виберіть опцію **Dump From Client**, укажіть назву файлу, у якім буде зберігатися образ, наприклад **image.gho**, і місце розташування **C:\Users\Software\Img**. У цьому ж вікні вкажіть ім'я сесії **session_1**, установіть перемикач **Disk** і вкажіть номер диска **1**. Клацніть на **Accept Client**.

3) На робочій станції завантажтеся з дискети. Після закінчення завантаження клацніть на **OK**. У меню виберіть **Multicast**.

4) Уведіть ім'я сесії **session_1**.

5) У наступнім вікні погодитеся із запропонованим варіантом і клацніть на **OK**.

6) Далі необхідно режим стиску. Виберіть **High**.

7) У наступнім вікні клацніть на **Yes**.

1.4. Розгортання образу диску

Завдання. Потрібно розгорнути на робочій станції підготовлений образ.

1) На сервері запустіть утиліту **Multicast Server** програмної групи **Symantec Ghost** меню **Пуск**.

2) Виберіть опцію **Load to Client**, укажіть назву файлу **image.gho**, у якім зберігається образ, і місце розташування **C:\Users\Software\Img**. У цьому ж вікні введіть ім'я сесії **session_1**, клацніть на **More Options** і привласніть параметру **Client count** значення **1**. Клацніть на **Accept Client**.

3) На робочій станції завантажитеся з дискети. Після закінчення завантаження клацніть на **OK**. У меню виберіть **Multicast**.

4) Уведіть ім'я сесії **session_1**.

5) У наступнім вікні погодитеся із запропонованим варіантом і клацніть на **OK** і далі, погодившись із розмірами дисків, клацніть ще раз на **OK**.

6) У наступнім вікні клацніть на **Yes**.

1.5. Symantec Ghost 11.5

В версії Symantec Ghost 11.5 приведені раніше операції можна виконати в наступній послідовності:

1. Створення образу диска

Вводимо **Local.** Вибираємо **Partition**. Вибираємо пункт **To Image.** Це означає, що ми прагнемо зберегти розділ в образ (рис. 1)

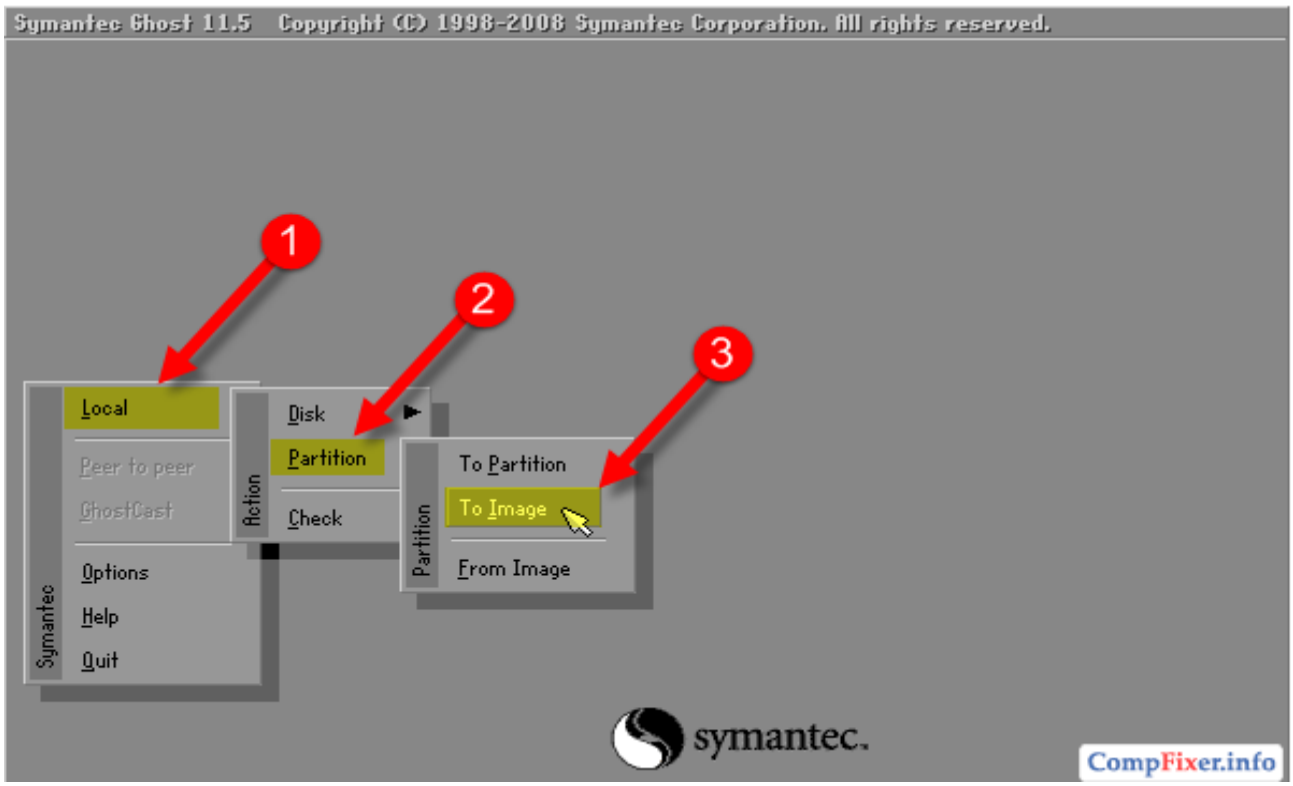


Рис. 1. Вибір початкових команд

Виберіть фізичний диск.Натисніть **ОК** (рис. 2)

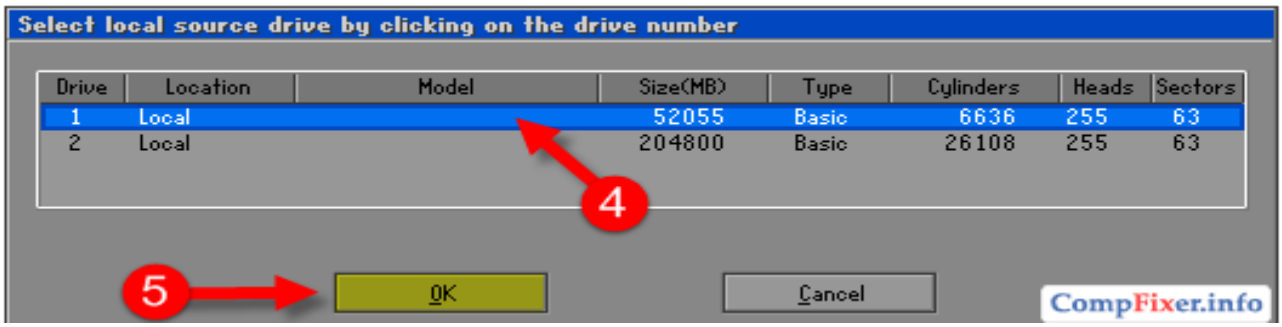


Рис. 2. Відбір фізичного диску

Виберіть розділ.Натисніть **ОК** (рис. 3)

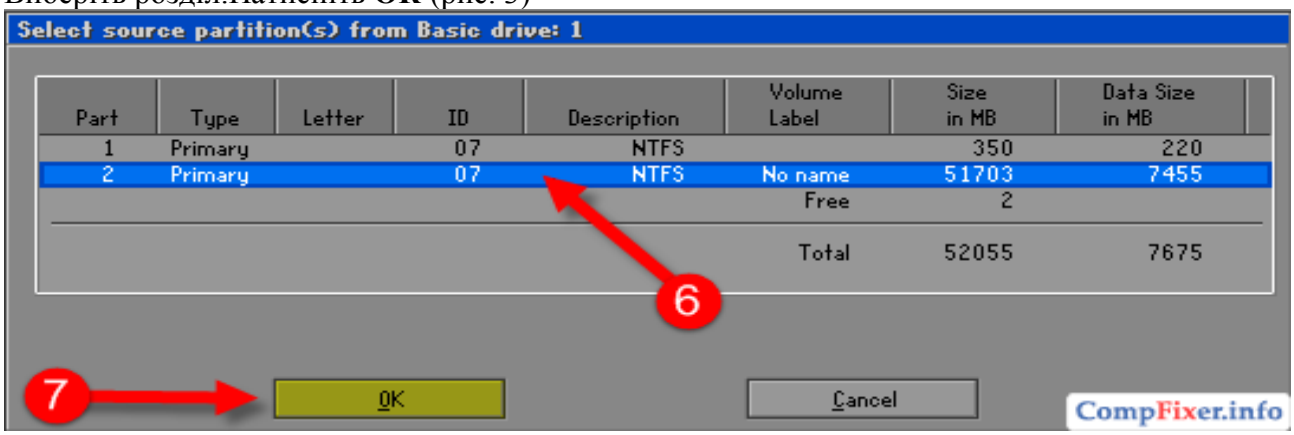


Рис. 3. Відбір розділу

У верхньому меню, що випадає, виберіть інший диск, куди ви прагнете помістити образ першого диска. У поле **File name** задайте ім'я файлу образу. Натисніть **Save** для збереження файлу, у який буде записуватися образ (рис. 4).

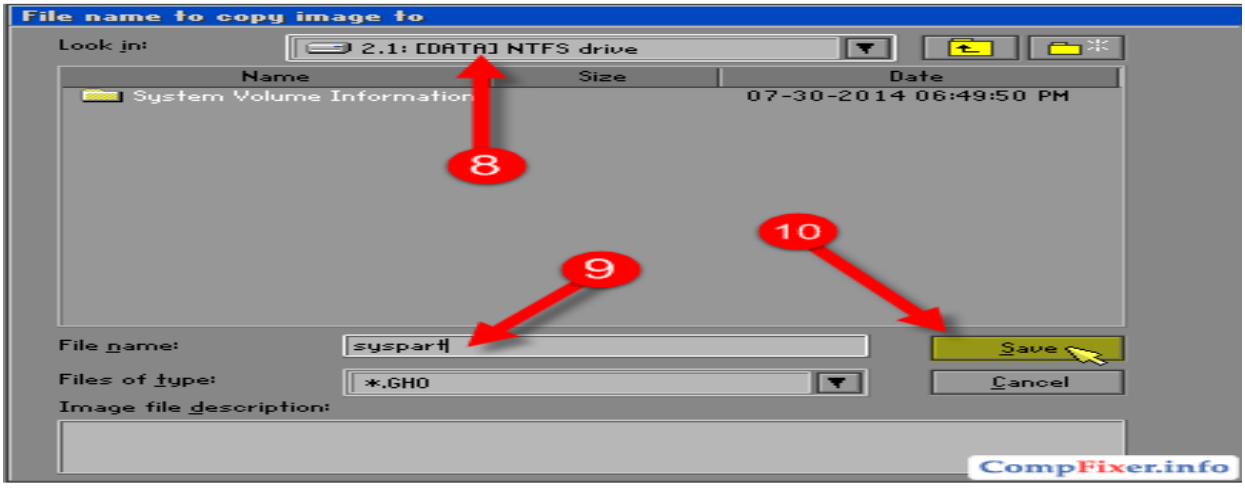


Рис. 4. Відбір диску для збереження образу

Виберіть ступінь стиску образу. Рекомендуємо вибирати **Fast** (рис. 5).

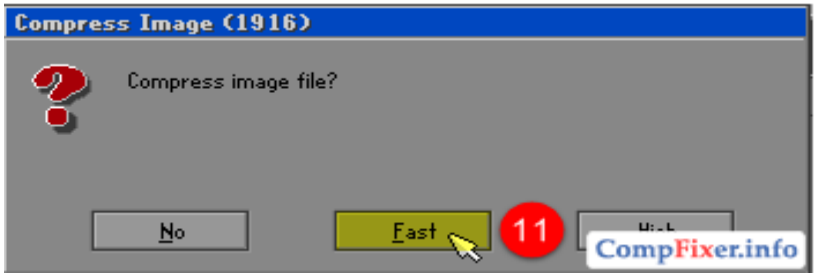


Рис. 5. Вибір ступеня стиснення

Відповідаємо **Yes** для продовження створення образу (рис. 6).

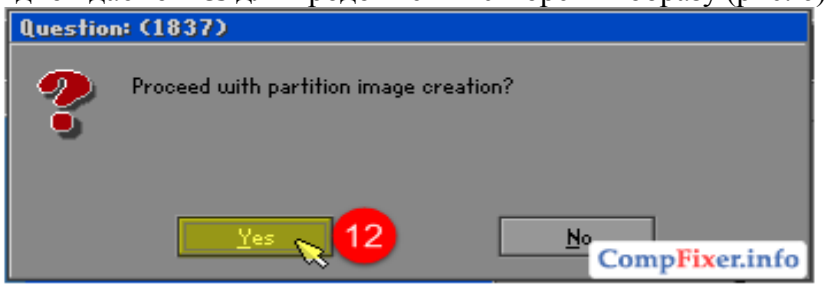


Рис. 6. Продовження створення образу

Іде процес створення образу. Дочекайтеся, коли прогрес дійде до 100% (рис. 7).

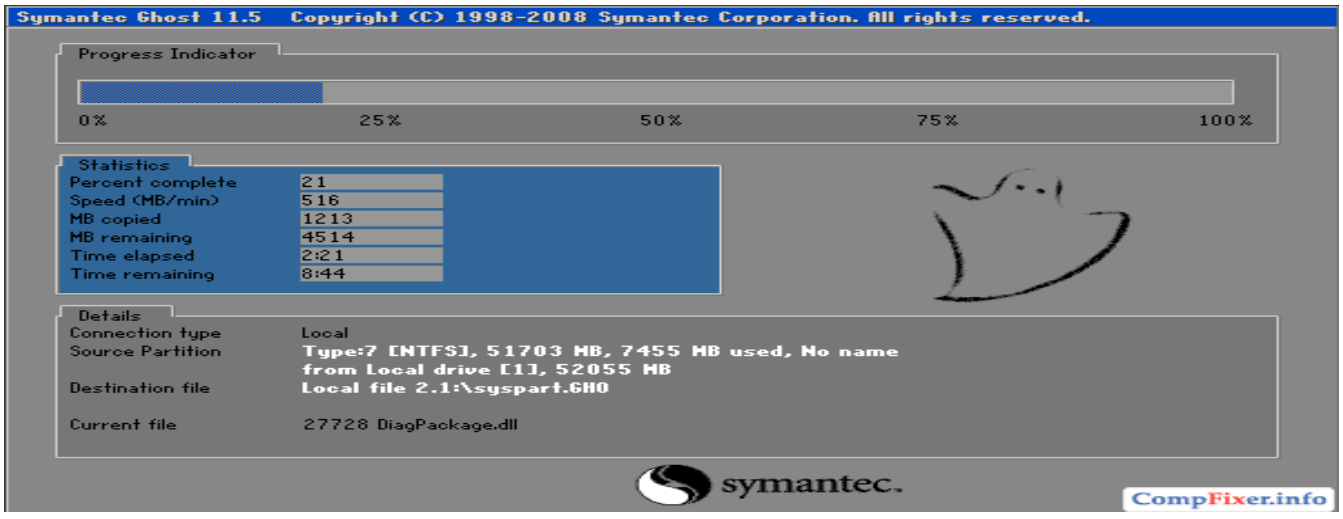


Рис. 7. Процес створення образу

За завершенням ви побачите таке повідомлення (рис. 8). Натисніть **Continue.**

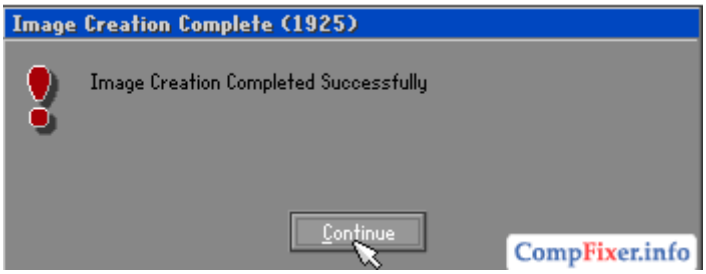


Рис. 8. Закінчення процесу

Тепер можна нажати на **Quit** і перезавантажити комп'ютер кнопкою RESET.

Відновлення розділу (диска) з образа

В головному меню програми натисніть **Local**. Виберіть пункт **Partition**. Виберіть **From Image** (рис. 9).

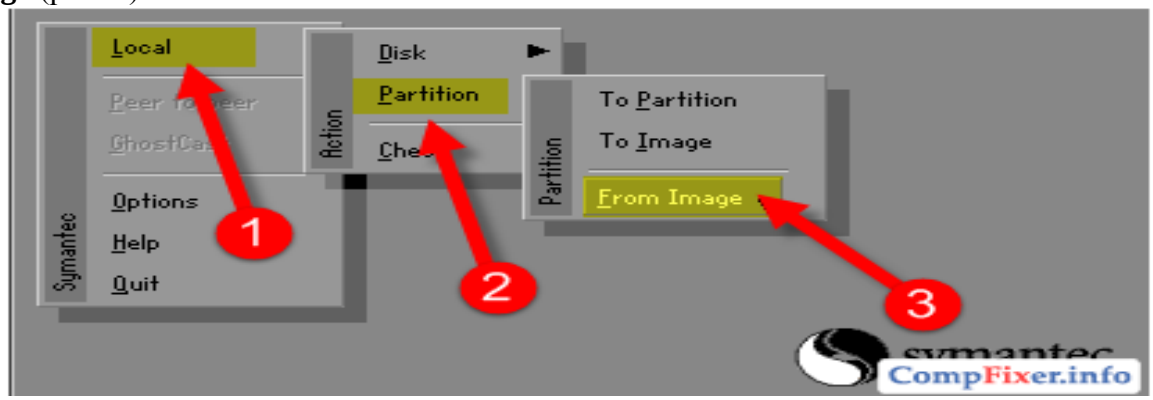


Рис. 9. Вікно відбору команд

Угорі в поле **Look In** виберіть локальний диск, що містить раніше створений у програмі Ghost образ розділу.Знайдіть потрібний файл образа. Він повинен мати розширення ***.GHO**. Натисніть на потрібний файл мишею для його вибору (кнопку **Open** натискати швидше за все не прийдеться) (рис.10).

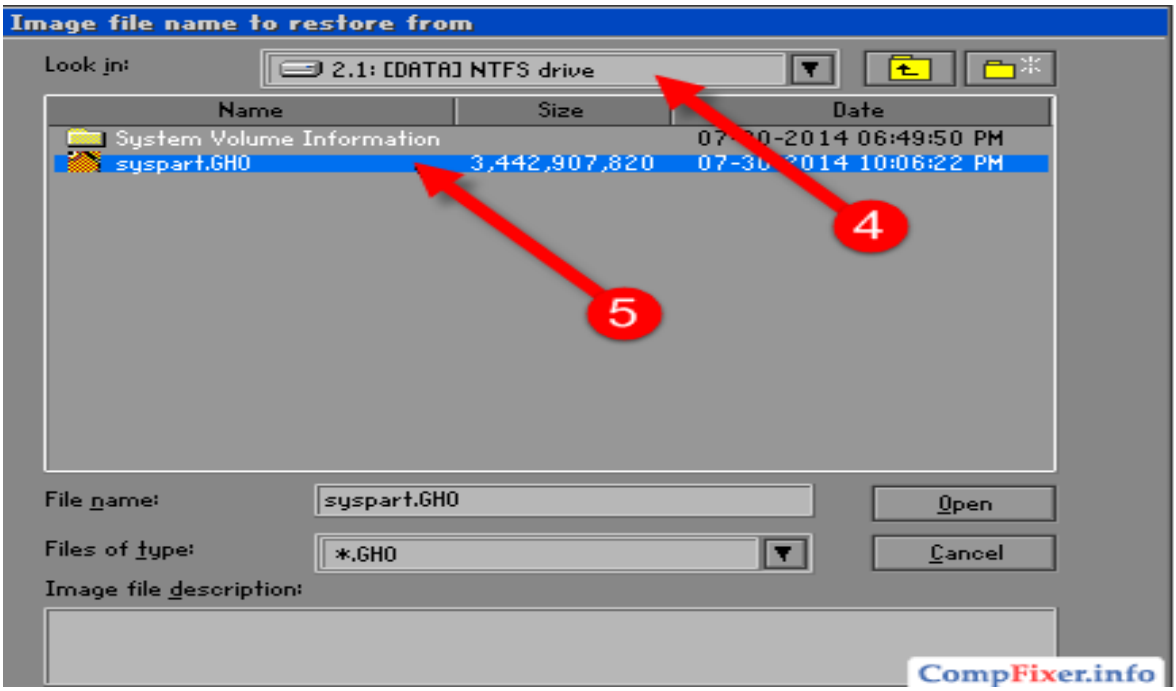


Рис. 10. Вибір диску

Виберіть вихідний розділ в образі. Потрібно нажати на нього мишею, навіть якщо він в списку один. Натисніть **ОК** (рис. 11).

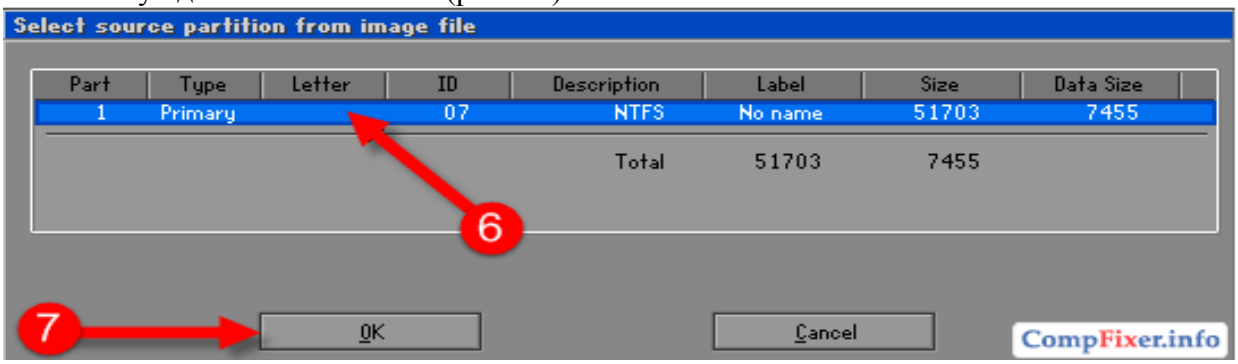


Рис.11. Вибір розділу

Виберіть фізичний диск, на який будемо відновлювати розділ. Натисніть **ОК** (рис.12).

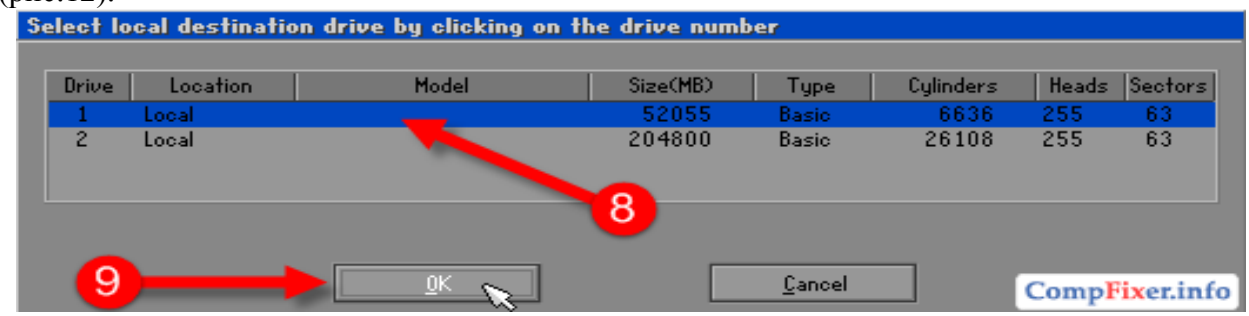


Рис. 12. Вибір диску

На обраному фізичному диску виберіть розділ, на який будемо розгортати образ (Іншими словами — потрібно вибрати розділ, який ви прагнете «відновити» або «перезаписати», як правило, це диск **C**). Натисніть **ОК** (рис. 13).

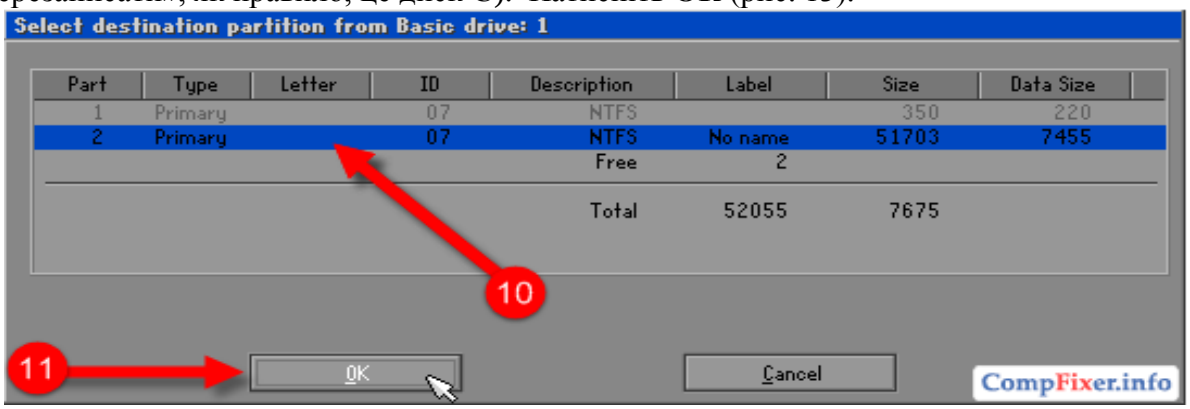


Рис. 13. Відбір розділу

Програма запитає «Продовжити з відновленням розділу? Цільовий розділ буде безповоротно перезаписаний.». Відповідаємо **Yes** (рис. 14).

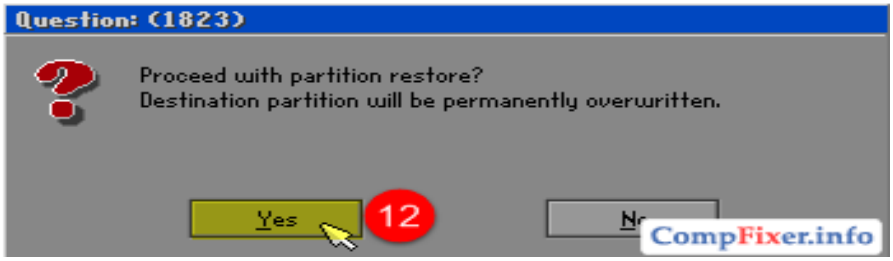


Рис.14. Підтвердження відновлення розділу

Після цього програма Ghost приступиться до відновлення розділу в зазначений розділ з образу (рис. 15).

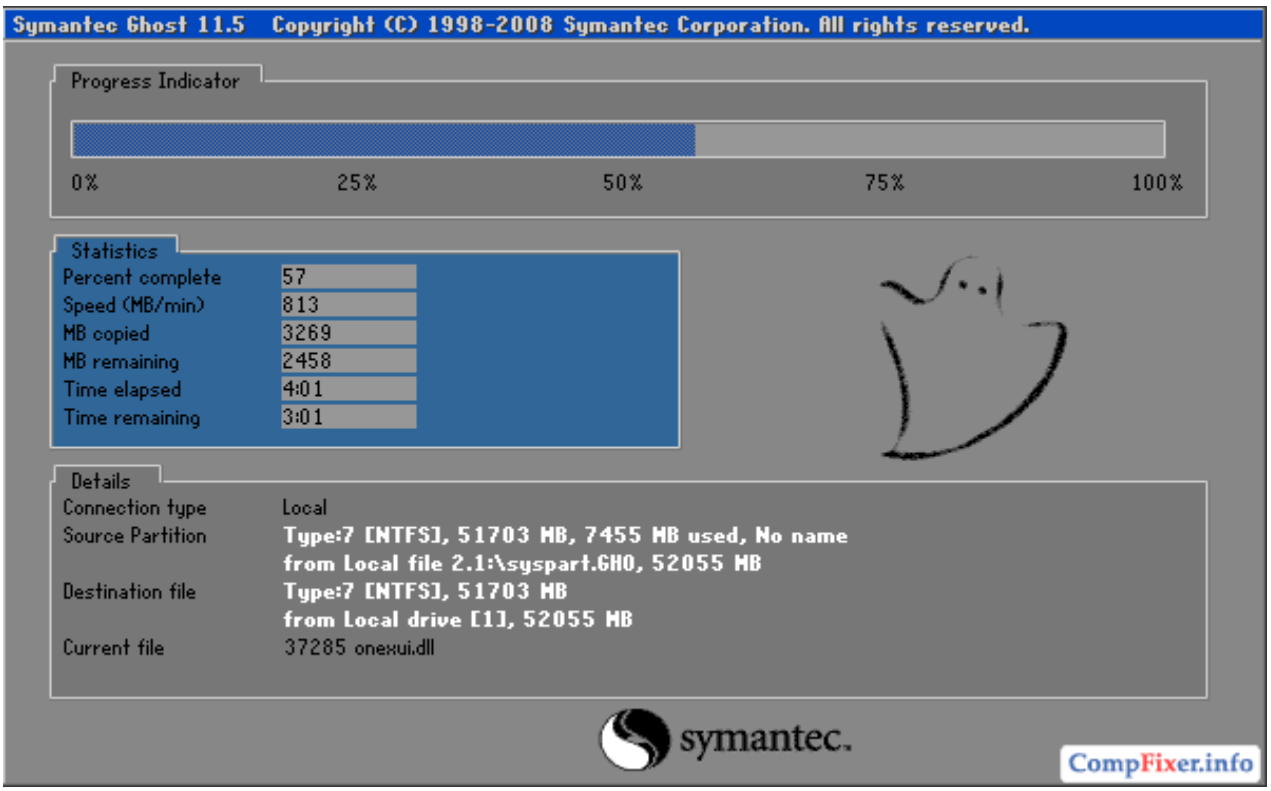


Рис. 15. Процес відновлення розділу

Натисніть кнопку **Reset Computer** для перезавантаження комп'ютера й перевірки результату (рис.16).

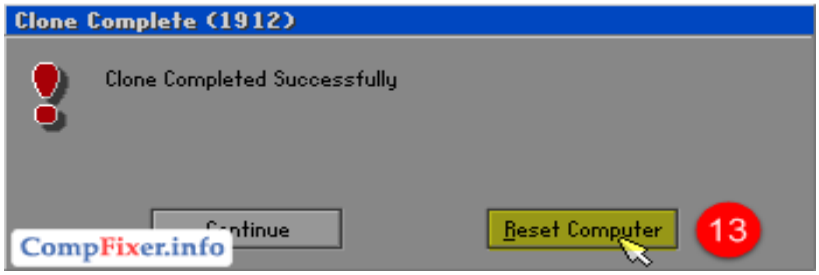


Рис. 16. Команда на перезавантаження комп'ютера

2. Контрольні питання

1. Як проводиться установка програми GHOST на сервер?
2. Як проводиться створення завантажувальної дискети?
3. Як проводиться створення образу диска?
4. Як проводиться розгортання образу диску?

РОЗДІЛ 3. ГЛОБАЛЬНІ МЕРЕЖІ

ЛАБОРАТОРНА РОБОТА 22. НАЛАГОДЖЕННЯ ПІДКЛЮЧЕННЯ ДО INTERNET В WINDOWS 10, D-LINK ТА CISCO

Мета роботи: практично відпрацювати налагодження підключення до Internet в Windows

Зміст

1. Хід роботи
1.1. Налагодження підключення до Internet в Windows 10
1.2. Налагодження підключення до Internet в D-Link
1.3. Налагодження підключення до Internet в CISCO
2. Контрольні питання

1. Хід роботи

1.1. Налагодження підключення до Internet в Windows 10

У певний час перед кожним користувачем постає питання налаштування мережі. Якщо ви домашній користувач – перед вами колись виникне завдання налаштування підключення до Інтернету, а якщо у вас в будинку кілька одиниць комп'ютерної техніки, то в кожному разі вам доведеться набудовувати кабельну або бездротову мережу, причому один комп'ютер повинен буде роздавати Інтернет на всі інші. У тому випадку, якщо ви працюєте системним адміністратором у невеликому офісі, вам потрібно буде налаштувати мережу зі статичними або динамічними адресами. Сучасні операційні системи з однієї сторони мають більший мережевий потенціал, але з іншої сторони з конфігурацією мережевих ситуацій розібратися можна. Оскільки ці системи більш доступні, вивчення яких, не дуже давно було прерогативою обмеженого кола осіб – мережевих адміністраторів.

Для Windows 10 можна розглядати наступні типи підключення:

- Налаштування звичайного з'єднання Ethernet. Підключення кабелю прямо від провайдера до комп'ютера, через роутер, або ADSL модем.
- Налаштування високошвидкісного з'єднання (Pppoe) в Windows 10.
- Підключення до Internet за Wi-Fi.
- Налаштування Internet через USB 3G/4G модем.

Почнемо напевно з Ethernet - дуже популярний спосіб підключення до Internet.

1.1.1. Ethernet: підключення до Internet в Windows 10 за мережевім кабелю (роутер, модем)

Розглянемо спочатку найпростіше з'єднання. Якщо у вас Internet-провайдер просто проклав мережевий кабель у будинок, і провайдер не надав логін і пароль для підключення до Internet, то у вас звичайне з'єднання за технологією Ethernet.

Точно так само налаштовується підключення до Internet в Windows 10 через роутер, або ADSL модем.

Для налаштування такого з'єднання досить підключити мережевий кабель від провайдера (роутера, або ADSL модему) до вашого комп'ютера (ноутбуку), у роз’єм мережної карти (рис. 1):

Рис. 1. Підключення кабелю

Якщо ж з'єднання з'явилося, але статус обмежено, або непізнана мережа, і Internet не працює, то потрібно перевірити параметри Ethernet адаптера (рис. 2).

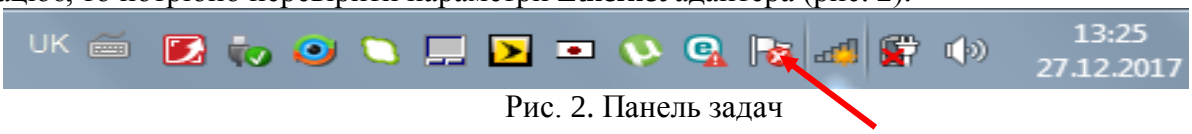


Рис. 2. Панель задач

F:\Users\Володя\AppData\Roaming\Microsoft\Đ□ Ñ□ Đ°ĐºÑ□ Đ¸Đ°Ñ□ Đ¼ Đ¼ĐµÑ□ ĐµĐ¶Ñ□\Đ□ Đ°Đº Đ½Đ°Ñ□ Ñ□ Ñ□ Đ¾Đ¸Ñ□ Ñ□ Đ¸Đ½Ñ□ ĐµÑ□ Đ½ĐµÑ□ Đ² Windows 10__files\Image-332.jpg

У Windows 10 це робиться так:

Натискаємо правою кнопкою миші на статус з'єднання з Internet, на панелі задач (рис. 2) і вибираємо пункт **Центр управления сетями и общим доступом** (рис. 3)**.** Далі, натисніть у новім вікні на пункт **Смена параметров адаптера**.

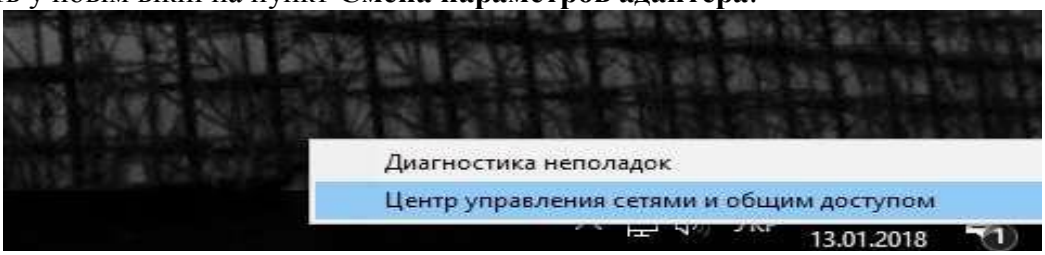


Рис. 3. Центр управління мережами

Натискаємо правою кнопкою миші на адаптер **Ethernet** і вибираємо **Свойства**. Виберіть у списку пункт **IP версії 4 (TCP/Ipv4)** вибираємо **Свойства**. Якщо прапорець біля цього пункту не встановлено, то обов'язково встановіть його, інакше Internet працювати не буде.

У новім вікні перевіряємо, що б були виставлені автоматичні налаштування одержання IP і DNS-Адрес, і натискаємо **Ok** (рис. 4)**.**

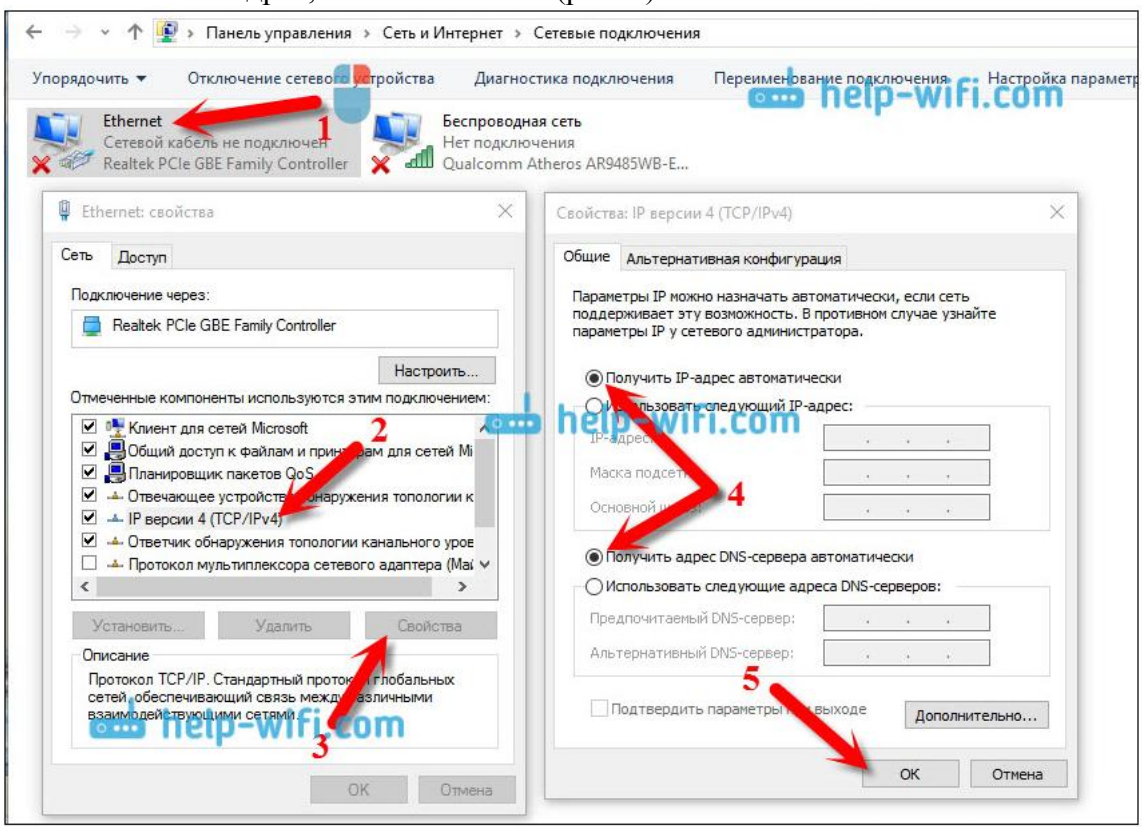


Рис. 4. Мережеві підключення

Internet уже повинен працювати. Якщо ні, то перезавантажте комп'ютер.

1.1.2. Налаштування високошвидкісного з'єднання (Pppoe) в Windows 10

Якщо у вас Internet провайдер проклав у будинок кабель, і надав вам логін, пароль, і можливо якісь інші дані для підключення до Internet, які потрібно задати в налаштуваннях комп'ютера, або Wi-Fi роутера, то вам на Windows 10 потрібно налаштувати Високошвидкісне з'єднання (Pppoe).

Відкриваємо **Центр управления сетями и общим доступом** (рис. 5)**:**

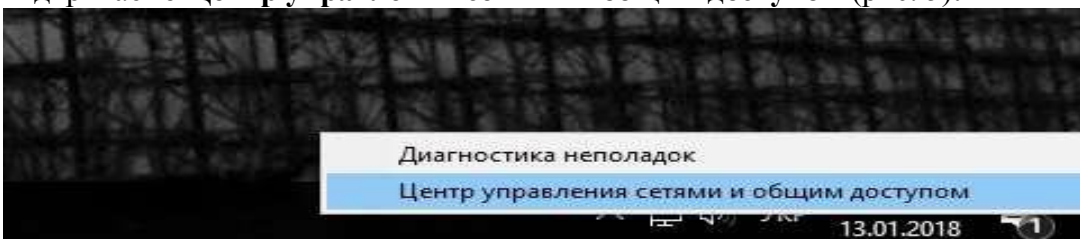


Рис. 5. Центр управління мережами і загальним доступом

Натискаємо на пункт **Создание и настройка нового соединения или сети**. Потім, виділяємо пункт **Подключение к Интернету**, і натискаємо на кнопку **Далее** (рис. 6)**.**

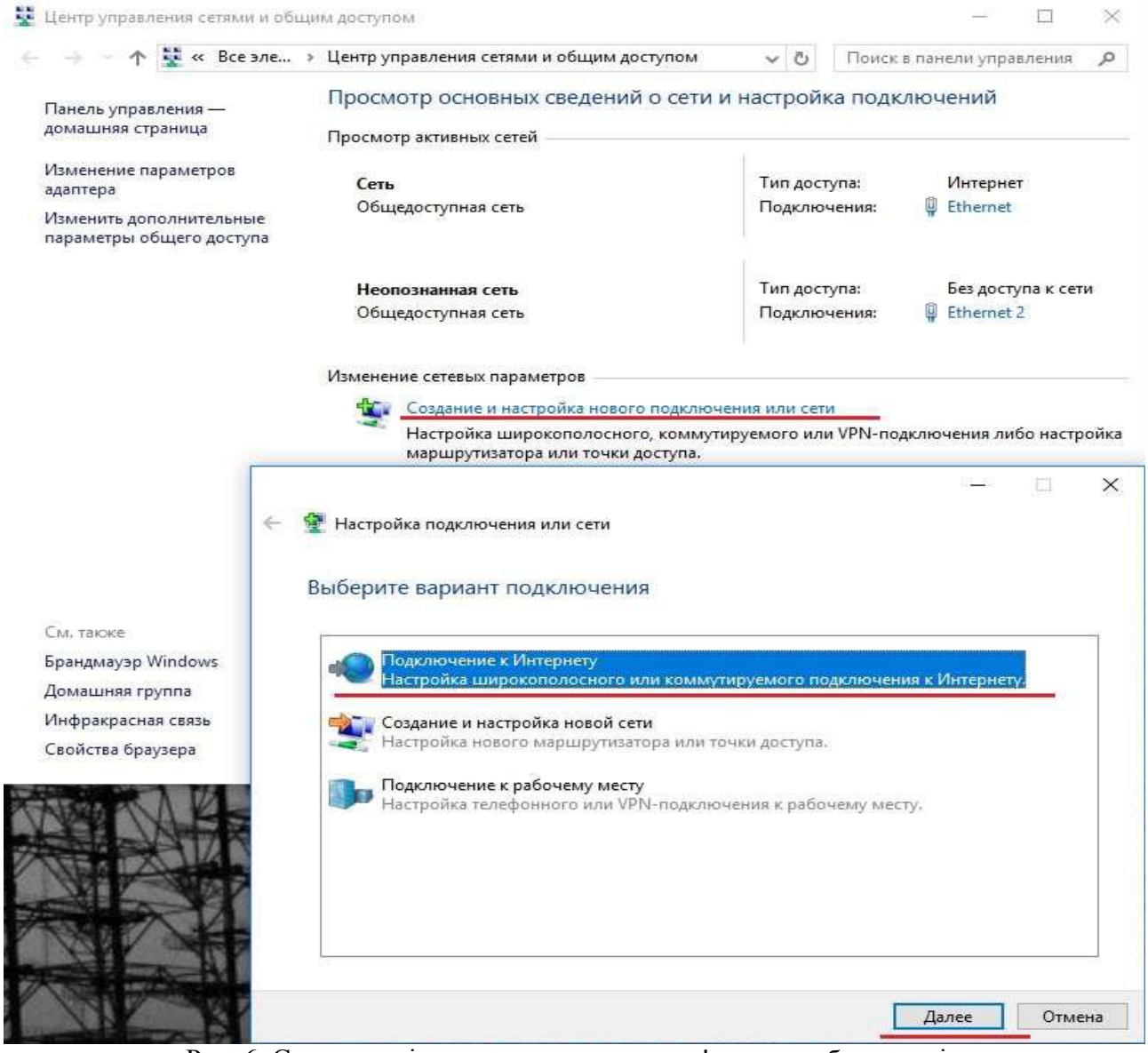


Рис. 6. Створення і налагодження нового з'єднання або мережі

У наступнім вікні вибираємо пункт: **Високошвидкісне (з PPPoE)**.

Далі, задаємо ім'я користувача й пароль, які вам повинен надати Internet-провайдер (рис. 7).

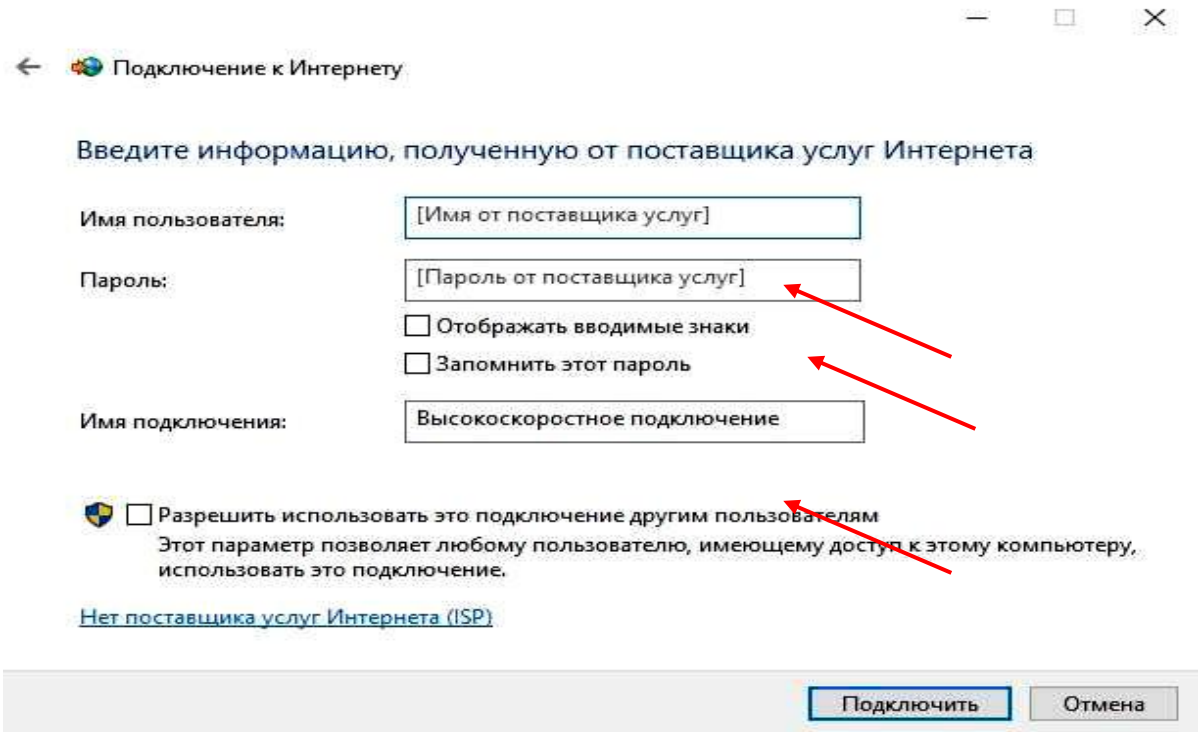


Рис. 7. Підключення до Internet

Натискаємо на кнопку **Подключить**, і якщо все правильно підключене, і правильно задані параметри, то буде створене підключення й установлене з'єднання з Internet.

Побачити це з'єднання й управляти їм, ви можете нажавши на значок Internet на панелі повідомлень (рис. 8).

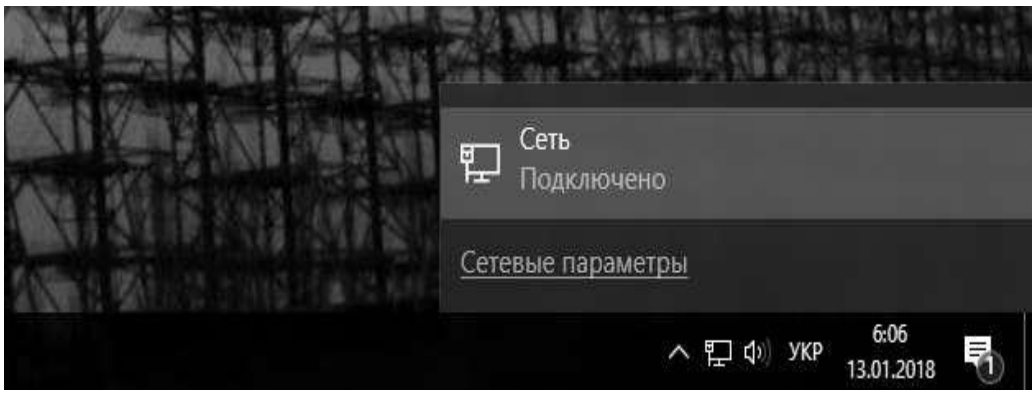


Рис. 8. Доступні з’єднання

Нажавши на з'єднання, відкриється меню **Набір номера**, де ви зможете підключитися, вилучити, або редагувати налаштування з'єднання.

1.1.3. Підключення до Internet за Wi-Fi

Якщо у вас будинку встановлений Wi-Fi роутер, або ви прагнете підключити свій ноутбук до Internet в друзів, у кафе і т.п., то можна використовувати для цієї справи Wi-Fi. Якщо у вас уже встановлений драйвер на Wi-Fi адаптер, а Windows 10 практично завжди встановлює його автоматично, то залишається тільки відкрити список доступних для підключення мереж, вибрати потрібну, указати пароль (якщо мережа захищена), і ви вже підключені до Internet (рис. 9).

F:\Users\Володя\AppData\Roaming\Microsoft\Đ□ Ñ□ Đ°ĐºÑ□ Đ¸ĐºÑ□ Đ¼ Đ¼ĐµÑ□ ĐµĐ¶Ñ□\Đ□ Đ°Đº Đ½Đ°Ñ□ Ñ□ Ñ□ Đ¾Đ¸Ñ□ Ñ□ Đ¸Đ½Ñ□ ĐµÑ□ Đ½ĐµÑ□ Đ² Windows 10__files\Image-3.jpg

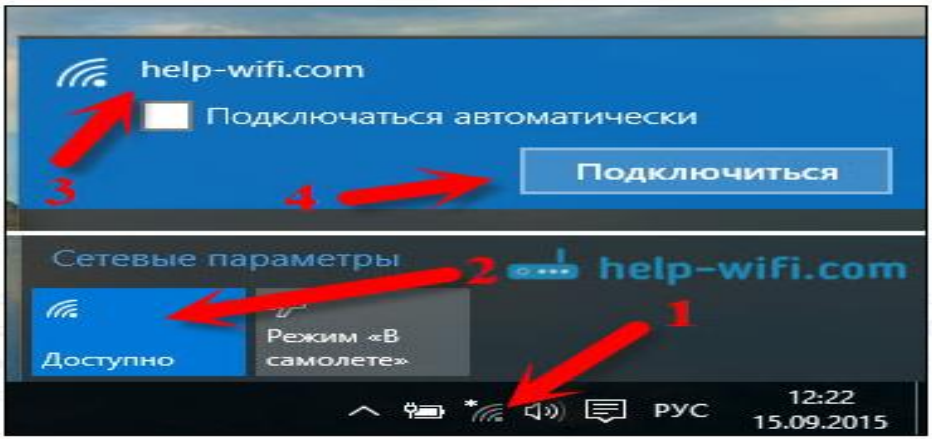


Рис. 9. Підключення до Internet

F:\Users\Володя\AppData\Roaming\Microsoft\Đ□ Ñ□ Đ°ĐºÑ□ Đ¸ĐºÑ□ Đ¼ Đ¼ĐµÑ□ ĐµĐ¶Ñ□\Đ□ Đ°Đº Đ½Đ°Ñ□ Ñ□ Ñ□ Đ¾Đ¸Ñ□ Ñ□ Đ¸Đ½Ñ□ ĐµÑ□ Đ½ĐµÑ□ Đ² Windows 10__files\Image-3.jpg

1.1.4. Налаштування Internet через 3G/4G модем в Windows 10

Залишилося тільки розглянути налаштування підключення через USB 3G, або 4G модем. Першою справою, нам потрібно підключити модем до комп'ютера й установити драйвер на наш модем.

Після того, як драйвер ви встановили, підключіть модем до комп'ютера, і можна приступати до налаштування 3G з'єднання на Windows 10.

Відкриваємо **Центр управления сетями и общим доступом** (рис. 10)**.**

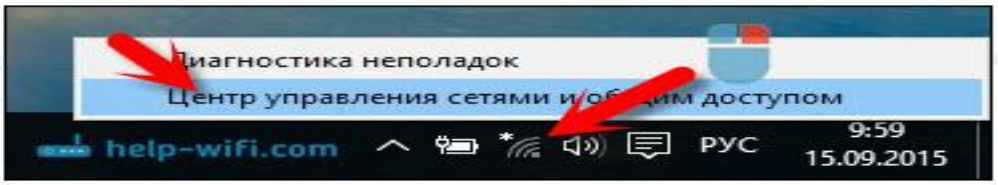


Рис. 10. Центр управления сетями и общим доступом

F:\Users\Володя\AppData\Roaming\Microsoft\Đ□ Ñ□ Đ°ĐºÑ□ Đ¸ĐºÑ□ Đ¼ Đ¼ĐµÑ□ ĐµĐ¶Ñ□\Đ□ Đ°Đº Đ½Đ°Ñ□ Ñ□ Ñ□ Đ¾Đ¸Ñ□ Ñ□ Đ¸Đ½Ñ□ ĐµÑ□ Đ½ĐµÑ□ Đ² Windows 10__files\Image-71.jpg

F:\Users\Володя\AppData\Roaming\Microsoft\Đ□ Ñ□ Đ°ĐºÑ□ Đ¸ĐºÑ□ Đ¼ Đ¼ĐµÑ□ ĐµĐ¶Ñ□\Đ□ Đ°Đº Đ½Đ°Ñ□ Ñ□ Ñ□ Đ¾Đ¸Ñ□ Ñ□ Đ¸Đ½Ñ□ ĐµÑ□ Đ½ĐµÑ□ Đ² Windows 10__files\Image-71.jpg

Натискаємо на **Создание и настройка нового соединения или сети** й вибираємо **Подключение к Интернету** (рис. 11)**.**

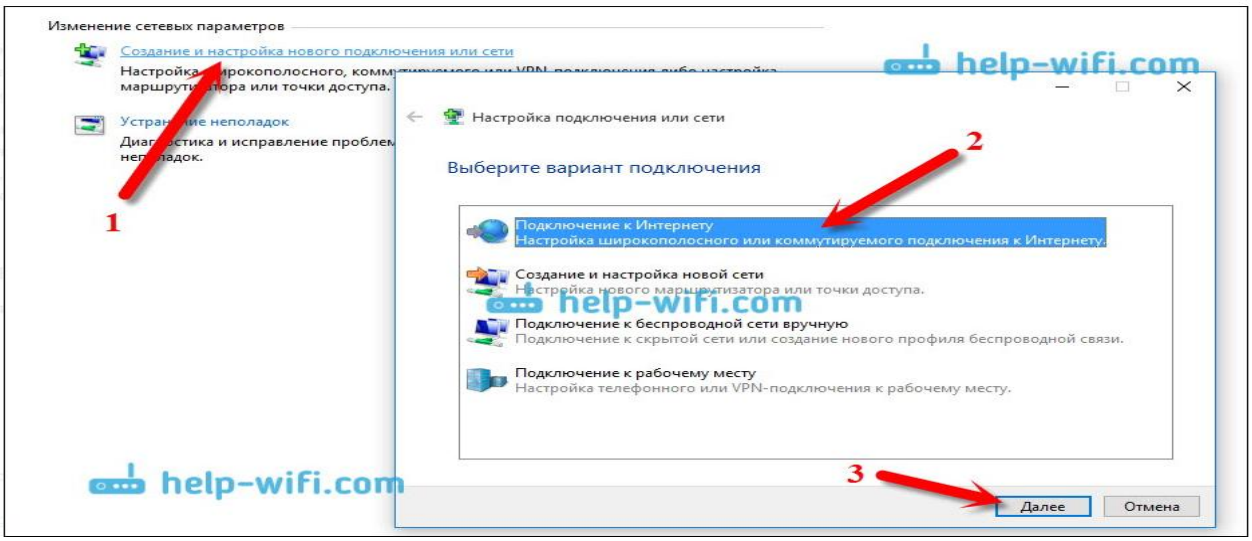


Рис. 11. **Подключение к Интернету**

Далі виберіть тип, **Коммутируемый** (рис. 12)**.**

І задаємо параметри, які надає провайдер: номер, ім'я користувача й пароль. Я показав на прикладі провайдера Інтертелеком (рис. 13). Рекомендую поставити галочку біля пункту Запам'ятати цей пароль. Ім'я підключення задаєте довільне. Як заповните всі поля, натискайте на кнопку **Создать.**

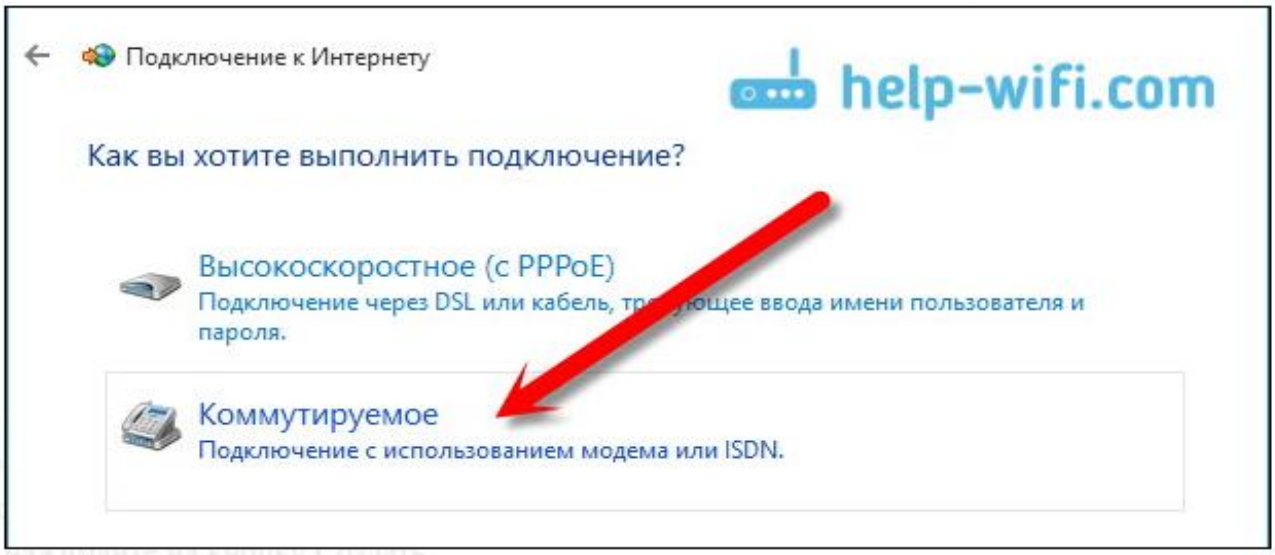


Рис. 12. Відбір з’єднання

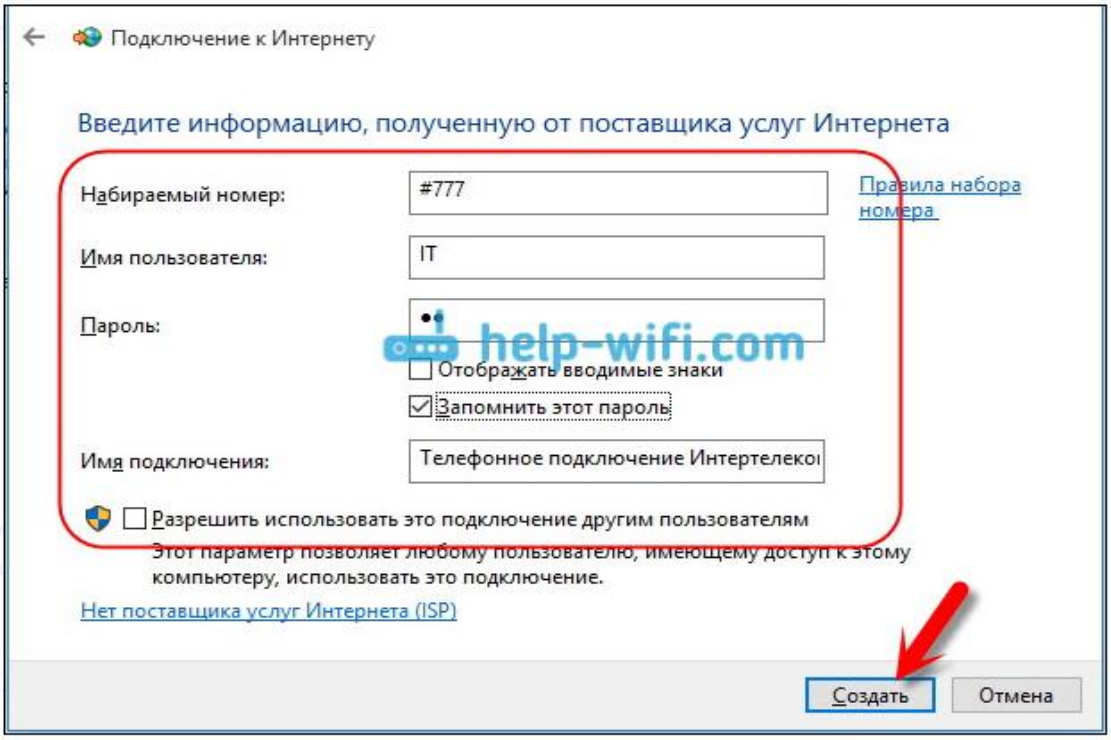


Рис. 13. Параметри з'єднання

Запускати створене підключення, зупиняти, вилучити, або відредагувати ви можете нажавши на значок підключення до Internet (рис. 14) й вибравши створене з'єднання.

Статус з'єднання з Internet, завжди відображається на панелі повідомлень. Нажавши на нього, можна відключиться від Internet, або запустити потрібне з'єднання.

1.2. Налагодження підключення до Internet в D-Link

Скидання налаштувань роутера проводиться шляхом натискання й утримання кнопки Reset на задній панелі роутера (рис. 15).

Налагодження рекомендується робити через web-інтерфейс. Для того щоб в нього ввійти, треба відкрити браузер (Internet Explorer або Mozilla Firefox) і ввести в адресному рядку **192.168.0.1**

У вікні, що з'явилося (рис. 16), уведіть:

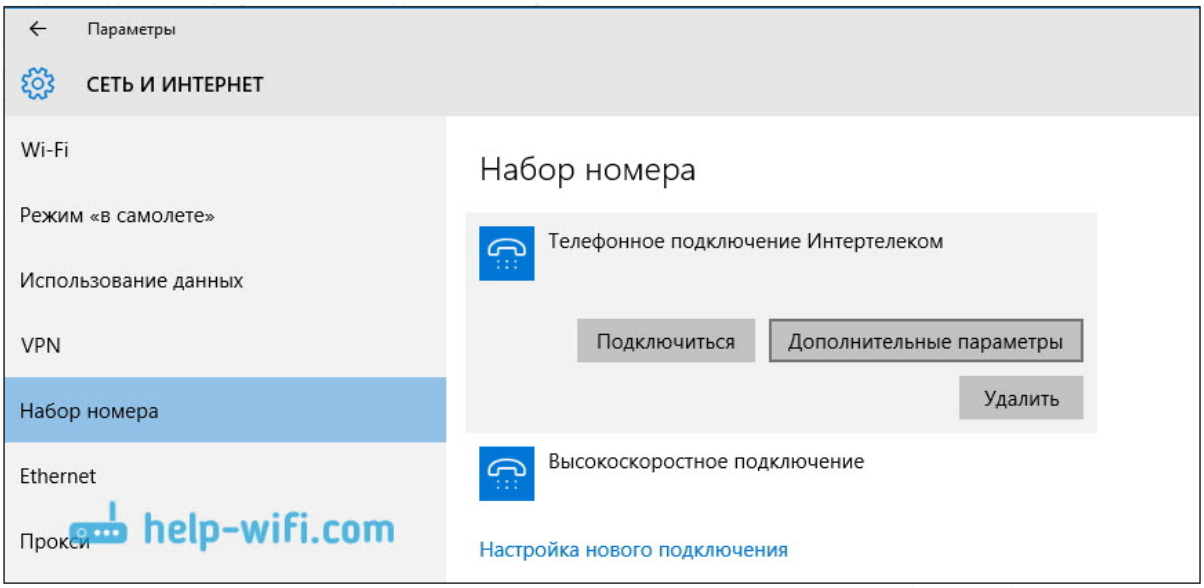


Рис. 14. Підключення до Internet

Рис. 15. Роутер D-Link DIR-300NRu/330NRu/310NRu

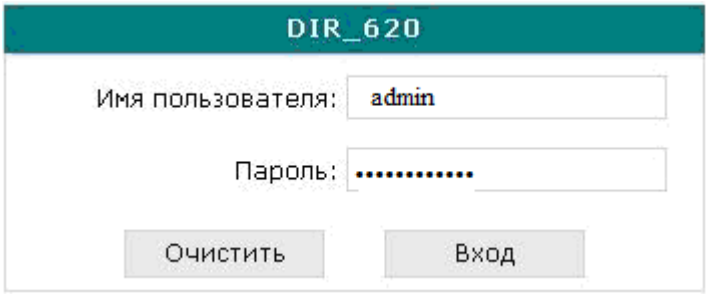


Рис. 16. Введення логіну та паролю

Ім'я користувача – **admin**
Пароль – **admin**
Натисніть **Вход**.
З'явиться повідомлення «**Сейчас установлен пароль по умолчанию. В целях безопасности Вам рекомендуется сменить пароль.**». Натисніть «**ОК**», установіть новий пароль для доступу на WEB-інтерфейс і натисніть «**Сохранить**».
Ще раз уведіть: Ім'я користувача – **admin**
Пароль – установлений Вами
Перейдіть у меню **Wi-Fi** => **Общие настройки** і перевірте, щоб стояв прапорець «**Включить беспроводное соединение**» (рис. 17).

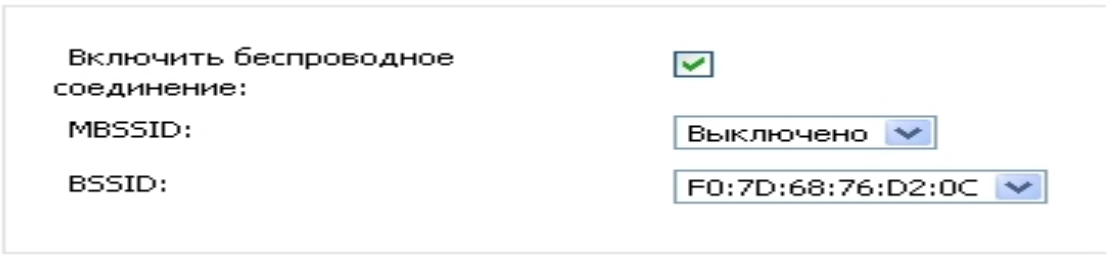


Рис. 17. Перевірка параметрів

Далі перейдіть у меню **Wi-Fi** > **Основные налаштування.**
SSID– пропишіть ім'я бездротової мережі. Можна використовувати латинські букви і цифри.
Країна – введіть Ukrain. **Канал** – замість AUTO установіть будь-який канал с 1 по 11.
Бездротовий режим – можете залишити без змін.

Максимальна кількість клієнтів – можете установити максимальну кількість беспроводових клієнтів. Якщо установлено **0**, **кількість** клієнтів необмежено.

Натисніть **Изменить.**

Після зміни налаштувань натисніть **Сохранить** (рис. 18).

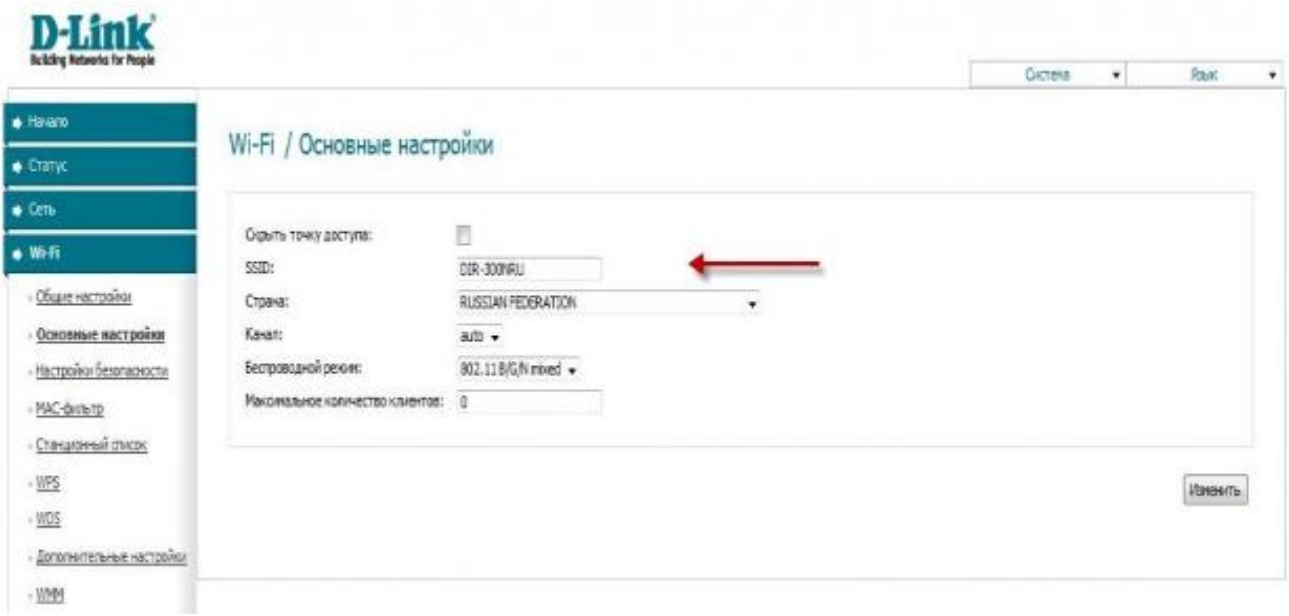


Рис. 18. Збереження налагодження

Далі перейдіть в меню **Wi-Fi** => **Налаштування безопасности.**

Сетевая аутентификация – рекомендується установити шифрування WPA-PSK/WPA2-PSKmixed.

Ключ шифрования PSK – може використовувати ключ за умовчанням або установити свій (от 8 до 63 символів, можна використовувати латинські букви і цифри). Ці цифри вказуються при підключенні до мережі.

WPA-шифрование – виберіть TKIP+AES

WPA период обновления ключа – залиште без змін.

Натисніть **Изменить**

Після зміни налагоджень натисніть **Сохранить** в правому верхньому куті (рис. 18).

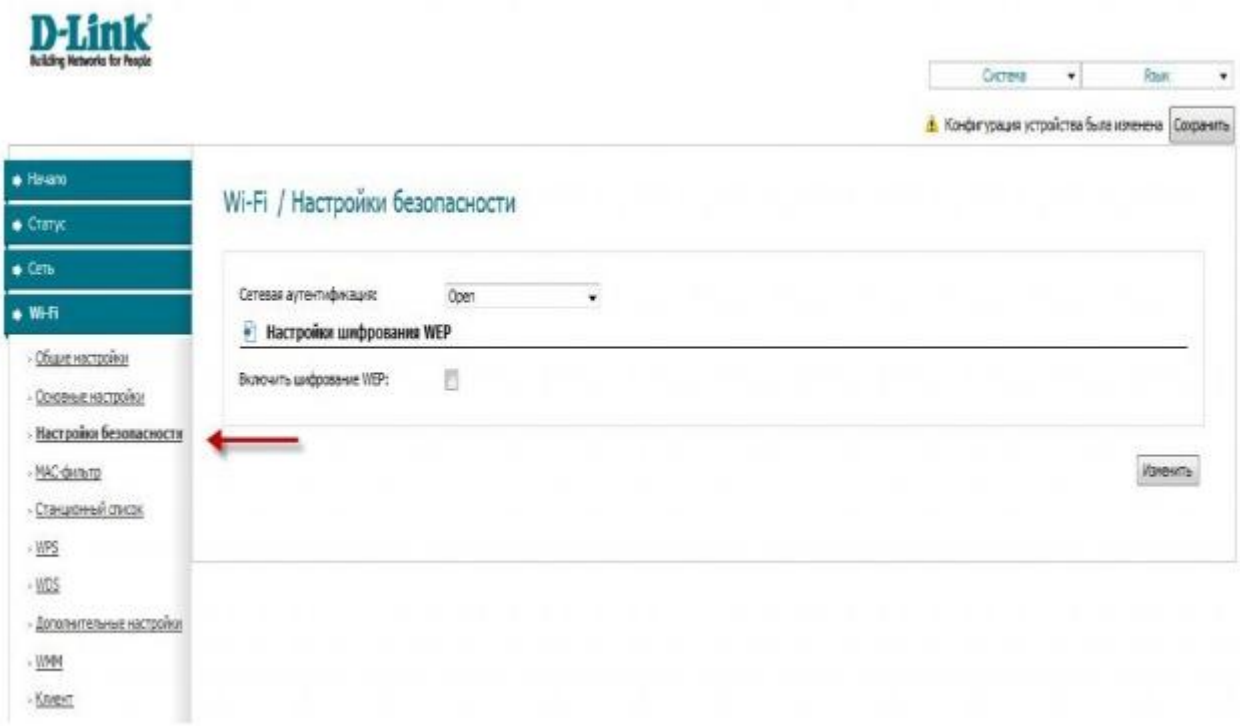


Рис. 18. Налагодження безпеки роутера

В інтерфейсі роутера необхідно зайти у вкладку **Сеть** меню **Соединение (**Тут Ви можете додавати, редагувати й видаляти з'єднання). Натисніть на кнопку **Добавить** (рис. 19).

Рис. 19. Вкладка мережа, з’єднання

Налаштування PPPoE при автоматичнім одержанні локального IP адреси (DHCP)

1. Тип з'єднання (**Connection Type**): **PPPoE**
2. У поле MAC уводите номер вашої мережевої карти (довідатися його можна в стані підключення за локальною мережею,
3. PPP ім'я користувача(**PPP Username**): Ваш логін з договору
4. Пароль **(Password)**: Ваш пароль із договору
5. Підтвердження пароля **(Confirm Password):** повтор пароля
6. Алгоритм аутентифікації: **Auto**
7. Інші поля залиште за замовчуванням.

8. Зберігаємо налаштування кнопкою (**Save)** і кнопкою **Перезагрузка** перезавантажуємо роутер (рис. 20).

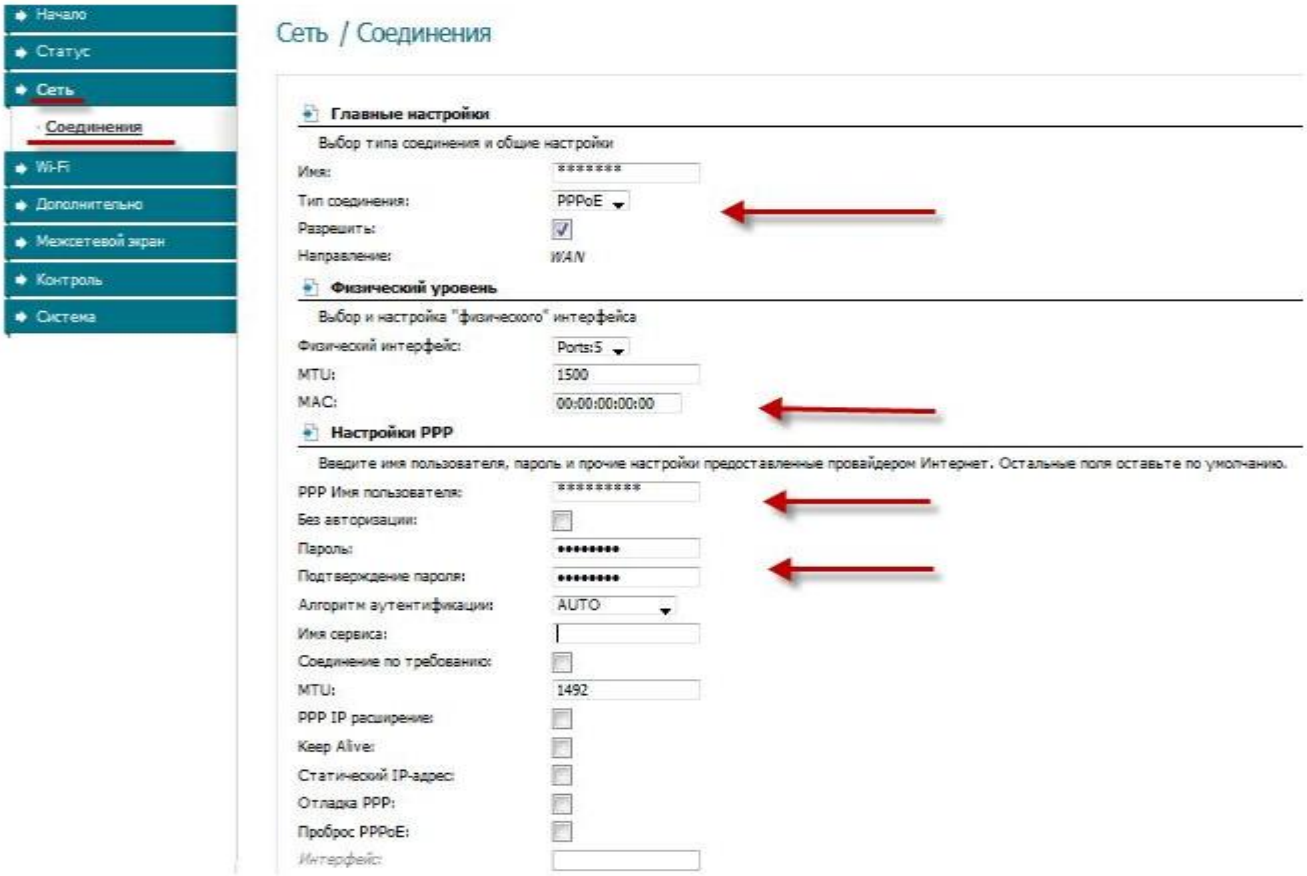


Рис. 20. Налаштування PPPoE при автоматичнім одержанні локального IP адреси (DHCP)

Налаштування Pptp (VPN) при автоматичнім одержанні локальної IP адреси (DHCP)
1. Тип з'єднання (**Connection Type**): PPTP (PPTP і L2TP — тунельні протоколи типу крапка-крапка, що дозволяють комп'ютеру встановлювати захищене з'єднання із сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі.)
2. PPP ім'я користувача(**PPP Username**): Ваш логін з договору
3. Пароль **(Password)**: Ваш пароль із договору
4. Підтвердження пароля **(Confirm Password):** повтор пароля
5. Ім'я сервісу(**Service name**): - IP/Ім'я сервера провайдера.
6. Значення **MTU – 1372**
7. Алгоритм аутентифікації: **Auto**
8. Зберігаємо **налаштування** кнопкою (**Save)** кнопкою **Перезагрузить** перезавантажуємо роутер (рис. 21).

NAT при автоматичнім одержанні IP адреси (DHCP).
1. Тип з'єднання (**Connection Type**):
2. У поле **MAC** вводите номер вашої мережевої карти (Довідатися його можна в стані підключення за локальною мережею.
3. У пункті **Настройка IP** вибираємо одержати **IP автоматично.**
4.У пункті **Настройка IP** вибираємо одержати **адресу DNS автоматично.**
5. Зберігаємо налаштування кнопкою (**Save)** і перезавантажуємо роутер (рис. 22).

Перевірка статусу підключення до Internet.
1. В інтерфейсі роутера необхідно зайти у вкладку **Статус** (**Status**),меню **Сетевая статистика**(**Network Statics**) (рис. 23)

Сохранение/восстановление настроек роутера.

Після проведення налаштувань, рекомендується зберегти їх, щоб у випадку виникнення проблем, можна було відновити. Для цього необхідно зайти у вкладку **Система**, меню **Конфигурация** (рис. 24).

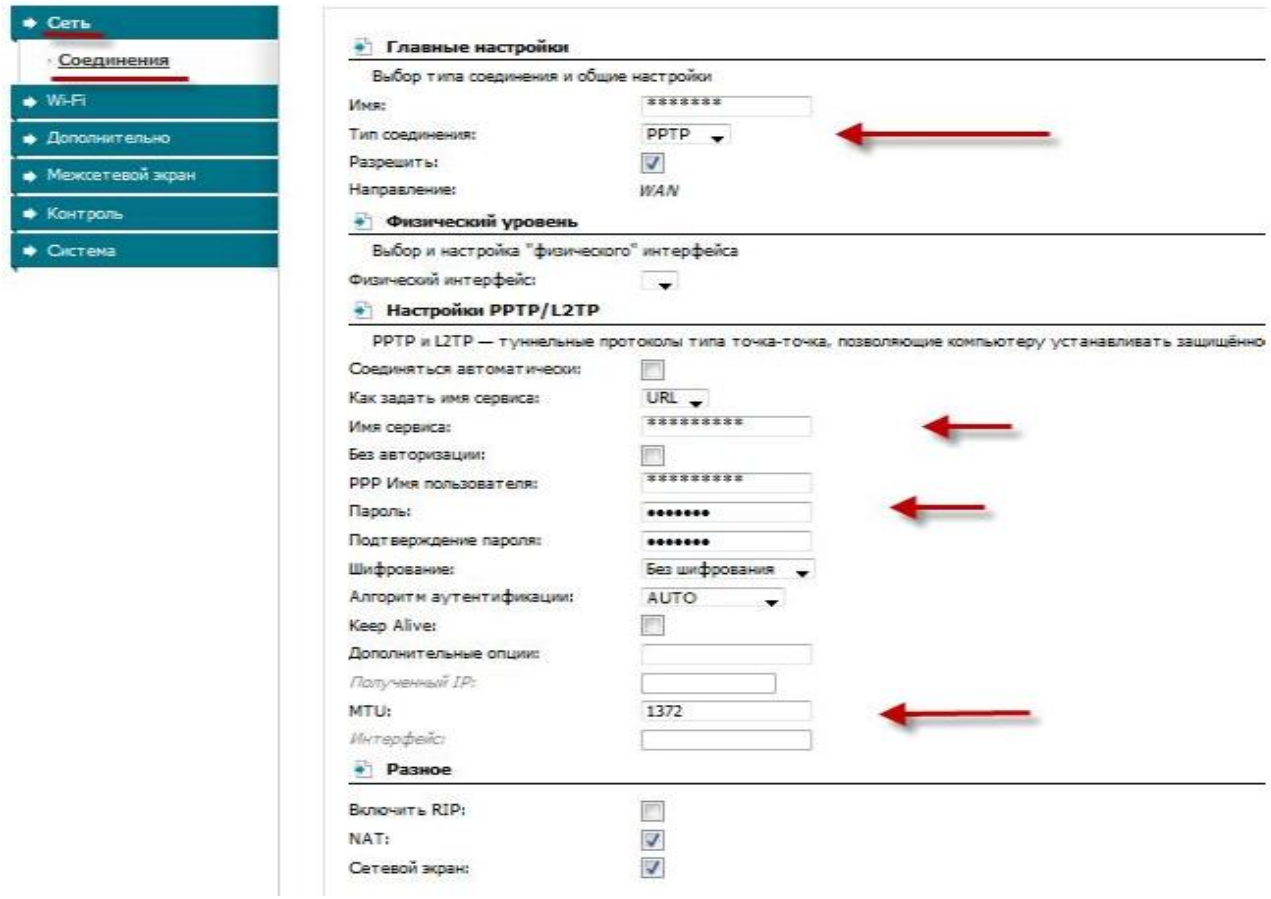


Рис. 21. Налаштування Pptp (VPN) при автоматичнім одержанні локальної IP-адреси (DHCP)

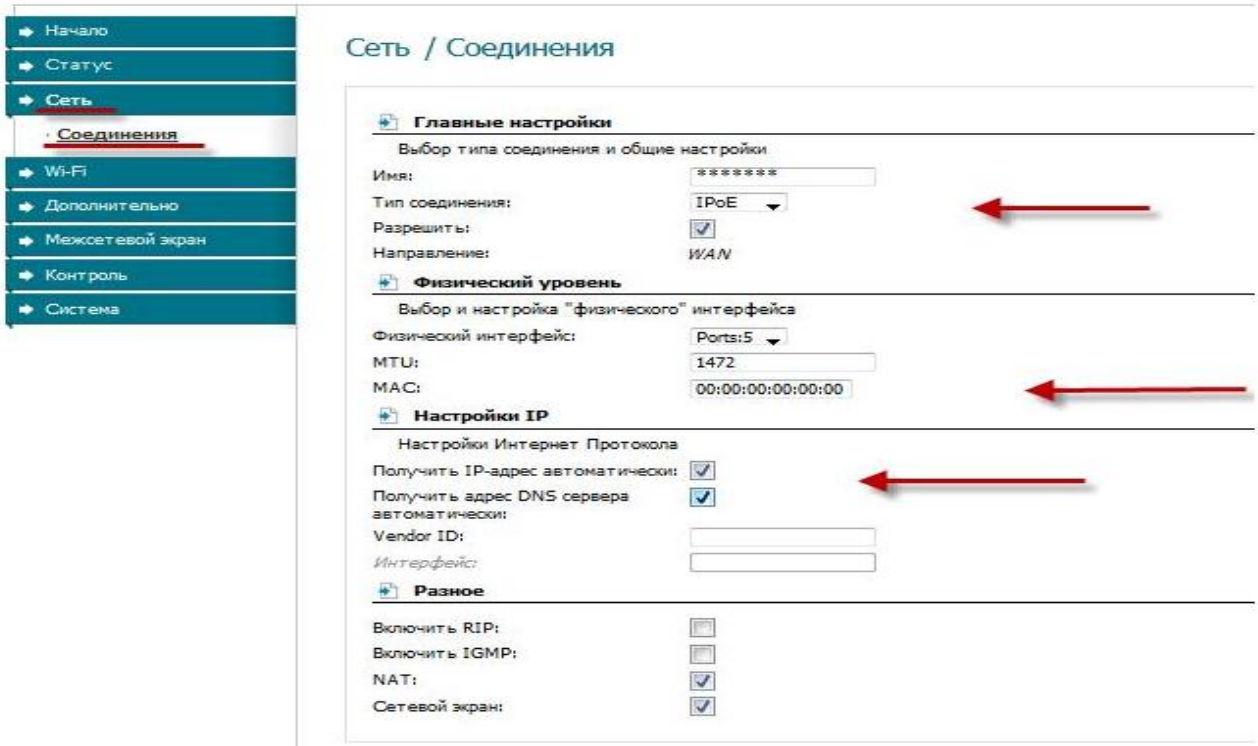


Рис. 22. NAT при автоматичнім одержанні IP адреси (DHCP).

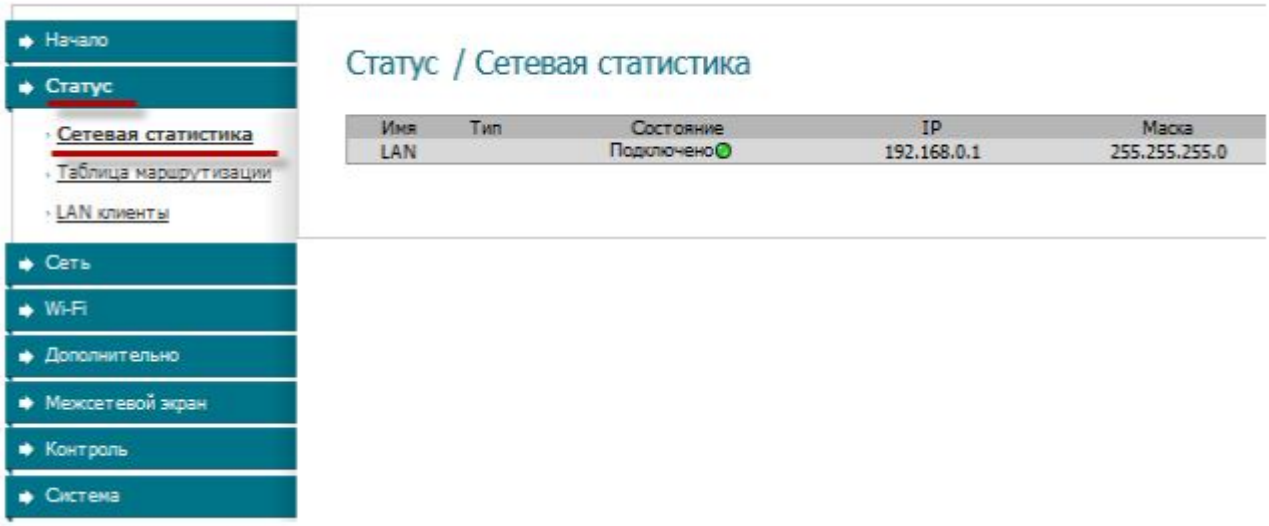


Рис. 23. Перевірка статусу підключення до Internet

1. Виберіть збереження поточної конфігурації. Для збереження поточних налаштувань роутера Файл із налаштуваннями буде збережений у зазначене місце на жорсткому диску.

2. Для відновлення налаштувань із файлу, необхідно вибрати **Загрузка ранее сохраненной конфигурации**, указати шлях до файлу з налаштуваннями.

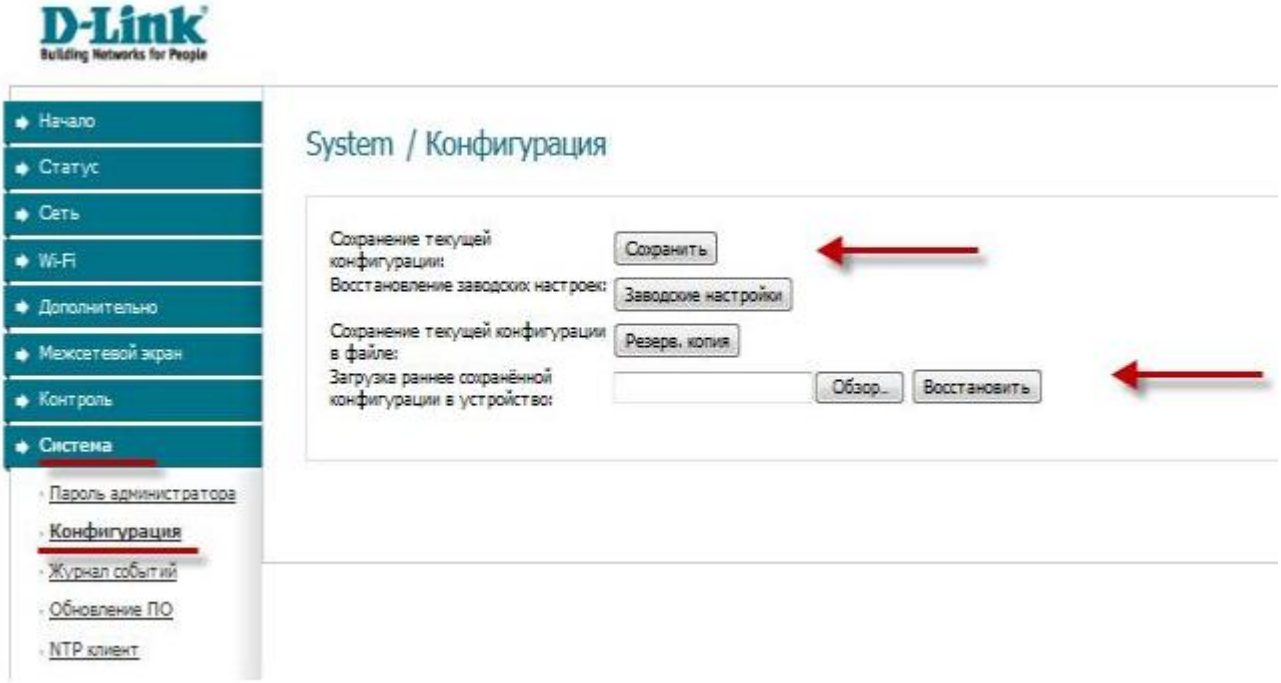


Рис. 24. Збереження/відновлення налаштувань роутера

1.3. Налагодження доступу до Internet через маршрутизатор Cisco

Початкове налаштування мережі

Маршрутизатор Cisco 831 залежно від прошивання має 2-3 порти для маршрутизації **E0** і **E1** (доп. **E2**) і 4-х портовий комутатор, прив'язаний до порту **E0/**

Порт **E1** знаходиться відособлено. У нього й будемо підключати Internet. Це може бути через модем ZTE або через оптичний конвертор.

Тому що IP адреса ADSL модемів за замовчуванням звичайно 192.168.1.1, то прописуємо на **E1** цю ж підмережу.

interface Ethernet1
ip address 192.168.1.2 255.255.255.0
no shutdown

Комп'ютери будуть підключені в порти **FE1- FE4** через порт маршрутизації **E0**, тому набудовуємо порт **E0** під локальну мережу

interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no shutdown

Піднімаємо DHCP сервер.

ip dhcp excluded-address 192.168.14.0 192.168.14.10
!
ip dhcp pool home
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 42 ip 192.168.2.1
dns-server 8.8.8.8 208.67.222.222
lease 7

DNS сервера обрані від google і від opendns. Набудовуємо час. (годинниковий пояс для України 3 без переходу. NTP сервер 3.by.pool.ntp.org

clock timezone FET 3
ntp server 86.57.251.8

Включення PPPoE

Створюємо з'єднання з Byfly по PPPoE і піднімаємо NAT.

interface E1
pppoe enable
pppoe-client dial-pool-number 1

interface Dialer1
description byfly
bandwidth 2048
ip address negotiated
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
no ip mroute-cache
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname 2100xxxxxxxxx@beltel.by
ppp chap password пароль

interface E0
ip nat inside

ip route 0.0.0.0 0.0.0.0 Dialer1
access-list 1 permit 192.168.2.0 0.0.0.255
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface Dialer1 overload

Захист від доступу до маршрутизатора

Для прикладу перекриваємо порти telnet і http, щоб на наш маршрутизатор не могли потрапити зовні.

Взагалі HTTP на Cisco краще виключити. І не забуваємо прописати паролі на доступ по telnet і на enable

```
access-list 100 deny tcp any any eq 23
access-list 100 deny tcp any any eq 80
access-list 100 permit ip any any
interface Dialer1
ip access-group 100 in

no ip http server
no ip http secure-server

line vty 0 4
password пароль_на_telnet
login

enable secret пароль_на_enable
```

У загальному первинне налаштування зроблене, тепер приступаємо до додаткових налаштувань.

Використання Wi-Fi від модему ZTE

При налагодженнях за замовчуванням у модем включений у режимі моста LAN протокол RIP

Скористаємося RIP і передамо модему інформацію й нашої мережі 192.168.2.0 і про доступ в Internet.

```
router rip
 version 2
 network 0.0.0.0
```

Після чого одержуємо доступ до модему, набудовуємо пароль на Wi-Fi і перевіряємо налаштування DHCP на модемі (указуємо користувацькі DNS сервера). У випадку, якщо модем не видний з мережі можливо він не одержав за RIP список мереж. Заходимо на модем, перемкнувши кабель, і в секції Interface Setup / Lan / Direction указуємо Both.

У секції Advanced Setup / Routing дивимося, що з'явилися маршрути на Cisco.

Після чого додаємо правила й інтерфейс **E1** в NAT.

```
access-list 1 permit 192.168.1.0 0.0.0.255
interface E1
 ip nat inside
```

Передача портів із зовнішнього інтерфейсу на локальні комп'ютери для доступу з Internet до локальних сервісів.

У загальному випадку, наприклад, треба відкрити порти torrent або організувати доступ з Internet за radmin, ftp, http, Fidonet, камери спостереження в локальній мережі.

Необхідно вказати, куди маршрутизатор буде відсилати пакети призначені torrent.

Для цього необхідно мати локальну IP адресу на комп'ютері, яка не змінюється. Два варіанти: Прописати статику або налагодити DHCP/

```
ip dhcp pool pc_1
host 192.168.2.200 255.255.255.0
hardware-address 001e.8ee7.aaaa
```

І вказати для torrent TCP і UDP порти (дивимося в налагодженнях torrent. наприклад 11111)

ip nat inside source static tcp 192.168.2.200 11111 interface Dialer1 11111
ip nat inside source static udp 192.168.2.200 11111 interface Dialer1 11111

Відповідно, якщо Ви піднімаєте на своєму комп'ютері ftp сервер і прагнете мати до нього доступ зовні, то налаштування виглядають так:

ip nat inside source static tcp 192.168.2.200 20 interface Dialer1 20
ip nat inside source static udp 192.168.2.200 21 interface Dialer1 21

Використання DDNS

Тепер якщо ви знайдете себе з Internet, то побачите, що зовнішня адреса динамічна, і вона міняється при кожнім пере з'єднанні.

Один варіант – купити статичну IP-адресу, другий використовувати DDNS, тобто повідомити DNS серверам, що за певним іменем зареєстрована певна IP адреса.

Можна використати dyndns.dk. Після реєстрації одержуєш ім'я типу vasya.dyndns.dk

Там же пропонують посилання для зіставлення свого імені й адреси

Можна запит цього посилання доручити виконувати Cisco за розкладом.

kron policy-list DDNS

cli copy
http://dyndns.dk/opdat.php?name=**vasysa**&domain=**dyndns.dk**&pw=**який_те_табір_буковок**
&silent=1 null:

kron occurrence ddns in 1:00 recurring

policy-list DDNS

У такий спосіб маршрутизатор буде щогодини нагадувати DNS серверам про свою адресу.

Мінус тільки в тому, що після пере з'єднання й зміни IP адреси повинен пройти час (до 2-х годин) для поширення інформації з DNS сервера.

2. Контрольні питання

1. Яка послідовність налагодження підключення до Internet в Windows 10?
2. Як налагодити параметри захисту мережі в Windows 10?
3. Як встановити селектор режиму перегляду як Категорія?
4. Яке призначення Центру управління мережами і загальним доступом?
5. Як налагодити потрібні параметри адаптера?
6. Яка послідовність налагодження підключення до Internet в D-Link?
7. Як налагодити параметри захисту мережі в D-Link?
8. Яка послідовність налагодження підключення до Internet в Cisco?
9. Як налагодити параметри захисту мережі в Cisco?

ЛАБОРАТОРНА РОБОТА 23.
ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ INTERNET В ОС WINDOWS XP.

Мета роботи: отримати практичні навички підключення до мережі Internet

Зміст

1. Хід роботи
1.1. Установка драйверів дата-кабелю й модему Huawei
2. Контрольні питання

1. Хід роботи

1.1. Установка драйверів дата-кабелю й модему Huawei

Вставте диск із драйверами, що поставляється разом з дата-кабелем в CD-дисковод вашого комп'ютера. Знайдіть на ньому папку **Setup** і запустіть файл **Setup.exe** (рис. 1).

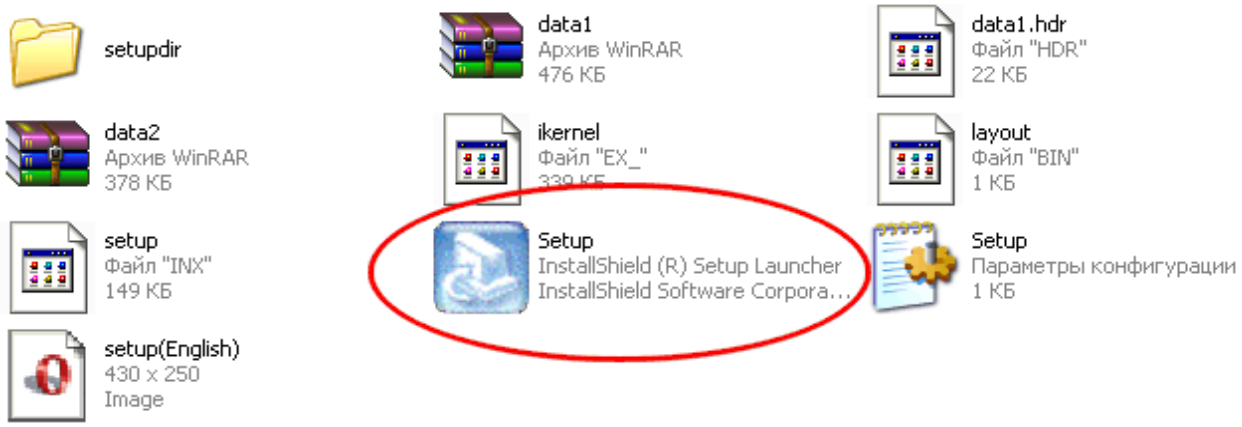


Рис. 1. Запуск драйвера модему

Почнеться установка модему Huawei. Виберіть англійську мову установки. Натисніть **ОК** (рис. 2).

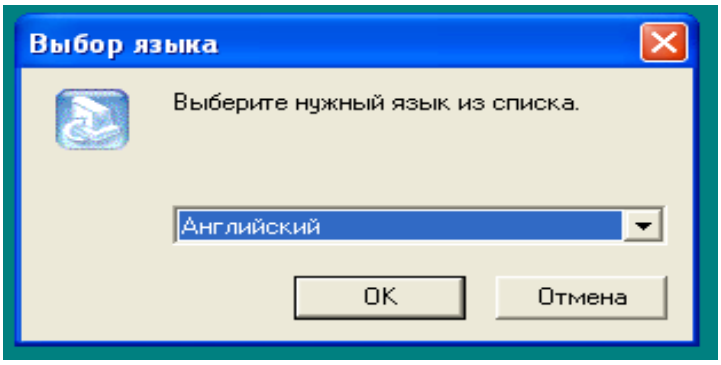


Рис. 2. Відбір мови встановлення драйверу

Програма почне установку необхідних файлів на ваш комп'ютер.

Перед початком установки слід пам'ятати, що дата кабель не повинен бути підключений до комп'ютера. Ваш комп'ютер не повинен бути підключений до Internet. Натисніть кнопку **Next** (рис. 3).

Виберіть диск, на який потрібно встановити драйвера (За замовчуванням це системний диск **C** на вашому комп'ютері) і натисніть кнопку **Next** (рис. 4).

Програма почне копіювання необхідні файли на ваш комп'ютер (рис. 5).

Після закінчення копіювання файлів система видасть повідомлення про те, що TIUMP USB Serial Port не виявлений (рис. 6).

Згорніть програму установки модему (рис. 7).

Підключіть USB кабель до комп'ютера. Система виявить новий пристрій (рис. 8).

Далі буде запропоновано встановити драйвера для нього. Виберіть пункт **«Автоматическая установка»**. Натисніть кнопку **Далее** (рис. 9).

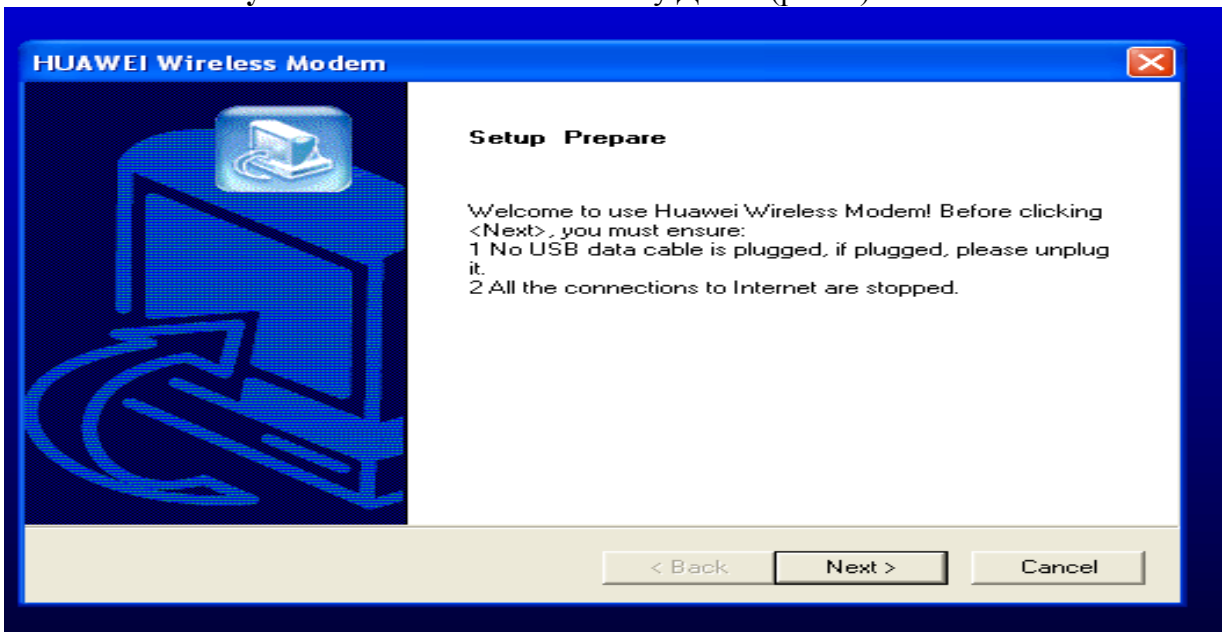


Рис. 3. Вікно майстра встановлення драйверу

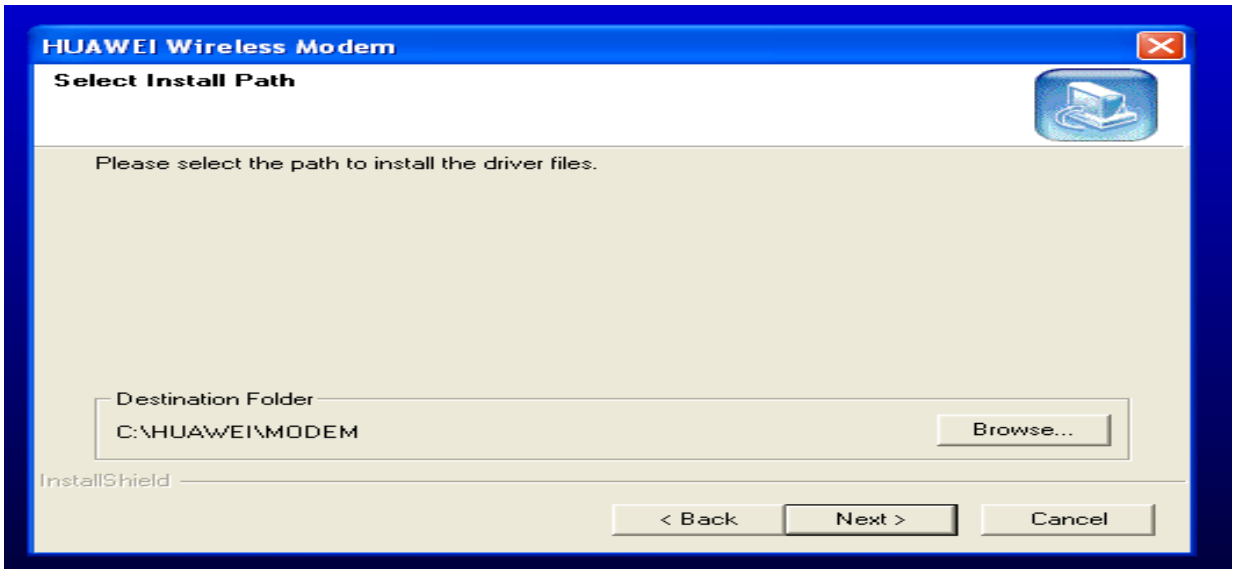


Рис. 4. Відбір диска встановлення драйверу

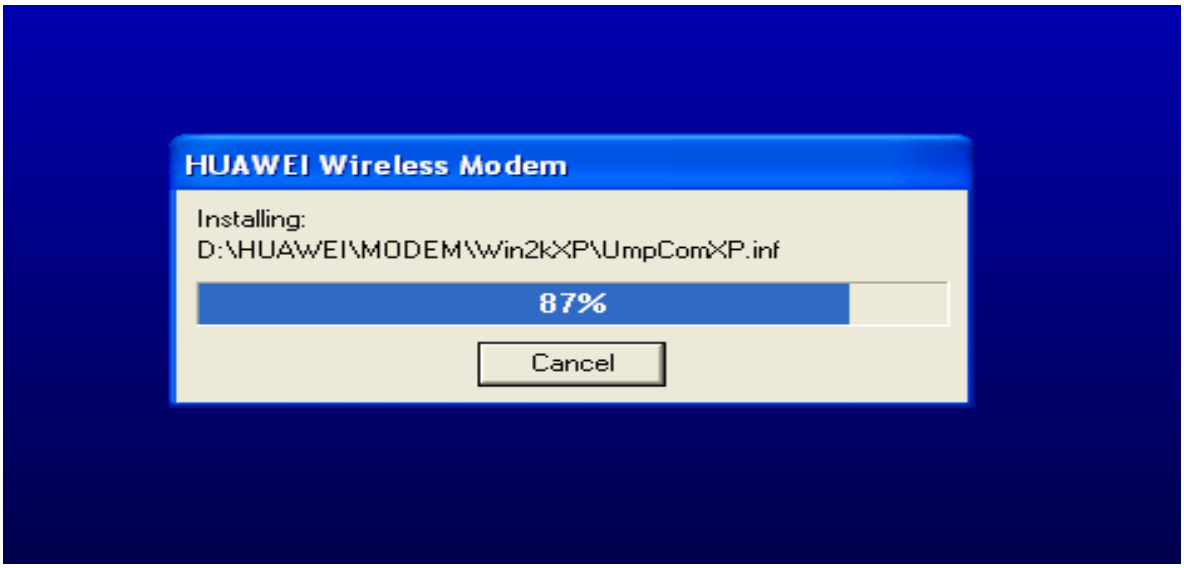


Рис. 5. Копіювання файлів

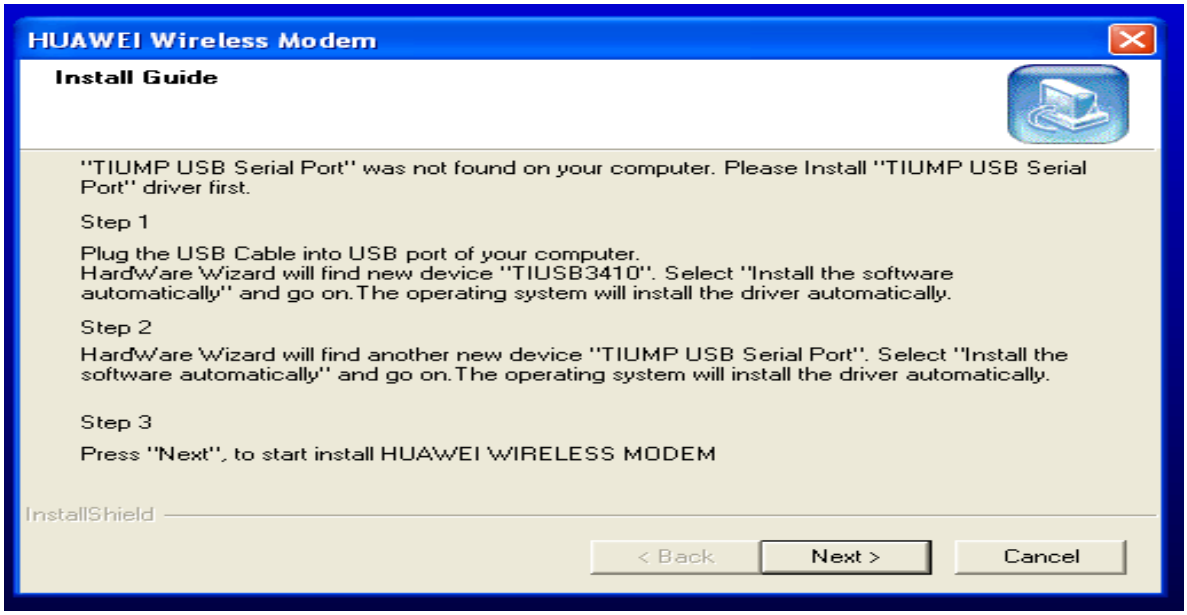


Рис. 6. TIUMP USB Serial Port не виявлений

Рис. 7. Згортання програми установки модему

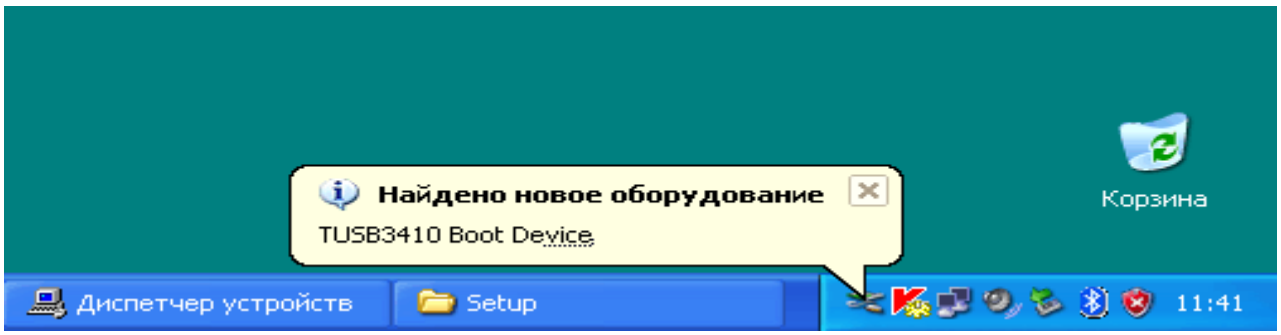


Рис. 8. Знайдено новий устрій

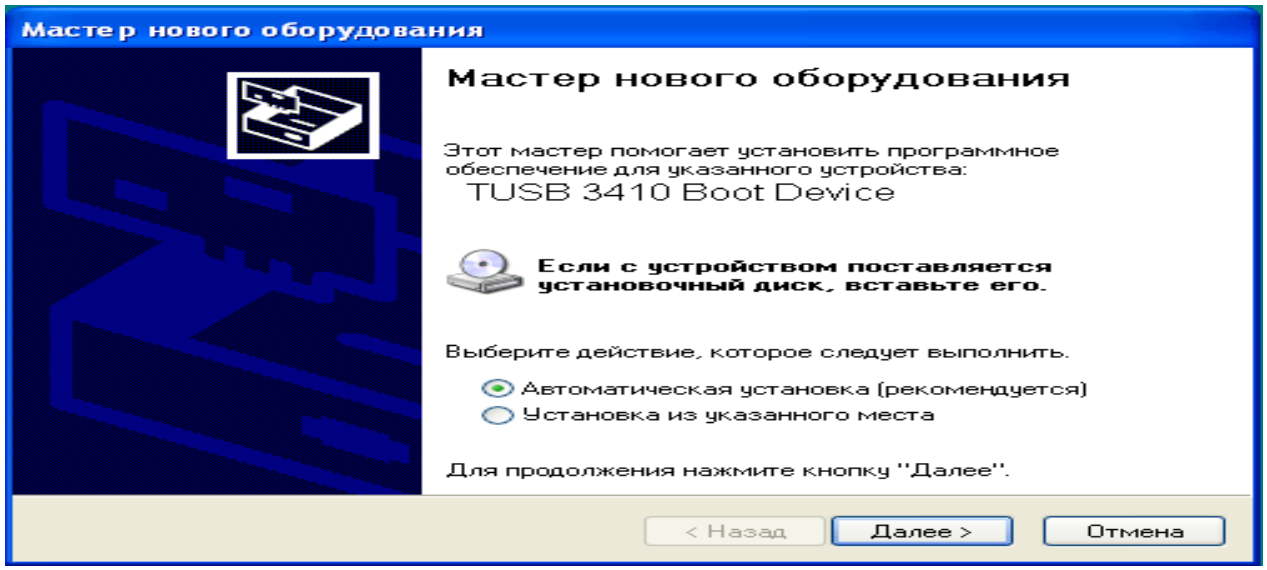


Рис. 9. Відбір автоматичного встановлення

Система знайде на вашім комп'ютері необхідні файли (рис. 10).

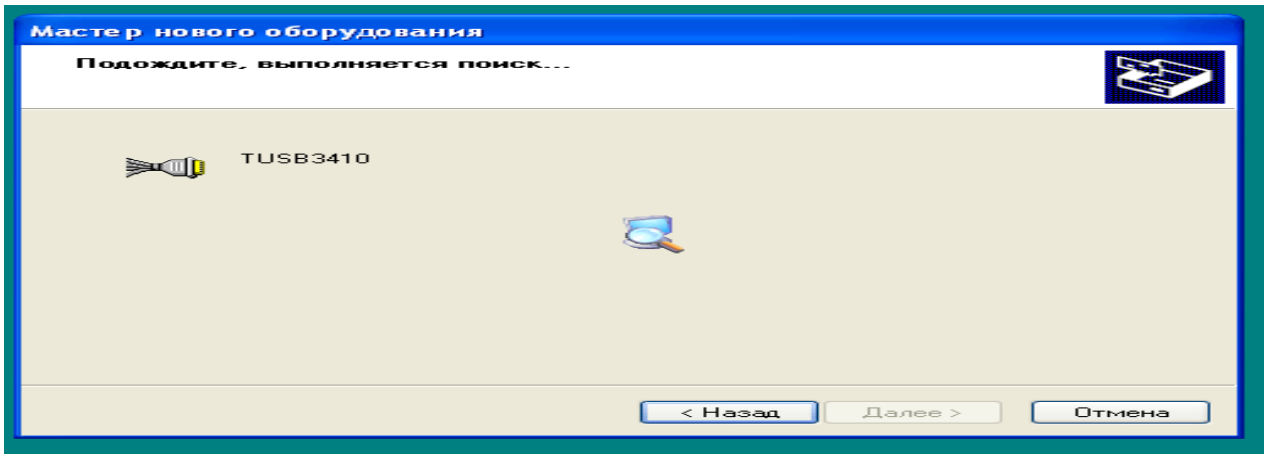


Рис. 10. Пошук потрібних файлів

І встановить їх автоматично.
За закінченням установки натисніть кнопку **Готово** (рис. 11).

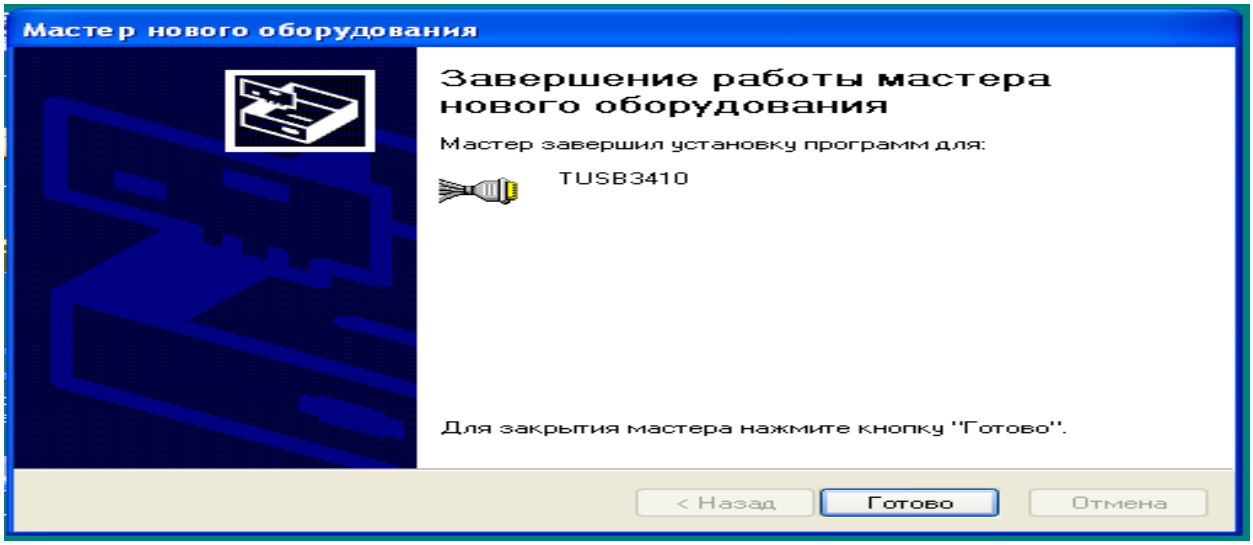


Рис. 11. Завершення роботи майстра

Після цього система видасть повідомлення, що виявлений ще один новий пристрій. Це TIUMP USB Serial Port (рис. 12).

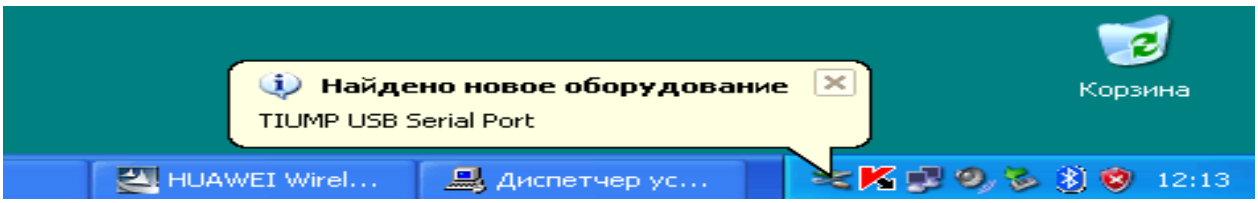


Рис. 12. Знайдено нове обладнання

Виберіть пункт **Автоматическая установка** й натисніть кнопку **Далее** (рис. 13-15).

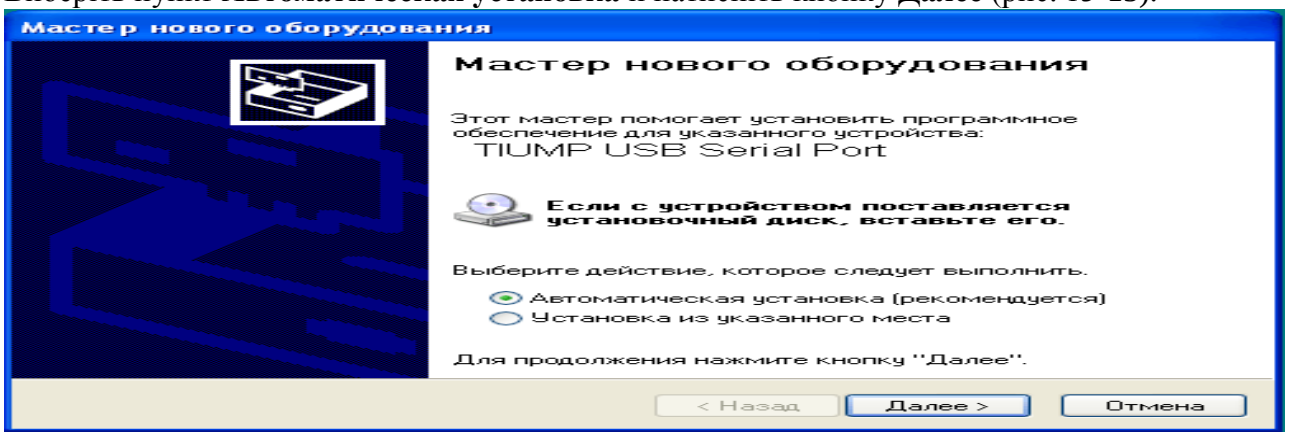


Рис. 13. Вікно майстра встановлення драйвера

Система зробить установку необхідних драйверів на ваш комп'ютер.

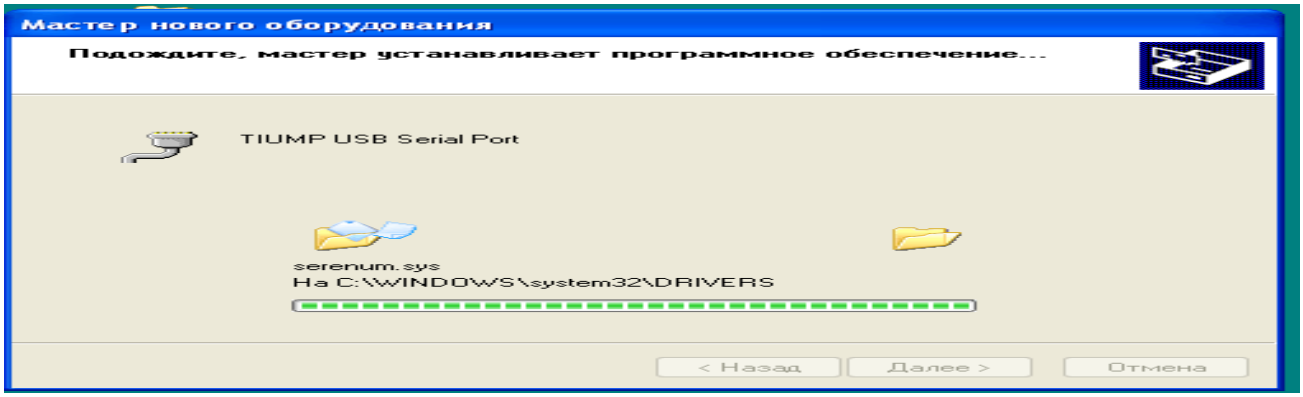


Рис. 14. Вікно майстра встановлення драйвера

За завершенням натисніть кнопку **Готово.**

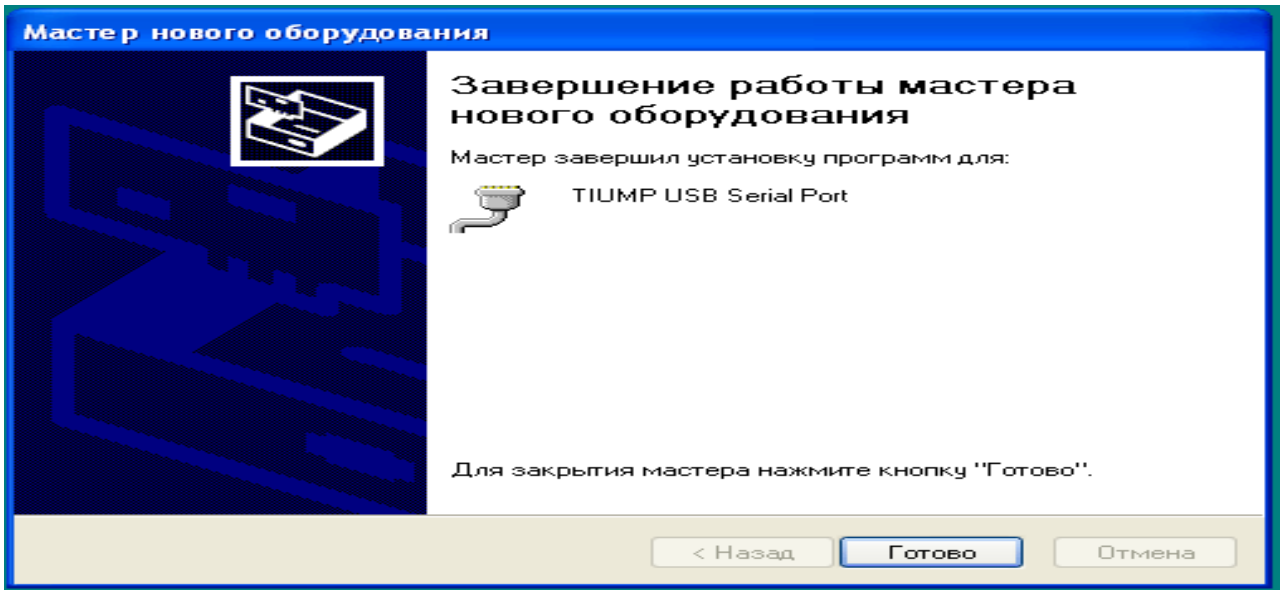


Рис. 15. Вікно майстра встановлення драйвера

За закінченням установки система видасть повідомлення, що встаткування встановлене й готове до використання (рис. 16).

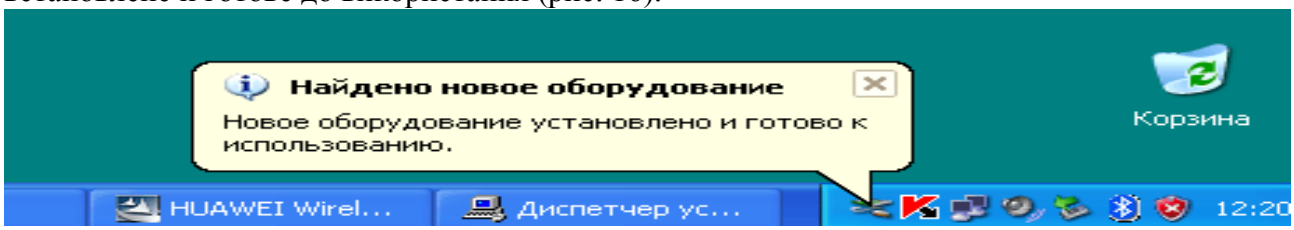


Рис. 16. Обладнання готове до використання

Розгорніть згорнуту раніше програму установки модему Huawei (рис. 17).

Рис. 17. Розгортання згорнутої раніше програми установки модему

Підключіть дата кабель із однієї сторони до вашого термінала Huawei, з іншої сторони до USB порту вашого комп'ютера й натисніть кнопку **Next** (рис. 18).

Рис. 18. Вікно майстра встановлення модему

Програма установки видасть повідомлення, що модем виявлений на зазначеному порту. (У цьому випадку на малюнку ви бачите, що це порт COM14. У вашім випадку це може бути будь-який інший вільний порт: COM3, COM5, COM9 і т.д.). Потім програма почне установку драйверів модему на комп'ютер (рис. 19, 20).

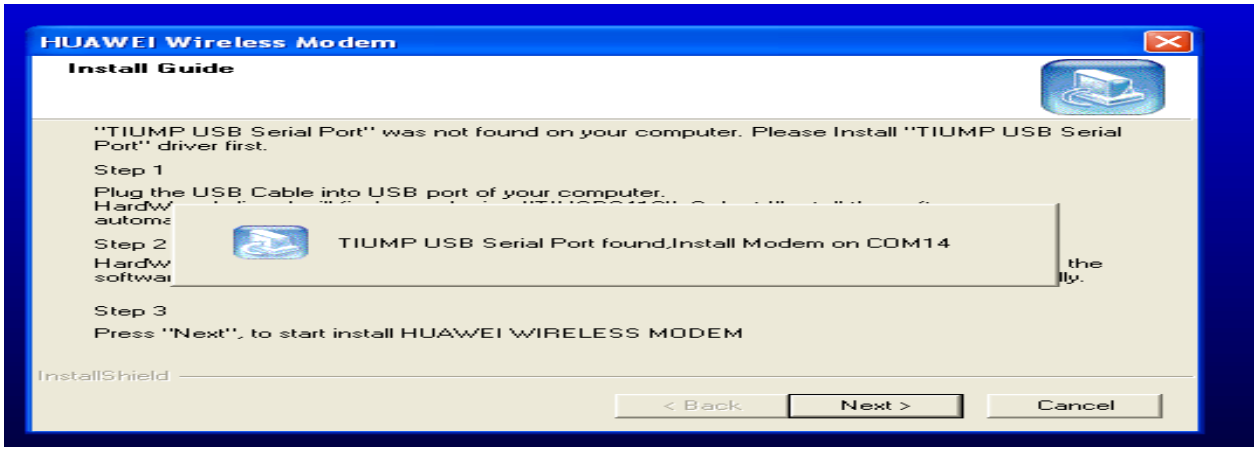


Рис. 19. Вікно майстра встановлення модему

За закінченням установки натисніть кнопку **Finish**.

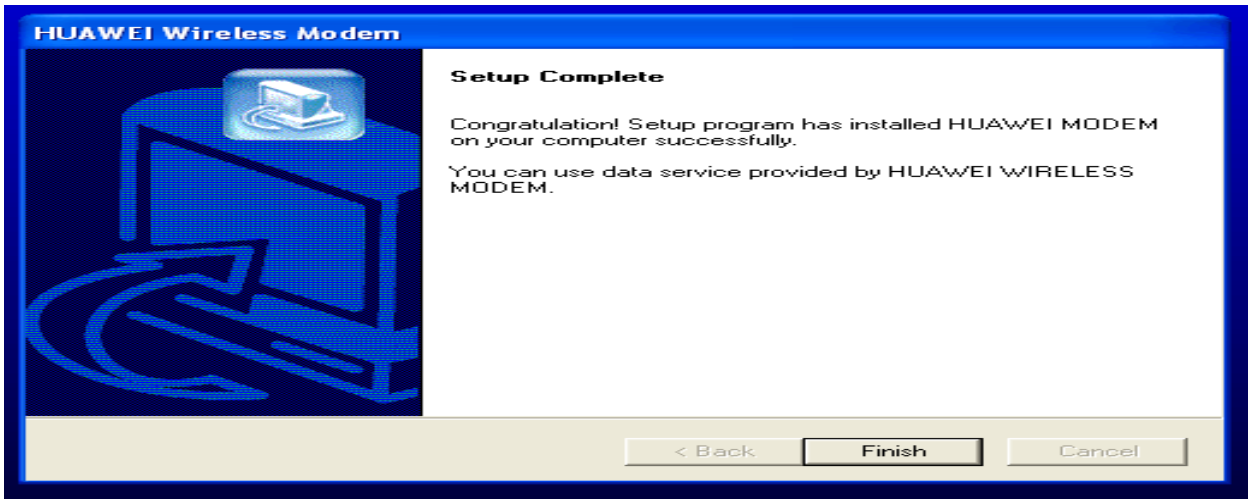


Рис. 20. Вікно майстра встановлення модему

Натисніть кнопку **Пуск**, виберіть **Панель управления**, зайдіть у розділ **Телефон и модем** (рис. 21).

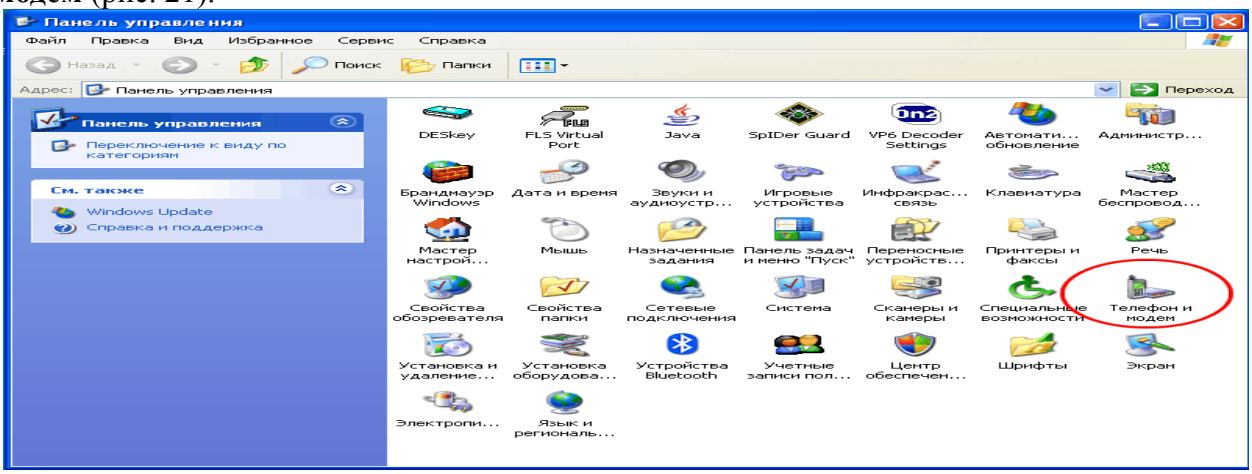


Рис. 21. Відбір розділу **Телефон и модем**

Виберіть закладку **Модеми.** Виділіть встановлений **модем Huawei Wireless Modem** курсором і натисніть кнопку **Свойства** (рис. 22).

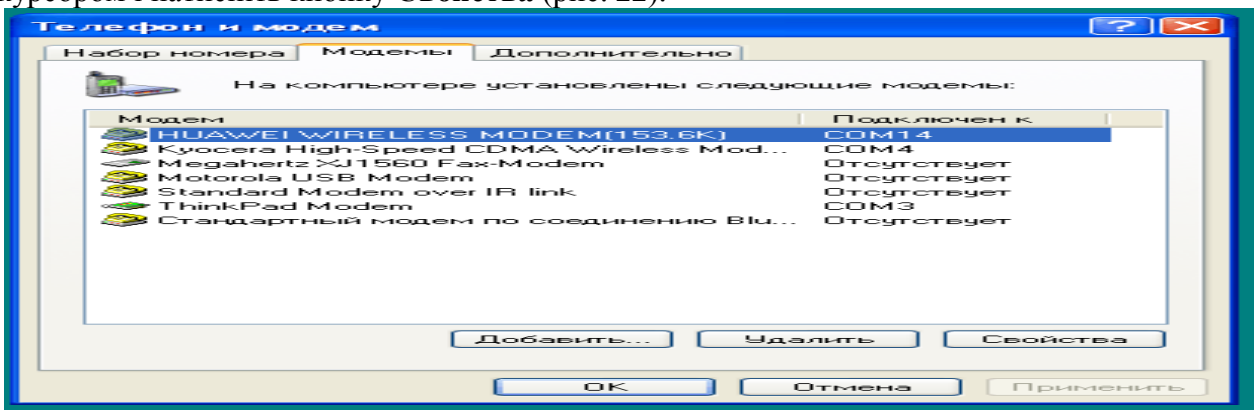


Рис. 22. Відбір властивостей модему

Виберіть закладку **Диагностика** й натисніть кнопку **Опросить модем** (рис. 23).

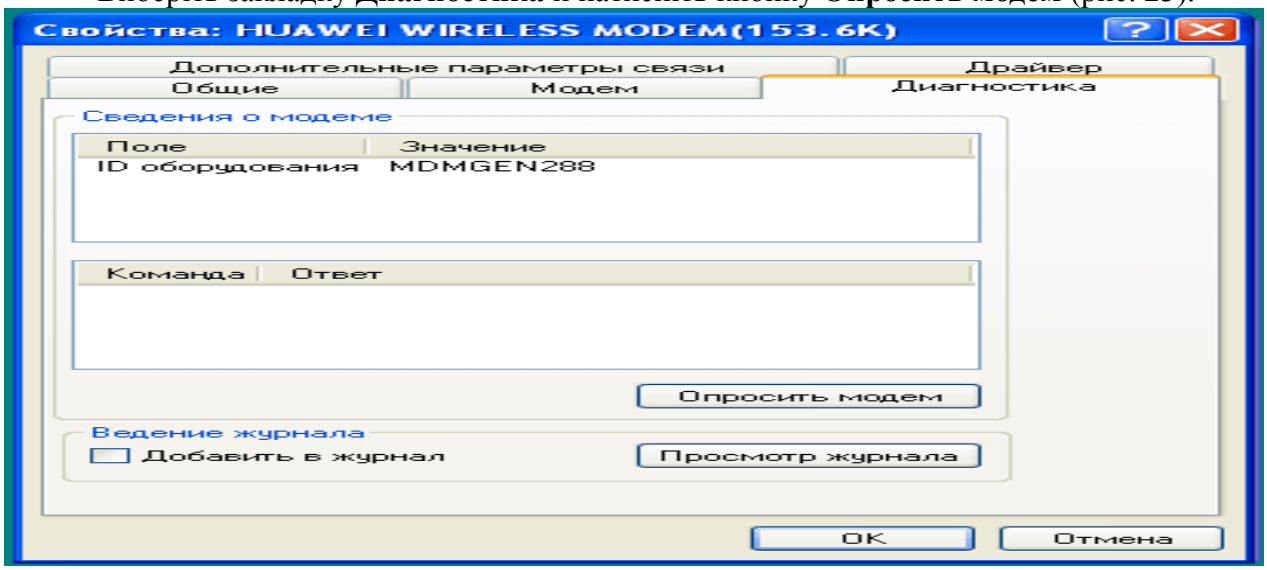


Рис. 23. Опитування модему

Система почне обмін даними з модемом. Це може зайняти якийсь час (рис. 24).

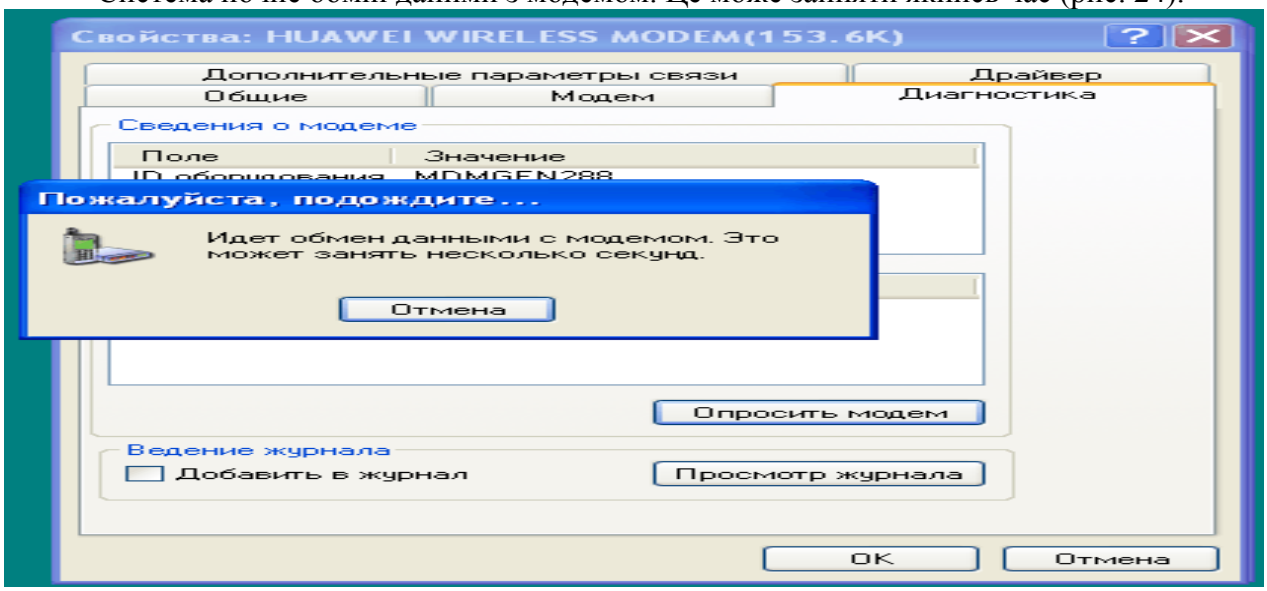


Рис. 24. Опитування модему

Якщо модем установлений правильно. Скрізь нажати **ОК**.

2. Контрольні питання

1. Який порядок встановлення драйверів обладнання?
2. Як відібрати диск, каталог на який встановлюється драйвер?
3. Які особливості роботи майстра встановлення драйверів?
4. Як підібрати необхідні параметри модему?
5. Як перевірити працездатність модему?

ЛАБОРАТОРНА РОБОТА 24. НАЛАГОДЖЕННЯ ДОСТУПУ ДО МЕРЕЖІ INTERNET З ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ WIN 2003 SERVER

Мета роботи: розглянути різні варіанти підключення до мережі Internet з локальної мережі, використовуючи різні програмні засоби.

Зміст

1. Теорія
2. Хід роботи:
2.1. Налагодження підключення через Win2003 Server. NAT
2.2. Налагодження підключення через Winxp. Internet Connection Sharing.
2.3. Налагодження підключення через Winxp. Проксі-Сервер
3. Контрольні питання

1. Теорія

Є локальна мережа представлена на рис. 1.

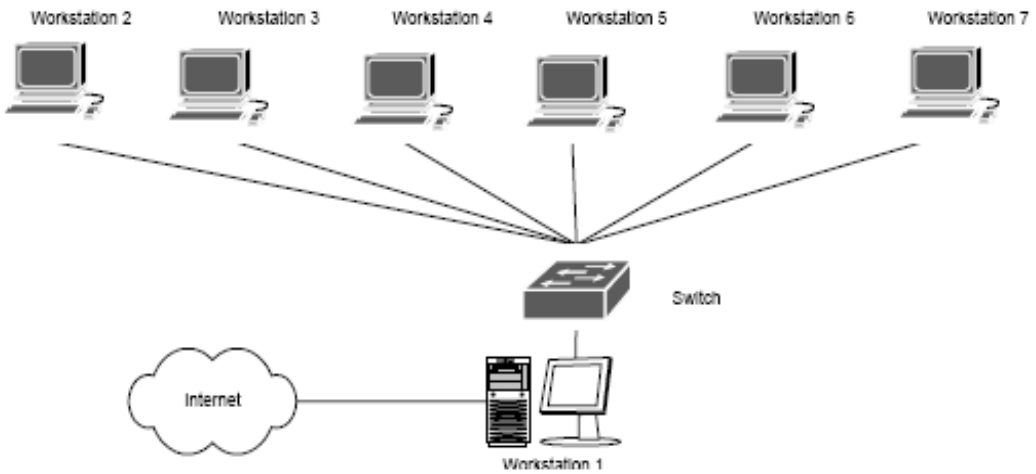


Рис. 1. Схема мережі

На комп'ютері (шлюзі), через який планується підключення локальної мережі до Internet необхідна наявність двох мережевих адаптерів (підключень).

Завдання: Необхідно забезпечити доступ до мережі Internet із усіх робочих станцій.

Є три основні варіанти підключення локальної мережі до Internet:

1. «Пряме» Ір-Підключення,
2. Підключення через NAT,
3. Підключення через Проксі-сервер.

Розглянемо переваги, недоліки й область застосування кожного методу, а також деякі переваги та недоліки. Вибір конкретного способу підключення залежить від потреб користувачів, мети підключення й, в деякому ступені, фінансових можливостей.

Комп'ютер ***Workstantion 1***. У нього є доступ, як до Internet, так і до локальної мережі. Наше завдання – надати комп'ютерам локальної мережі доступ до Internet через підключений до нього комп'ютер. Далі цей комп'ютер ми будемо називати шлюзом або маршрутизатором.

Розгляд способів ми почнемо з, що найменш часто використовуємого, найбільш дорогого, але також найбільше «правильного» і природнього способу, що дає найбільші в порівнянні з іншими способами можливості.

«Пряме» Ір-Підключення до Internet. Для того, щоб локальна мережа була повноцінно підключена до Internet, повинні дотримуватися, як мінімум, три умови:

1. Кожна машина в локальній мережі повинна мати "реальну", інтернетівську Ір-Адресу;

2. Ці адреси повинні бути не будь-якими, а виділеними провайдером для локальної мережі (швидше за все, це буде підмережа класу С);

3. На комп'ютері-шлюзі, підключеному до двох мереж - локальної мережі й мережі провайдера, повинна бути організована Ip-Маршрутизація, тобто передача пакетів з однієї мережі в іншу.

У цьому випадку локальна мережа стає як би частиною Internet. Властиво, це той спосіб підключення, яким підключені до Internet самі Internet-Провайдери й хостинг-провайдери.

На відміну від звичайного підключення, розрахованого на один комп'ютер, при такім підключенні " під клієнта" виділяється не одна Ip-Адреса, а так звана " Ip-Підмережа".

При такому способі підключення можна організувати у своїй мережі сервіси, доступні з Internet – адже при данім підключенні не тільки Internet повністю доступний з мережі, але й мережа – з Internet, тому що є його частиною. навіть призначені для "внутрішнього" використання, стануть доступними ззовні через Internet. Щоб це не мало місця, доступ у локальну мережу ззовні трохи обмежують. Звичайно це робиться установкою на шлюзі програми-firewall. Це своєрідний фільтр пакетів, що проходять із однієї мережі в іншу. Шляхом його Налагодження можна заборонити вхід-вихід з локальної мережі пакетів, відповідних до певних критеріїв – типу IP-пакета, Ip-Адреси призначення, TCP/ Udp-Порту й т.п.

Firewall вирішує такі завдання, як:

блокіровку доступу ззовні до певних TCP/ Ip-Сервісів локальної мережі;

блокіровку доступу до певних комп'ютерів локальної мережі. Таким чином, можна заборонити доступ ззовні до всіх машин, крім певних серверів, призначених для доступу з Internet;

Незважаючи на універсальність такого методу підключення локальної мережі до Internet, цей метод має недоліки. Завдяки ним, його реально й використовують тільки лише ті організації, яким треба зробити свої сервера доступними з Internet – в основному, ті ж Internet-провайдери й хостинг-провайдери, а також інформаційні служби. Найголовніший недолік полягає в дорожнечі виділення Ip-Адрес і тим паче Ip-Підмереж, до того ж цю плату треба вносити періодично.

Тому на практиці розглянемо інші, описані далі способи, що не вимагають більших витрат і, що саме головне, що дозволяють підключити локальну мережу через звичайне підключення з одною зовнішньою Ip-Адресою.

Підключення через NAT (Ip-Маскарадінг)

Технологія Network Address Translation (NAT) – "трансляція мережевих адрес" дозволяє декільком машинам локальної мережі мати доступ до Internet через одне підключення й один реальну зовнішню Ip-Адресу.

Для того, щоб комп'ютери локальної мережі могли встановлювати з'єднання із серверами мережі Internet, потрібно, щоб:

ip-пакети, адресовані серверу в Internet, змогли його досягтися;

важливі Ip-Пакети, що йдуть від сервера Internet на машину в локальній мережі, також змогли її досягтися.

З першою умовою проблем не виникає, а як бути із другою? Адже комп'ютери локальної мережі не мають своєї "реальної" інтернетівської Ip-Адреси! Як же вони можуть одержувати Ip-Пакети з Internet?

А працює це в такий спосіб – на комп'ютері-шлюзі встановлена програма Nat-Сервера. Комп'ютер-Шлюз прописаний на машинах локальної мережі як "основний шлюз", і на нього надходять усі пакети, що йдуть в Internet (не адресовані самій локальній мережі). Перед передачею цих Ip-Пакетів в Internet Nat-Сервер заміняє в них IP-адреси відправника на свій, одночасно запам'ятовуючи в себе, з якої машини локальної мережі прийшов цей Ip-Пакет.

Коли приходить відповідний пакет (на адресу шлюзу, звичайно), NAT визначає, на яку машину локальної мережі його треба направити. Потім в отриманому пакеті міняється адреса одержувача на адресу потрібної машини, і пакет доставляється цій машині через локальну мережу.

Як бачимо, робота Nat-Сервера прозора для машин локальної мережі (як і робота звичайного Ip-маршрутизатора).

Єдиним принциповим обмеженням цього методу підключення локальної мережі до Internet є неможливість установити вхідне Tcp-З'єднання з Internet на машину локальної мережі. Однак для "клієнтських" мереж цей недолік перетворюється в перевагу, що різко збільшує (у порівнянні з першим методом підключення) їх захищеність і безпеку. Адміністратори деяких провайдерів навіть уживають слова NAT і Firewall як синоніми.

Підключення через Проксі-сервер

Це найпростіший тип підключення. При цьому ніякої маршрутизації Ip-Пакетів між локальною мережею й мережею Internet не відбувається. Машини локальної мережі працюють із Internet через програму-посередник, так званий Проксі-сервер, установлений на комп'ютері-шлюзі.

Основною особливістю цього методу є його "непрозорість". Якщо, скажімо, у випадку NAT програма-клієнт просто звертається до Internet-Серверу, не "замислюючись", у якій мережі й через яку маршрутизацію вона працює, то у випадку роботи через Проксі-сервер програма повинна явно звертатися до Проксі-серверу. Мало того, клієнтська програма повинна вміти працювати через Проксі-сервер. Однак проблем із цим не виникає - усі сучасні й не дуже браузери вміють працювати через Проксі-сервери.

Іншою особливістю є те, що Проксі-сервер працює на більш високому рівні, ніж, скажімо, NAT. Тут уже обмін з Internet іде не на рівні маршрутизації пакетів, а на рівні роботи з конкретним прикладним протоколом (HTTP, FTP, POP3...). Відповідно для кожного протоколу, за якими повинні "уміти" працювати машини локальної мережі, на шлюзі повинен працювати свій Проксі-сервер.

Ця "протокольна залежність" і є основний недолік цього методу підключення як самостійного. Однак, з іншого боку, "маршрутизація" на такому високому рівні може дати й чималі переваг. Майже кожний Internet-провайдер має один або декілька Проксі- серверів, через які рекомендує працювати своїм клієнтам. Незважаючи на те, що це зовсім необов'язково (як правило, клієнт провайдера може звертатися до Internet прямо), це дає виграш у продуктивності, а при погодинній оплаті, відповідно, заощаджувати час он-лайн. Це відбувається тому, що Проксі-сервери здатні кешувати (запам'ятовувати) запитувані користувачем документи, і при наступних до них зверненнях видавати копію з кешу, що швидше, ніж повторно запитувати з Internet-сервера. Крім того, Проксі-сервери можуть бути налагоджені так, що будуть блокувати завантаження банерів найпоширеніших баннерных служб, тим самим також (часом значно) прискорюючи завантаження Web-сторінок.

При установці HTTP Проксі-сервера в локальній мережі й роботі через нього за рахунок кешування заощаджується не тільки час, але й трафік – тому, що кешування відбувається в самій локальній мережі, до каналу з провайдером, у якім враховується трафік (при оплаті за обсяг перекачаної інформації).

2. Хід роботи

2.1. Налагодження підключення через Win2003 Server. NAT

Для створення умов, заданих у лабораторній роботі, необхідно виконати ряд дій:

1. Додаємо Win2003 Server і додаємо мережевий адаптер, який підключаємо за схемою «NAT». Другий підключаємо до «LAN1»

2. Після завантаження Win2003 Server налагоджуємо новий мережевий адаптер на автоматичне одержання IP-адреси.

3. Перевіряємо доступ до Internet.

4. Запустіть режим керування сервером.
5. Виберіть додати нову роль (рис. 2).
6. У списку ролей виберіть наступний пункт (рис. 3).
7. Виберіть варіант «NAT» (рис. 4).
8. Виберіть інтерфейс підключений до Internet (рис. 5).
9. Відключіть брандмауер.
10. Уведіть наступні параметри на клієнтській машині (рис. 6).

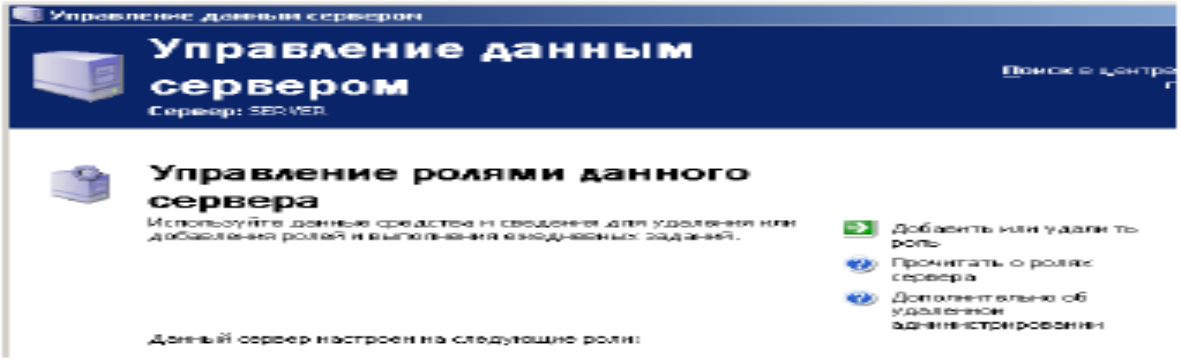


Рис. 2. Додавання ролі

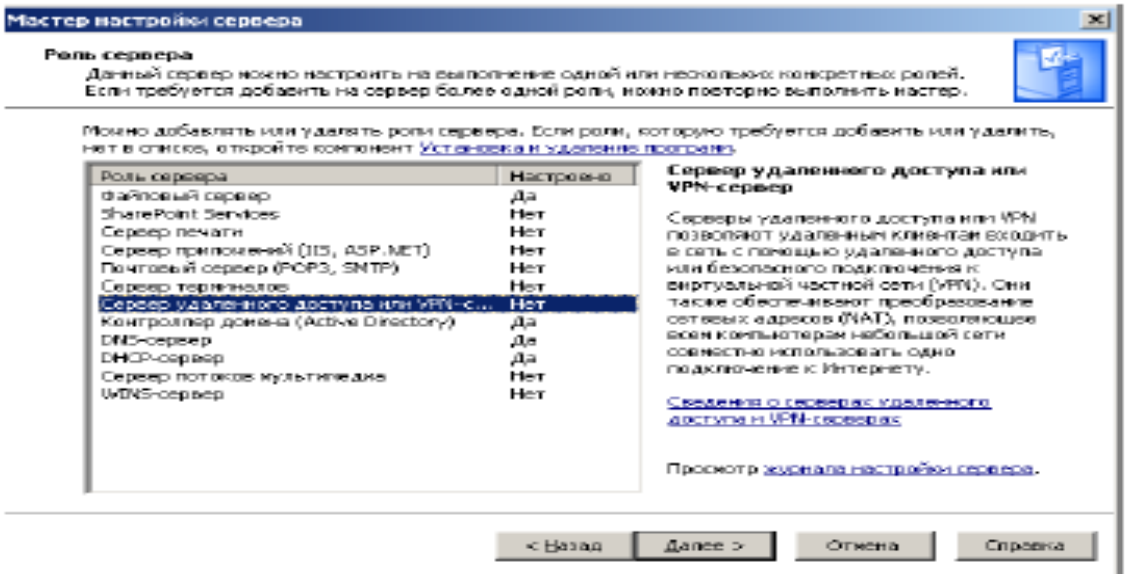


Рис. 3. Вибір параметру ролі

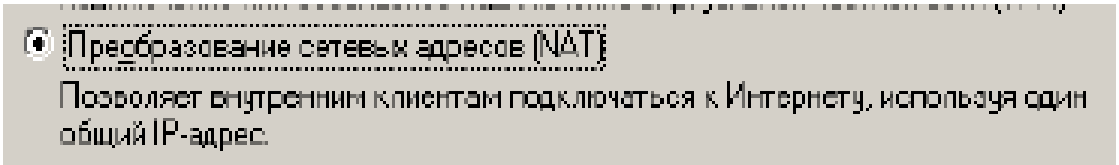


Рис. 4. Відбір варіанту NAT

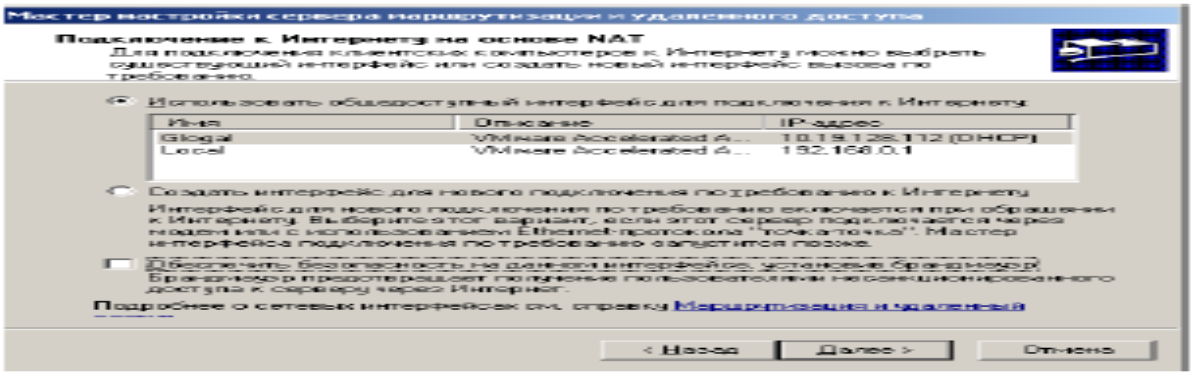


Рис. 5. Відбір інтерфейсу

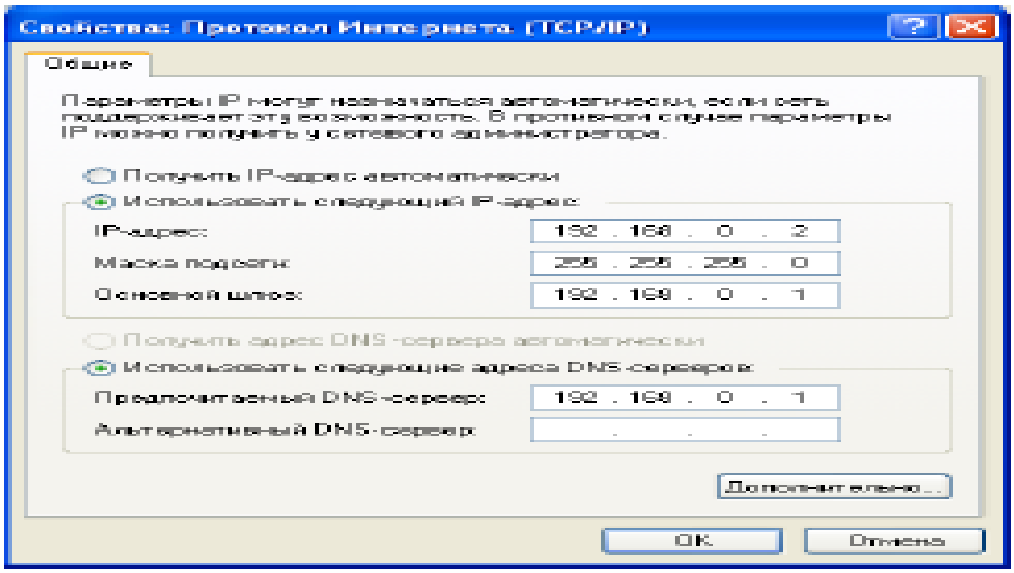


Рис. 6. Введення параметрів

11. Перевірте працездатність NAT за допомогою команд (із клієнтської машини): ping 192.168.0.1 ping [адреса адаптера сервера, підключеного до Internet].

2.2. Налагодження підключення через Winxp. Internet Connection Sharing

Для виконання наступних двох етапів необхідно проробити наступні дії:
Виключіть Win2003 Server і вилучите його з Вашої групи.
Створіть клон Winxp.
Виконуйте дії згідно з рисунком 7.

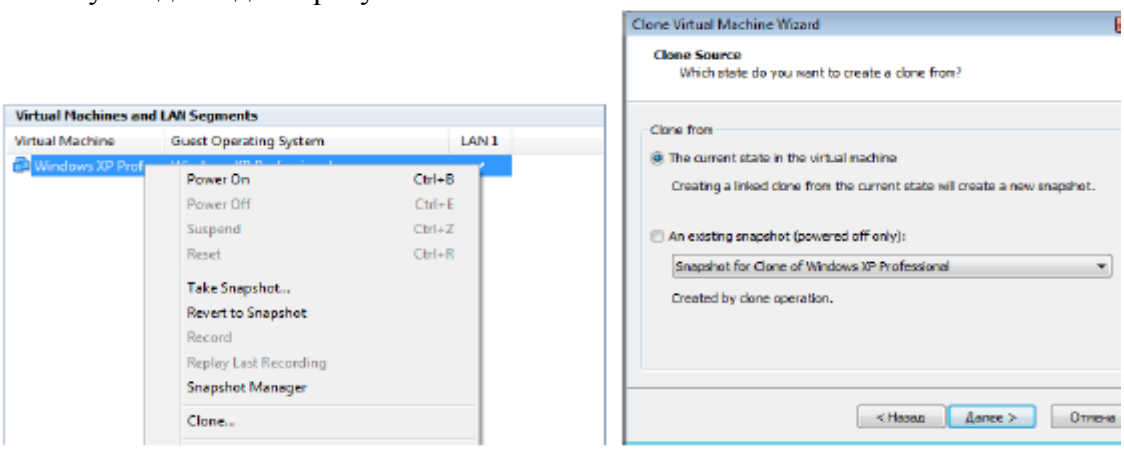


Рис. 7. Створення клону Winxp

Додайте нову ОС у групу (рис. 8).

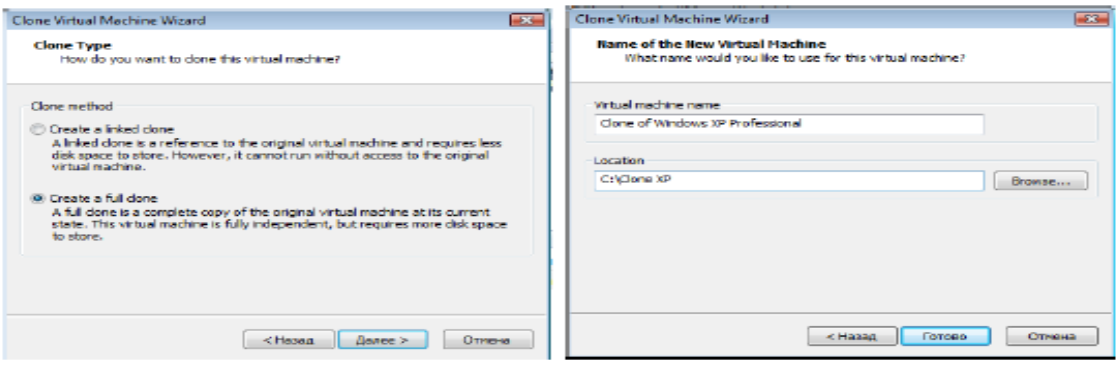


Рис. 8. Додавання ОС

Додати мережевий адаптер, як показано на рис. 9.

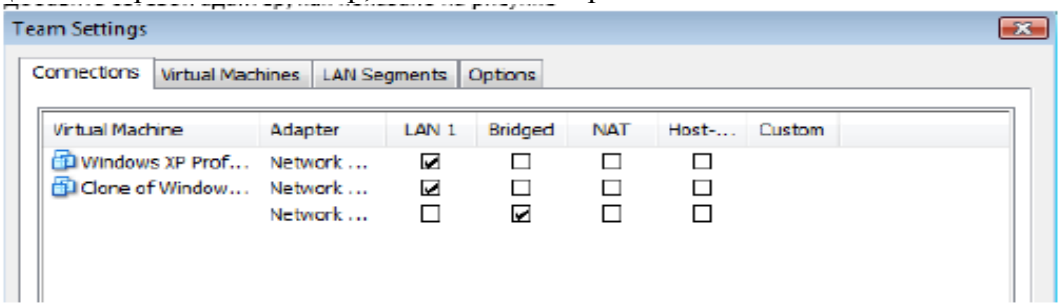


Рис. 9. Додавання адаптера

Запустіть віртуальні машини.
Налагодьте на шлюзі адаптери, як показано на рисунку 10.

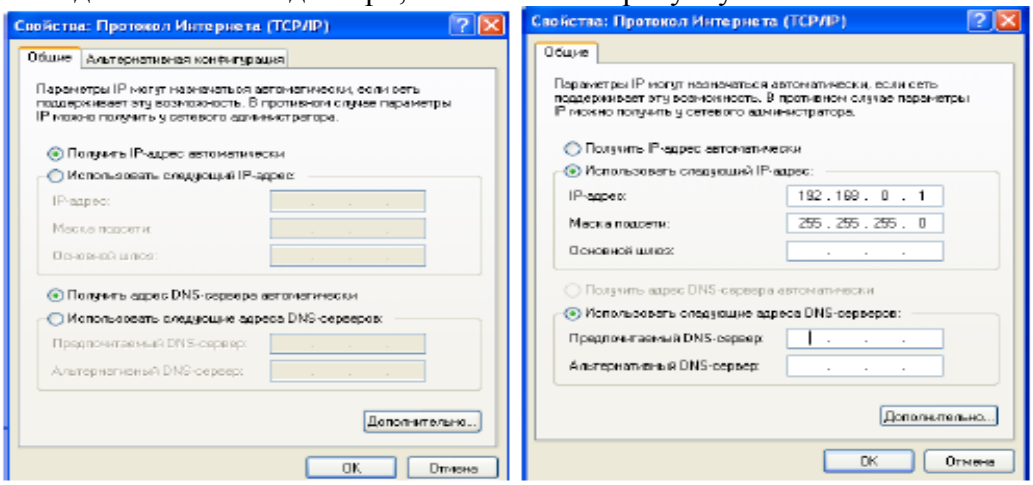


Рис. 10. Налаштування адаптерів

Для зручності перейменуйте їх (рис. 11).

Рис. 11 Перейменування адаптерів

На шлюзі, відкриваємо **Панель управления > Сеть и дистанционный доступ к сети** *(Control Panel > Network Connections)*,

виберіть ваше підключення правою кнопкою миші й натисніть **Свойства** *(Properties)*. У закладці **Дополнительно** (рис. 12) *(Advanced)* встановіть прапорець **Общий доступ у моей сети для этого подключения** *(Allow Other Network Users To Connect Thought This Computer's Internet Connection)*.

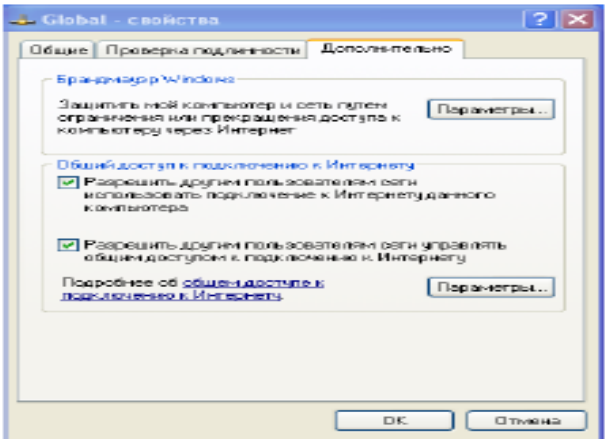


Рис. 12. Вкладка **Дополнительно**

ICS сконфігурований і призначає комп'ютеру, що забезпечує доступ, статичну внутрішню адресу 192.168.0.1. (рис. 13) Усі клієнти розміщаються в одній фізичній підмережі, одержують адреси з діапазону 192.168.0.0/24 (/24 означає перші 24 одиниці в масці мережі, представленої у двійковій формі, тобто це маска 255.255.255.0) і використовують для дозволу імен тільки DNS-Сервер, розміщений на цьому ж комп'ютері.

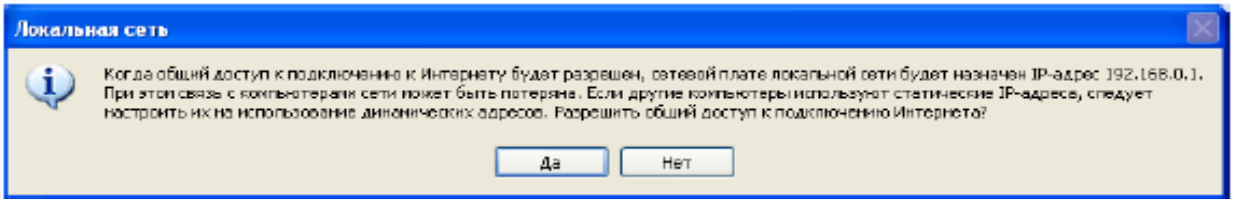


Рис. 13. Призначення IP-адреси

На клієнтських машинах установлюємо Автоматичне одержання Ip-Адреси.

2.3. Налагодження підключення через Winxp. Проксі-Сервер

На першому етапі необхідно встановити Проксі-сервер на комп'ютері підключеному до мережі Internet.

Використовуйте дискету або флешку для переносу програми.

Установіть й налагодьте програму.

Налагодження підключення через Winxp. NAT

Спробуйте самостійно налагодити цей режим

Вивід. Тепер Ви повинні зуміти побудувати мережу з декількох комп'ютерів, а також організувати доступ до мережі Internet.

3. Контрольні питання

1. Які варіанти підключення до мережі Internet з локальної мережі існують?
2. Які переваги та недоліки «Прямого» Ip-Підключення до Internet?
3. Які переваги та недоліки підключення через NAT (Ip-Маскарадінг)?
4. Які переваги та недоліки підключення через Проксі-сервер?
5. Який порядок налагодження підключення до Internet через Win2003 Server. NAT?
6. Який порядок налагодження підключення до Internet через Winxp. Internet Connection Sharing?
7. Який порядок налагодження підключення до Internet через Winxp. Проксі-Сервер?

ЛАБОРАТОРНА РОБОТА 25.
НАЛАГОДЖЕННЯ ВІДДАЛЕНОГО З'ЄДНАННЯ ІЗ СЕРВЕРОМ

Мета роботи: навчитись встановлювати з'єднання із сервером.

1.ТЕОРІЯ
1.1.Загальні відомості
1.2.MNP-протоколи
1.3. Протокол V90
1.4. Режими MNP-модемів
1.5. Внутрішні і зовнішні модеми
1.6. Марки модемів
2. Хід роботи
3. Контрольні питання

1.Теорія

1.1. Загальні відомості

В 80-х роках американська фірма Hayes випустила перший модем для комп'ютера IBM PC. Звичайно ж телефонні лінії розроблялися для передачі на відстань тільки звуків людського голосу. Взагалі кажучи, природні звуки характеризуються тональністю і інтенсивністю, які безперервно змінюються. Для передачі за телефонною лінією вони перетворюються в електричний сигнал з частотою і силою струму, що безперервно і відповідно змінюється. Такий сигнал називається аналоговим.

Комп'ютер же на відміну від модему розуміє тільки цифровий сигнал, тобто струм тільки двох рівнів. Кожний з них позначає одне з двох зрозумілих комп'ютеру значень – логічні “0” і “1”. Щоб передати цифровий сигнал за телефонною лінією, йому потрібно надати прийнятний для неї аналоговий вигляд.

Саме цією роботою займається модем (див. додаток 2). Так само він виконує зворотну процедуру, тобто переводить аналоговий сигнал в зрозумілий комп'ютеру цифровий. Слово “модем” – походить від скорочення двох термінів: Модулятор/Демодулятор. Модем організовує місток між цифровим сигналом, який видає комп'ютер і аналоговим сигналом, який, як було сказано вище розуміє телефонна лінія.

При передачі даних з комп'ютера в модем, перший видає послідовність нулів і одиниць, а останній перетворює їх в аналоговий сигнал. Потім дані відсилаються в телефонну лінію, і їх приймає модем, що стоїть на іншому кінці дроту. Коли модем приймає дані, то він фільтрує корисну інформацію від шумів в лінії. Для цього існують спеціальні протоколи корекції помилок. Самий просунутий з них – MNP10. Окрім цього існують MNP1, MNP2, MNP3, MNP4, MNP5, MNP7. В даний час понад усе поширений MNP5, оскільки MNP7 і MNP10 встановлюються на спеціальних модемах, які працюють за виділеними лініями, наприклад, в глобальній мережі Internet. Після того, як модем відділив корисну інформацію від шумів в лінії він відбирає дані, які прийняв, від службової інформації. Так відбувається обмін даними при з'єднанні на протоколі Zmodem, Sealink, Ymodem і багатьох інших однонаправлених протоколах.

Звичайно, обидва комп'ютер можуть одночасно приймати і посилати дані. Тому що вони використовують певні угоди про частоти, різні для вхідних і вихідних сигналів. Для цього існують спеціальні двонаправлені протоколи. Наприклад Bimodem, Puma, Janus, Zedzap.

1.2. MNP- протоколи

MNP (Microsoft Network Protocols) – серія найпоширеніших апаратних протоколів, вперше реалізована на модемах фірми Microsoft. Ці протоколи забезпечують автоматичну корекцію помилок і компресію даних, які передаються. Зараз відомо 10 протоколів:

MNP1. Протокол корекції помилок, що використовує асинхронний напівдуплексний метод передачі даних. Це найпростіший з протоколів MNP.

MNP2. Протокол корекції помилок, що використовує асинхронний дуплексний метод передачі даних.
MNP3. Протокол корекції помилок, що використовує синхронний дуплексний метод передачі даних між модемами (інтерфейс модем – комп'ютер залишається асинхронним). Оскільки при асинхронній передачі використовується десять біт на байт – вісім біт даних, стартовий біт і стоповий біт, а при синхронній тільки вісім, то в цьому криється можливість прискорити обмін даними на 20%.
MNP4. Протокол, що використовує синхронний метод передачі, забезпечує оптимізацію фази даних, яка дещо покращує неефективність протоколів MNP2 і MNP3. Крім того, при зміні числа помилок на лінії відповідно міняється і розмір блоків передаваних даних. При збільшенні числа помилок розмір блоків зменшується, збільшуючи вірогідність успішного проходження окремих блоків. Ефективність цього методу складає близько 20% в порівнянні з простою передачею даних.
MNP5. Додатково до методів MNP4, MNP5 часто використовує простий метод стиснення інформації, яка передається. Символи, які часто зустрічаються в передаваному блоці, кодуються ланцюжками бітів меншої довжини, ніж символи, що рідко зустрічаються. Додатково кодуються довгі ланцюжки однакових символів. Звичайно при цьому текстові файли стискаються до 35% своєї початкової довжини. Разом з 20% MNP4 це дає підвищення ефективності до 50%. Відмітимо, що якщо ви передаєте вже стислі файли, а в більшості це так і є, додаткового збільшення ефективності за рахунок стиснення даних модемом не відбувається.
MNP6. Додатково до методів протоколу MNP5 протокол MNP6 автоматично перемикається між дуплексним і напівдуплексним методами передачі залежно від типу інформації. Протокол MNP6 також забезпечує сумісність з протоколом V.29.
MNP7. В порівнянні з ранніми протоколами використовує більш ефективний метод стиснення даних.
MNP9. Використовує протокол V.32 і відповідний метод роботи, що забезпечує сумісність з низькошвидкісними модемами.
MNP10. Призначений для забезпечення зв'язку на сильно зашумлених лініях, таких, як міжміських лініях, сільських лініях. Це досягається за допомогою наступних методів:

- багатократного повторення спроби встановити зв'язок
- зміни розміру пакетів відповідно до зміни рівня перешкод на лінії
- динамічної зміни швидкості передачі відповідно до рівня перешкод лінії

Всі протоколи MNP сумісні між собою від низу до верху. При встановленні зв'язку відбувається установка щонайвищого можливого рівня MNP-протоколу. Якщо ж один з модемів, що зв'язуються, не підтримує протокол MNP, то MNP-модем працює без MNP-протоколу.

1.3. Протокол V90

Технологія V.90 дає можливість модемам приймати дані на швидкості до 56 Кбіт/с на звичайних комутованих лініях. V.90 обходить теоретичні обмеження накладені на стандартні, аналогові модеми, використовуючи цифрові канали, які більшість провайдерів Internet використовує при підключенні до телефонних мереж.

Звичайно, єдина аналогова частина телефонної мережі – той шматок мідного кабелю, що сполучає ваш будинок і центральне відділення телефонної компанії. За останні два десятиріччя телефонні компанії проводили заміну аналогових частин їх ліній на цифрові канали. Але найбільш складно було поміняти невелику ділянку мережі від вашого будинку до телефонної компанії. Він швидше за все не зазнаватиме змін у кращу сторону ще декілька років.

Все, що потрібне для переобладнання модемів – програмний апгрейд (якщо такий передбачений). Програмною модернізацією, можна перетворити аналоговий US Robotics Courier V.Everything на V.90 аналоговий модем.

Як уже було відзначено, дані від цифрового V.90 модему посилаються за телефонною мережею у вигляді двійкових кодів. Але, щоб задовольнити умові x2 цифровий V.90 модем передає дані (8 біт кожного разу) клієнтському аналого-цифровому конвертору з тією ж частотою, що і телефонна мережа (8000 гц). Це означає, що символьна швидкість модему (Symbol Rate) повинна бути рівна частоті телефонної мережі.

У процесі встановлення з'єднання, V.90 модеми випробовують телефонну лінію на предмет знаходження низхідних аналого-цифрових перетворювачів. Якщо модем знаходить їх, він далі проводить з'єднання на протоколі V.34. Аналогічна ситуація відбувається в тому випадку, якщо модем на іншому кінці лінії не є V.90 модемом.

Задача клієнтського модему полягає в пізнанні 256 потенційних сигналів і відновлення 8000 PCM кодів у секунду. Якби йому це вдалося, швидкість від серверу до клієнта складала б 64 Кбіт/с (8000x8 біт у кожному коді). Але, як з'ясувалося, декілька проблем заважають використовуванню такої швидкості.

По-перше, не дивлячись на те, що проблема шуму квантування більш не стоїть, другий набагато менший шум від цифро-аналогового перетворювача все-таки відбувається. Крім того, цей шум чиниться устаткуванням на вашій станції АТС (від якої йдуть кабелі до вашого будинку). Сам по собі шум виникає через деякі нелінійні спотворення і взаємні наведення.

По-друге, мережеві цифро-аналогові перетворювачі не є лінійними конвертерами, а слідують деякому конвертуючому закону. в результаті, коди pcm визначаючі малі сигнали і проводять в цифро-аналоговому устаткуванні, тоді як коди з указівкою на великі за потужністю сигнали викликають при перетворенні.

Ці дві проблеми роблять практично неможливим використовування всіх 256 дискретних кодів, оскільки відповідний вихід від цифро-аналогового перетворювача малих сигналів дуже близький до нуля і втрачається на фоні хай навіть малого шуму. Таким чином, V.90 кодувальник використовує декілька варіантів 256 кодів які видаляють сигнали, найближчі до шуму. Наприклад, для передачі даних на швидкості 56 Кбіт/с використовуються 128-рівневі коди. Використовування меншого числа рівнів дозволяє стабілізувати передачу даних, але на меншій швидкості.

1.4. Режими MNP-модемів

MNP-модем забезпечує наступні режими передачі даних:

- Стандартний режим забезпечує буферизацію даних, що дозволяє працювати з різними швидкостями передачі даних між комп'ютером і модемом і між двома модемами. в результаті для підвищення ефективності передачі даних ви можете встановити швидкість обміну комп'ютер-модем вище, ніж модем-модем. В стандартному режимі роботи модем не виконує апаратної корекції помилок.

- Режим прямої передачі. Даний режим відповідає звичайному модему, що не підтримує MNP-протокол. Буферизація даних не проводиться і апаратна корекція помилок не виконується.

- Режим з корекцією помилок і буферизацією. Це стандартний режим роботи при зв'язку двох MNP-модемів. Якщо віддалений модем не підтримує протокол MNP, зв'язок не встановлюється.

- Режим з корекцією помилок і автоматичною настройкою. Режим використовується, коли наперед не відомо, чи підтримує віддалений модем протокол MNP. На початку сеансу зв'язку після визначення режиму віддаленого модему встановлюється один з трьох інших режимів.

1.5. Внутрішні і зовнішні модеми

Модеми внутрішні і зовнішні (існують так само спеціальні типи модемів у вигляді PC-карт (PCMCIA), але вони призначені для комп'ютерів типу ноутбуків, і тому вони тут не розглядаються.). Внутрішні модеми виконані у вигляді плати розширення, що вставляється в спеціальний слот розширення на материнській платі комп'ютера. Зовнішній модем, на

відміну від внутрішнього, виконаний у вигляді окремого пристрою, тобто в окремому корпусі і з своїм блоком живлення,в той час коли внутрішній модем одержує електрику від блоку живлення комп'ютера. Так які ж достоїнства і недоліки у зовнішніх і внутрішніх модемів?

Внутрішній модем

Достоїнства

1. Всі внутрішні моделі модемів без виключення(на відміну від зовнішніх) мають вбудоване FIFO. (First Input First Output - першим прийшов, першим прийнятий). FIFO це мікросхема, що забезпечує буферизацію даних. Звичайний модем при проходженні байта даних через порт кожного разу запрошує переривання у комп'ютера. Комп'ютер за спеціальними IRQ(Interrupt Request) лініями переривае на деякий час роботу модему, а потім знову відновлює її. Це уповільнює роботу комп'ютера в цілому. FIFO же дозволяє використовувати переривання у декілька разів рідше. Це має велике значення при роботі в багатозадачних середовищах. Таких як Windows98, OS/2, Windows 2000, UNIX і інших.
2. При використовуванні внутрішнього модему зменшується кількість дротів, натягнутих в найнесподіваніших місцях. Так само внутрішній модем не займає дорогоцінне місце на робочому столі.
3. Внутрішні модеми є послідовним портом комп'ютера і не займають існуючих портів комп'ютера.
4. Внутрішні моделі модемів завжди дешевше зовнішніх.

Недоліки

1. Займають слот розширення на материнській платі комп'ютера. Це дуже незручно на мультимедійних машинах, на яких встановлена велика кількість додаткових плат, а також на комп'ютерах, які працюють серверами в мережах.
2. Немає індикаторних лампочок, які при певному навику дозволяють стежити за процесами, які відбуваються в модемі.
3. Якщо модем завис, то відновити працездатність можна тільки клавішею перезавантаження комп'ютера “RESET”.

Зовнішні модеми

Достоїнства

1. Вони не займають слот розширення, і при необхідності їх можна легко відключити і перенести на інший комп'ютер.
2. На передній панелі є індикатори, які допомагають зрозуміти, яку операцію зараз проводить модем.
3. При зависанні модему не потрібно перезавантажувати комп'ютер, достатньо вимкнути і включити живлення комп'ютера.

Недоліки

1. Необхідна мультикарта з вбудованим FIFO. Без FIFO модем звичайно працюватиме, але при цьому падатиме швидкість передачі даних.
2. Зовнішній модем займає дорогоцінне місце на робочому столі і йому потрібні додаткові дроти для підключення. Це теж створює деяку незручність.
3. Він займає послідовний порт комп'ютера.
4. Зовнішній модем завжди дорожче аналогічного внутрішнього, оскільки включає корпус з індикаторними лампочками і блок живлення.

Роль індикаторних лампочок

1. *MR (Modem Ready)*
Показує, що модем включений і готовий до роботи.

2. TR (Terminal Ready)
Цей індикатор горить, коли модем знаходить DTR (Data Terminal Ready), який передається комунікаційною програмою.

3. HS (High Speed)

Цей індикатор спалахує, коли модем працює з максимально можливою для нього швидкістю.

4. CD (Carrier Detect)
   Він повинен горіти під час з'єднання модемів і протягом всього сеансу зв'язку, поки один з модемів не “покладе трубку”.
5. AA (Auto Answer)
   Показує, що модем включений в режим автовідповіді, тобто буде сам відповідати на всі вхідні дзвінки. Якщо модем знаходить Ring (Англ. - дзвінок), то цей індикатор мерехтить.
6. OH (Hook)
   Цей індикатор еквівалентний знятій трубці телефону. Він горить, коли модем займає лінію.
7. RD (Receive Data)
   Мерехтить при прийомі комп'ютером даних.
8. SD (Send Data)
   Цей індикатор мигає, коли комп'ютер посилає дані.

1.6. Марки модемів

На сьогоднішній день фактичним стандартом є модем із швидкістю з'єднання 14400 і протоколами передачі даних V32 і V32bis (і поліпшені наприклад, HST і V32terbo). Орієнтуватися сьогодні варто на цей стандарт. Але і він, як і все в комп'ютерному світі нестійке, і поступово відмирає. Звичайно, краще всього брати модем із швидкістю з'єднання 28800 і протоколами передачі даних V34(і його підмножини V.Fast і V.Everything). Також є поліпшений різновид протоколу V34+. Він дозволяє вести прийом/передачу на швидкостях до 33600. Модеми деяких фірм мають спеціалізовані протоколи для особливих умов експлуатації (звичайно на сильно зашумлених лініях. На них ці протоколи поводяться бездоганно. Але яка тоді розмова про нормальні “чисті” лінії? Такими протоколами є HST, розроблений фірмою USRobotics®. Так само існують два протоколи розроблені Zyxel® **.** ***Це*** Zyx і ZyCell. Zyx це протокол з можливістю зв'язку з аналогічними моделями на швидкостях 16800 і 19200. А ZyCell – спеціальний протокол для супутникового і настільного зв'язку. Єдиним недоліком таких протоколів є те, що вони зв'язуються на фірмових протоколах тільки з аналогічними моделями.).

Тепер можна розглянути деякі марки модемів.

GVC

Ця фірма відома перш за все тим, що проводить недорогі, але достатньо надійні моделі. Наприклад модель GVC 14440 F1114HV – модель, що добре зарекомендувала в наших умовах. Вона практично безпомилково “ловить” сигнал BUSY. Це факс-модем, і він має факс класу II. Так само в ньому реалізовано підстроювання рівня сигналу до якості лінії. Однією з його переваг є безшумне герконове реле.

ZyXEL

Декілька років тому це була одна з найпопулярніших і престижних моделей, але на сьогоднішній день фірма сильно здала свої позиції, в основному на фоні досягнень USRobotics. Всі різновиди модемів фірми ***ZyXEL*** розбиті на серії.

Серія 1496 – окрім стандартних протоколів V32 і V32bis, має власні протоколи: Zyx і ZyCell. В цих моделях є голосовий режим (VOICE) для того, що б посилати і приймати голосові повідомлення. Так само є режим визначення номера (АОН – Автоматичний визначник номера).

Моделі серії 1496 володіють адаптивним факсом, це означає що модем дозволяє автоматично ідентифікувати абонента і перемикатися відповідно на факс, модем або голос.

Так само модеми ***ZyXEL*** можуть працювати на виділених чотирьохдротових лініях, розвиваючи при цьому швидкість передачі до 115200 бод.

USRobotics®

Ця фірма випускає декілька серій модемів: USR Sportster, USR Courier, USR WorldPort і інші. Моделі WorldPort призначені для портативних комп'ютерів. Через це вони

не набули широкого поширення. Високопродуктивна серія Courier з деяких викладених нижче причин не набула в нашій країні великого поширення. Залишається тільки серія Sportster. Модеми цієї серії охоплюють всю гамму швидкостей від 14400 до 33600. Вони бувають як внутрішніми, так і зовнішніми і мають безліч модифікацій, що розрізняються як програмно, так і апаратно. Досить зручно, що модеми серії Sportster мають програмно-апаратного апгрейда до більш дорогої і набагато більш функціональної серії Courier. Після апгрейда звичайний USR Sportster перетворюється в Courier. При цьому він має таку важливу перевагу як вбудований протокол HST (High Speed Technology).

2. Хід роботи

Базові знання:

Перед початком Налагодження віддаленого з'єднання необхідно установити модем. Після цього виконується Налагодження віддаленого з'єднання.

Порядок виконання: при наявності операційної системи Windows

Установка контролера віддаленого доступу

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка -> Панель управления**.
2. Відкрийте об'єкт **Установка и удаление программ**. У вікні, що з'явилося:

2.1. На вкладці **Установка Windows** у вікні **Компонента** виберіть пункт **Связь** і натисніть кнопку **Состав**

2.2. У вікні, що з'явилося, виберіть пункт (установіть прапорець) **удаленный доступ к сети** і натисніть кнопку **OK**.

3. Почекайте, поки система встановлює програмне забезпечення. За завершенням перезавантажите комп'ютер.

Установка модему

4. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка -> Панель управления**..
5. Відкрийте об'єкт **Модемы** (з'явиться діалогове вікно Установка нового модему).
1. Установіть прапорець **Не определять тип модема (вибір зі списку**). Натисніть кнопку **Далее** >.
2. Прочитайте і законспектуйте повідомлення. Виберіть відповідні пункти у вікнах **Изготовители**: (Standard Modem Types) і **Модели**: Standard 28800 bps Modem. Натисніть кнопку **Далее** >.
3. У вікні Вкажіть порт, до якого він приєднаний: укажіть **Послідовний порт** (COM2). Натисніть кнопку **Далее** >.
4. Почекайте, поки йде установка модему. За завершенням натисніть кнопку **Готово.**

Створення віддаленого з'єднання

6. Відкрийте об'єкт **Мой компьютер**.
7. Відкрийте об'єкт **Удаленный доступ к сети.**
8. Відкрийте об'єкт **Новое соединение**. У вікні, що з'явилося:

8.1. Уведіть назву з'єднання **Лаб25**; виберіть у списку, що випадає, установлений модем. Натисніть кнопку **Далее**

8.2. Уведіть Код міста: 044; Телефон: 2130866, Код країни: Україна. Натисніть кнопку **Далее**

8.3. Натисніть кнопку **Готово**

Налагодження віддаленого з'єднання

9. У вікні **Удаленный доступ к сети** виберіть об'єкт **Лаб25**. Виберіть у меню **Файл** пункт **Свойства.** У вікні, що відкрилося:

9.1. На вкладці **Общие** перевірте код міста, код країни, телефон.

9.2. На вкладці **Тип сервера** відзначте тип віддаленого сервера; установіть **Допустимые сетевые протоколы**: TCP/IP.
9.3. Натисніть кнопку **ОК**.

Установка віддаленого з'єднання

10. У вікні **Удаленный доступ к сети** відкрийте об'єкт **Лаб25**. У вікні, що відкрилося:
10.1. Уведіть Ім'я користувача: **dial-up**
10.2. Уведіть Пароль: **12345**
10.3. Натисніть кнопку **Установить связь**

Фази встановлення з'єднання:

11. Набір номера.
12. Узгодження параметрів зв'язку.
13. Перевірка імені користувача і пароля.
14. Вхід у мережу.
15. Установка з'єднання.

Завершення роботи

16. Натисніть кнопку Пуск на панелі задач. Виберіть пункт **Настройка -> Панель управления**..
17. У вікні **Удаленный доступ к сети** виберіть об'єкт **Лаб25**. Виберіть у меню **Файл** пункт **Удалить.**
18. Відкрийте об'єкт **Модемы**. Виберіть **Standard 28800 bps Modem**. Натисніть кнопку **Удалить** Натисніть кнопку **Закрыть**
19. Відкрийте об'єкт **Сеть**. Виберіть **Контроллер удаленного доступа**. Натисніть кнопку **Удалить** Натисніть кнопку **ОК**
20. Уточніть у викладача порядок завершення роботи з комп'ютером. Приведіть комп'ютер у вихідний стан.

Примітка: якщо встановлена операційна система Windows XP, то драйвер модему встановлюється операційною системою автоматично.

Налагодження віддаленого з'єднання при наявності операційної системи Windows XP, та роботі в мережі Internet без використання локальної мережі.

1. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка -> Панель управления**.
2. Відкрийте піктограму **Сетевые подключения**.
3. Запустіть **Майстра нових підключень** на виконання.
4. В другому вікні майстра виберіть пункт **Подключение к Internet.**
5. В третьому вікні майстра виберіть пункт **Ввести параметры вручную.**
6. В четвертому вікні майстра виберіть пункт **Подсоединится к телефонной линии исспользуя модем.**
7. В п'ятому вікні майстра введіть назву з'єднання , яке створюєте.
8. В шостому вікні майстра вкажіть телефон дозвону.
9. В сьомому вікні майстра вкажіть логін та пароль з підтвердженням (надається провайдером).

Налагодження віддаленого з'єднання при наявності операційної системи Windows XP, та роботі в мережі Internet з використанням локальної мережі.

1. Встановити мережеву карту та її драйвер.
2. Натисніть кнопку **Пуск** на панелі задач. Виберіть пункт **Настройка -> Панель управления**.
3. Відкрийте об'єкт **Свойства пользователя.**
4. Відкрийте вкладку **Подключение.**
5. Введіть команду **Свойства сети.**
6. Встановіть прапорець **Исспользовать Прокси-Сервер.**

7. Введіть адресу Проксі-Сервера **(server)** та його порт (**3128**).
8. Введіть команду **ОК**.

3. Контрольні питання

1. Принцип роботи модемів.
2. Поняття MNP-протоколи.
3. Режими роботи модемів.
4. Внутрішні і зовнішні модеми.
5. Роль індикаторних лампочок модему.
6. Марки модемів.
7. Порядок Налагодження віддаленого доступу в мережу.
8. Протоколи канального рівня: UUCP, SLIP, PPP.
9. Особливості налагодження з'єднання з Internet при використанні локальної мережі і без неї.

ЛАБОРАТОРНА РОБОТА 26. СТВОРЕННЯ INTERNET ПІДКЛЮЧЕННЯ НА ПРИКЛАДІ АБОНЕНТІВ CDMA WLL, З'ЄДНАННЯ ЧЕРЕЗ РАДІОМОДЕМ, В MICROSOFT WINDOWS XP ТА WINDOWS 7

Мета роботи: навчитись створювати підключення через радіомодем, з сервером в операційних системах Microsoft Windows XP та Windows 7.

Зміст

1. Хід роботи
1.1. Створення Internet підключення в Microsoft Windows XP
1.2. Створення Internet підключення в Microsoft Windows 7
2. Контрольні питання

1. Хід роботи

1.1. Створення Internet підключення в Microsoft Windows XP

1. Встановлюємо драйвер радіомодема (рис. 1) (див. додаток 3).

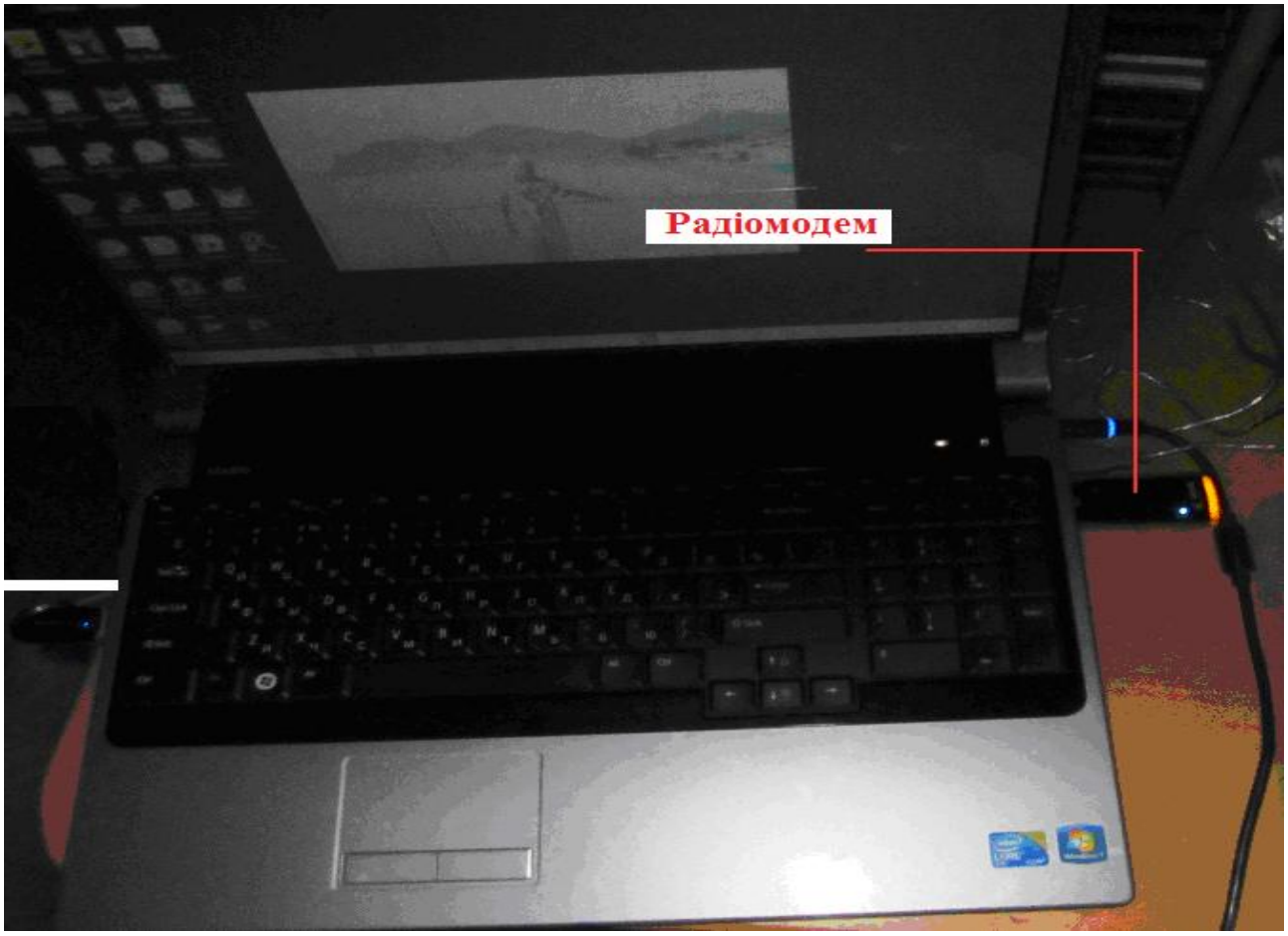


Рис. 1. Ноутбук з радіомодемом

Для створення Internet підключення натискаємо **ПУСК** і вибираємо пункт меню **Панель управления.**

У **Панели управления** вибираємо пункт **Свойства обозревателя** (рис. 2)

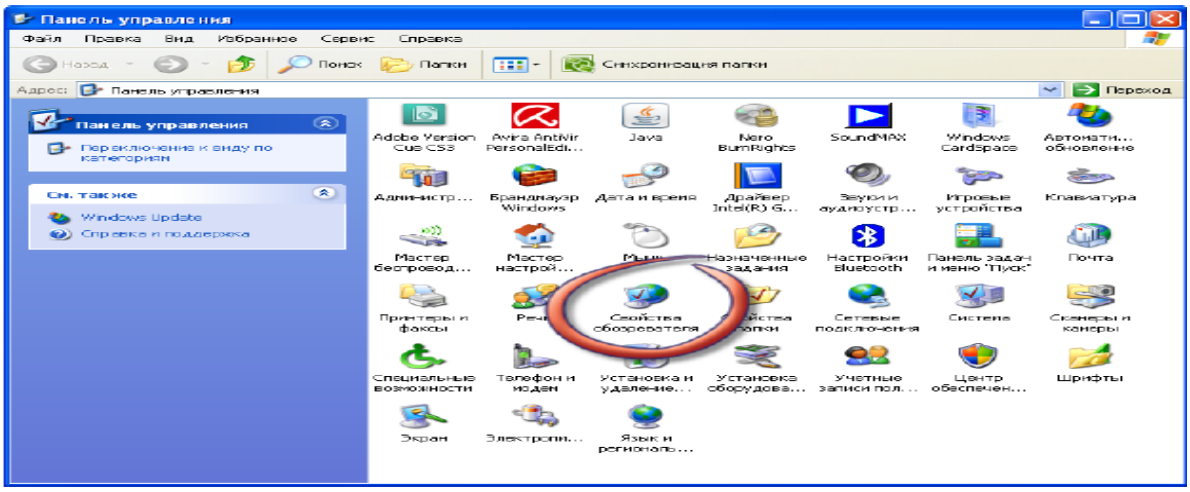


Рис. 2. Панель керування

Вибираємо вкладку **Подключения** й тиснемо кнопку **Добавить** (рис. 3)

У вікні, що **з'явилося, Тип подключения** вибираємо перший **пункт Телефонное подключение к часной сети** (рис. 4).

Тиснемо **Далее**. Потім уводимо номер телефону **#777** (рис. 5).

Натискаємо **Далее**. У наступнім вікні називаємо Наше підключення, наприклад Almatytelecom, і кликаєм на кнопку **Готово** (рис. 6).

Далі, у вікні, що з'явилося, заповнюємо **поля Имя пользователя Пароль**. В обох випадках необхідно написати **cdma**. (рис. 7)

Наступне поле **Домен** залишаємо порожнім. Тиснемо **ОК**. З'являється вікно **Свойства: интернет**: Знову натискаємо **ОК**. (рис. 8). Телефонне підключення готове.

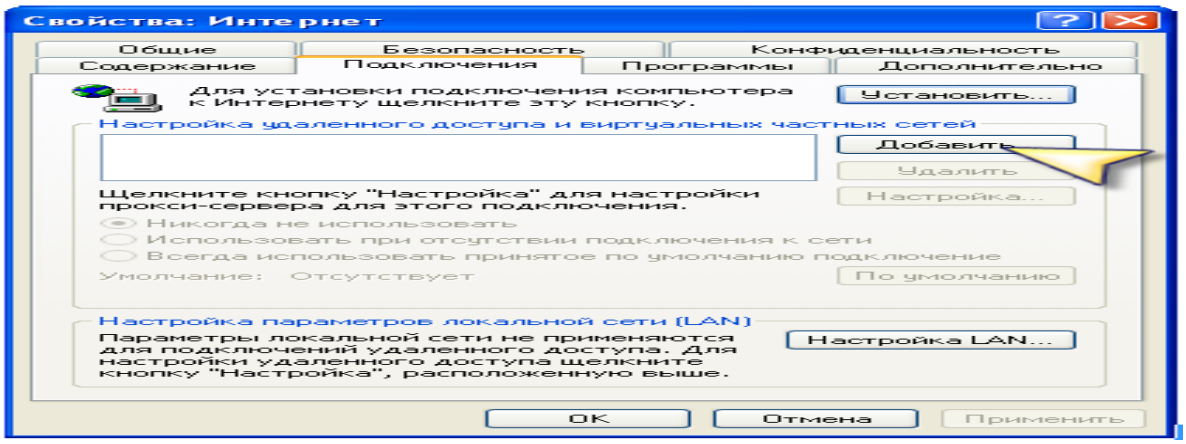


Рис. 3. Додавання підключення

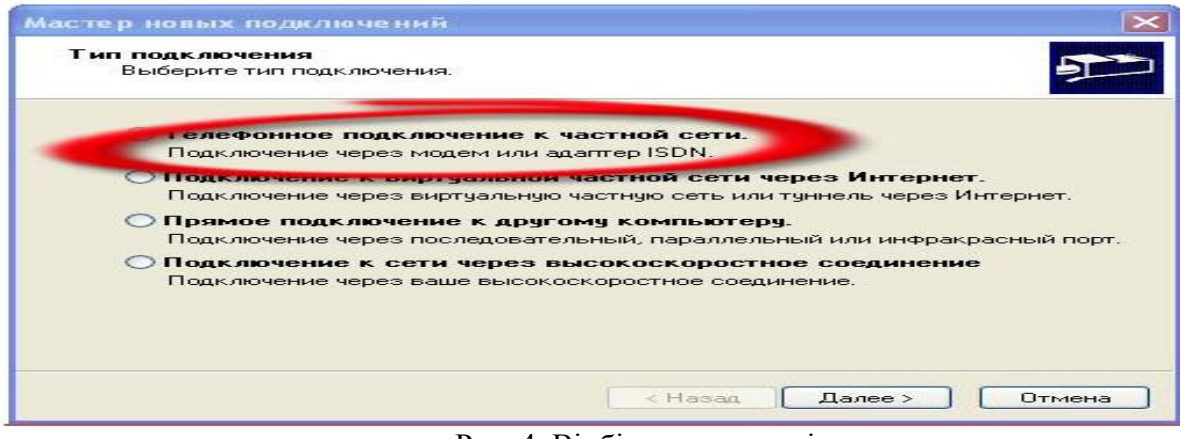


Рис. 4. Відбір типу мережі

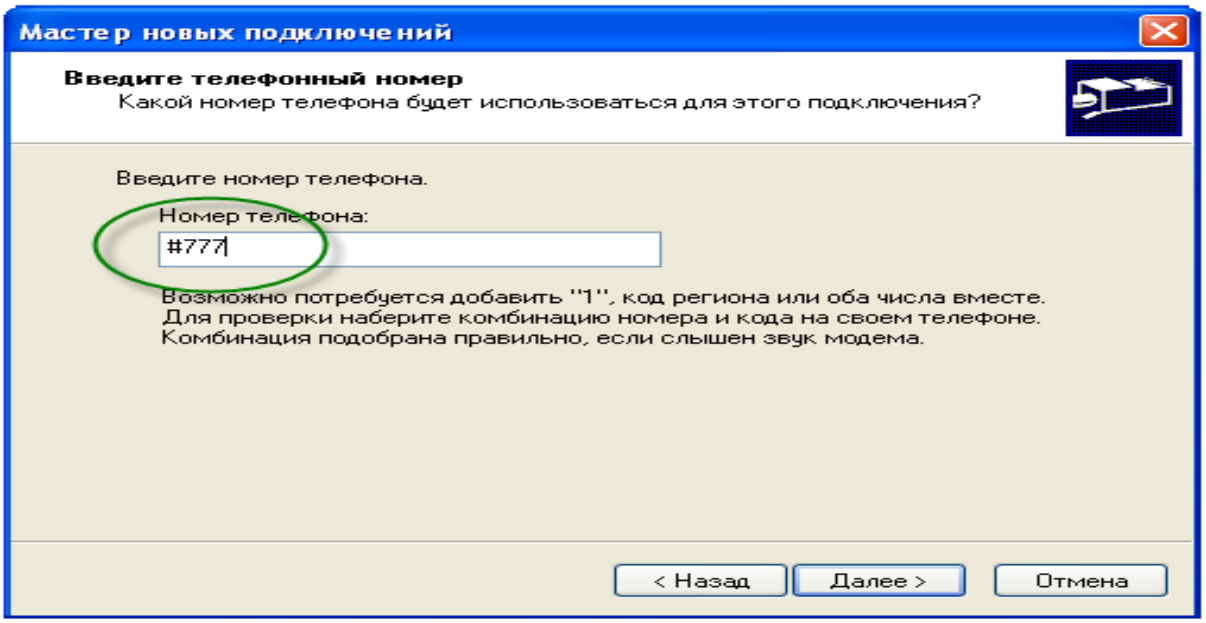


Рис. 5. Введення номеру дозвону

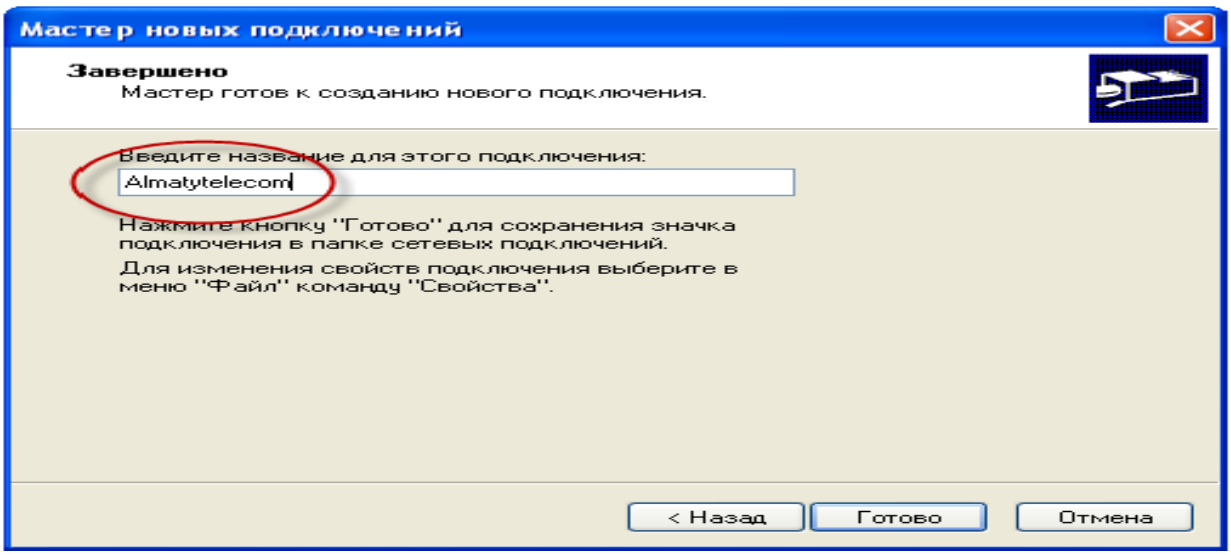


Рис. 6. Назва підключення

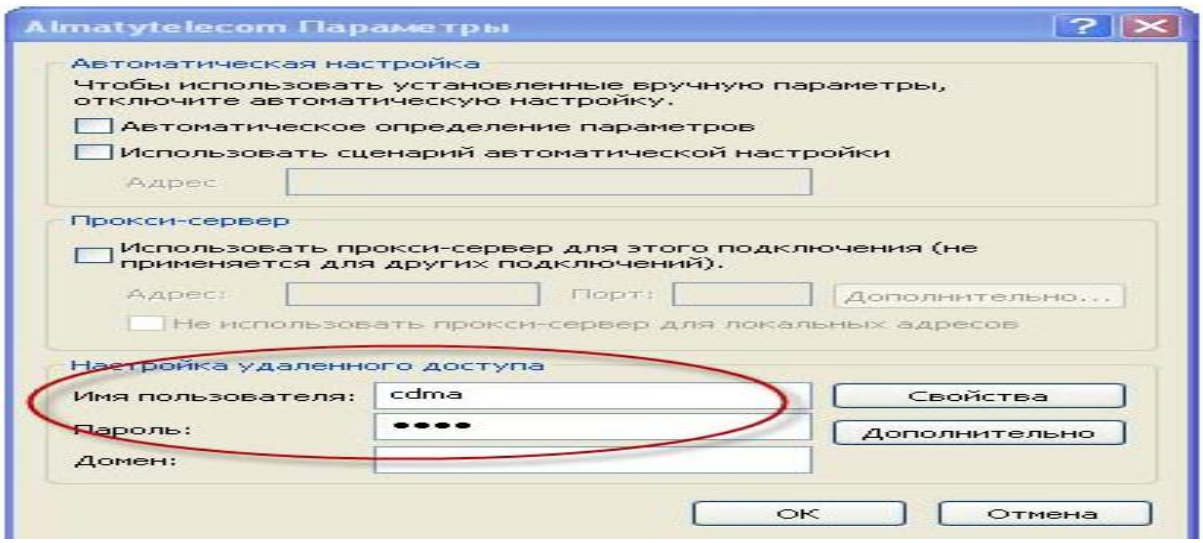


Рис. 7. Введення паролю

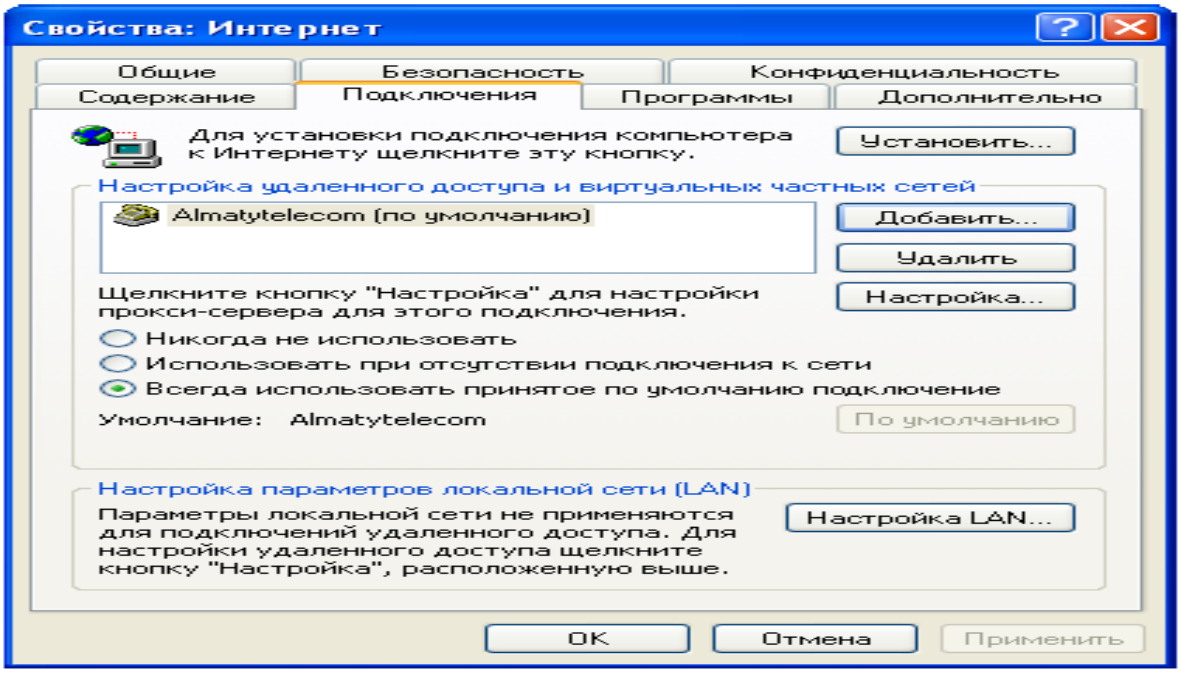


Рис. 8. Заключне вікно налаштування

Тепер для того щоб вийти в Internet тиснемо **Пуск**, потім меню **Подключения** й вибираємо створене нами Almatytelecom. У вікні, що з'явилося, (рис. 9) натискаємо на кнопку **Вызов.**

Рис. 9. Вікно визову з'єднання

Після встановлення з'єднання можна приступати до web серфінгу.

1.2. Створення Internet підключення в Microsoft Windows 7

1. Встановлюємо драйвер радіомодема.

2. Для створення Internet підключення натискаємо **Пуск** і вибираємо пункт меню **Панель управления.**

У **Панели управления** вибираємо пункт **Сеть и Интернет и Подключение к Интернету**(рис. 10)

Рис. 10. Відбір параметрів

3. Вибираємо: **Нет, создать новое подключение** (рис. 11)

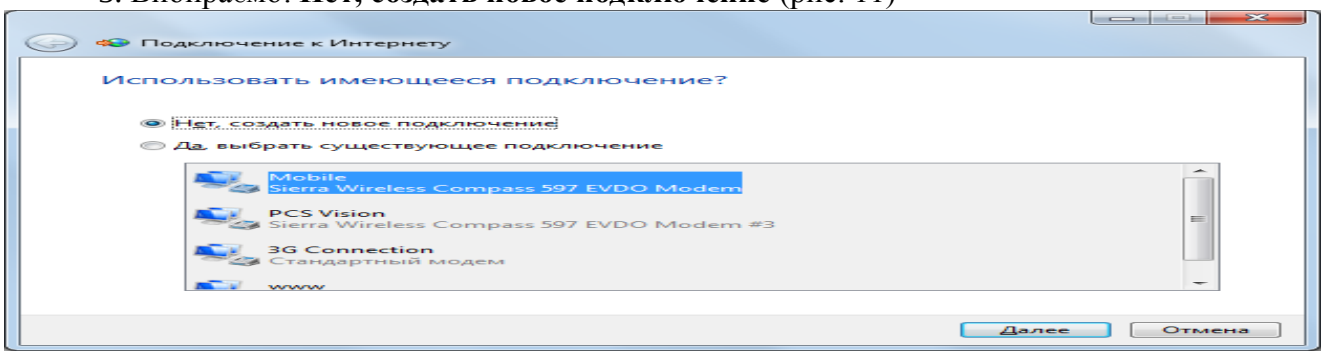


Рис. 11. Відбір створення нового підключення

Натискуємо кнопку **Далее** і слідуємо вказівкам майстра.
В результаті роботи майстра отримаємо відповідне підключення (рис. 12)

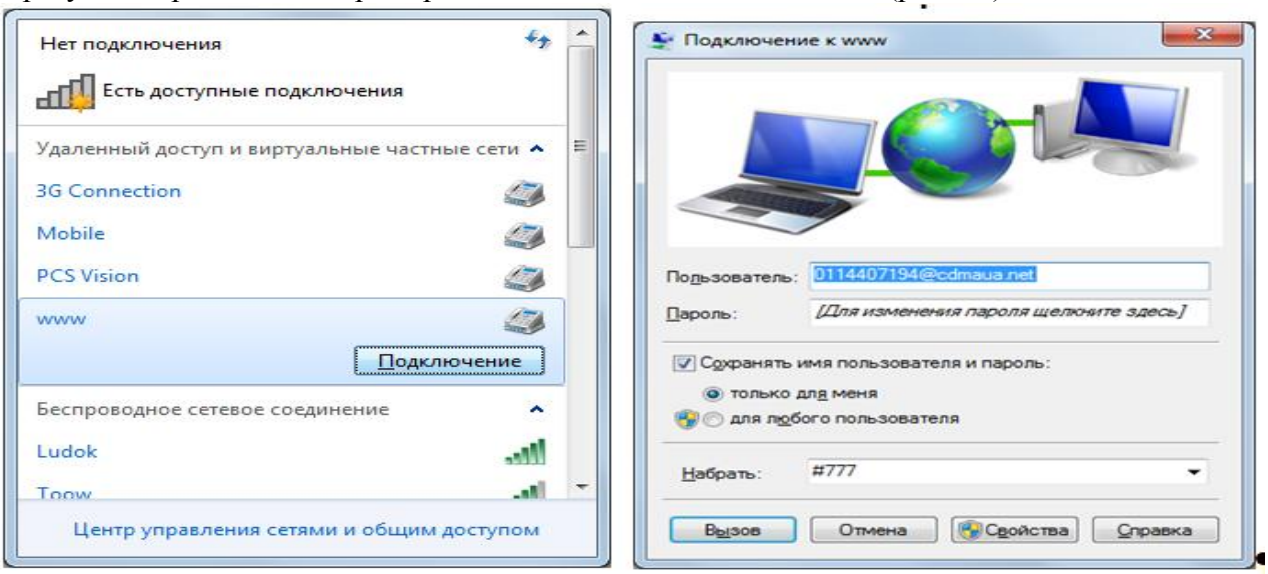


Рис. 12. Підключення до мережі

Керувати таким підключенням зручно з панелі задач (рис. 12).

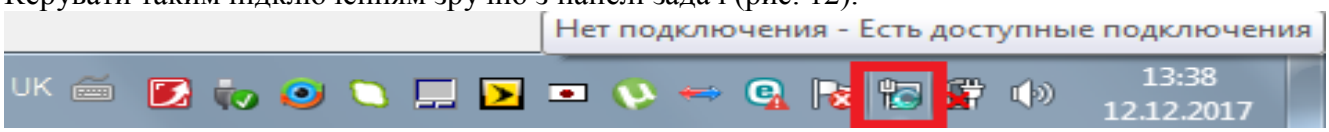


Рис. 13. Панель задач

2. Контрольні питання

1. Який порядок створення Internet підключення, з'єднання через радіомодем, в Microsoft Windows XP?
2. Який порядок створення Internet підключення, з'єднання через радіомодем, в Microsoft Windows 7?

ЛАБОРАТОРНА РОБОТА 27. МОНІТОРИНГ МЕРЕЖ

Мета роботи: Освоїти базові навички моніторингу мережі з використанням програм для аналізу протоколів.

Зміст

1. Теорія
1.1. Вступ
1.2. WIRESHARK NETWORK ANALYZER
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Вступ

Під моніторингом мережі розуміють процес збору й аналізу мережевого трафіка, за результатами якого можна судити про ефективність роботи всієї мережі або її окремих компонентів.

Для моніторингу використовують спеціальні програми - аналізатори мережі. Таких програм багато, наприклад Windows Network Monitor, tcpdump, Ethereal Network Analyzer (ENA), Wireshark і т.п. Вони схожі за функціями, а відрізняються в основному користувацьким інтерфейсом і можливостями генерації статистичних звітів. На рис. 1 наведені приклади таких програм.

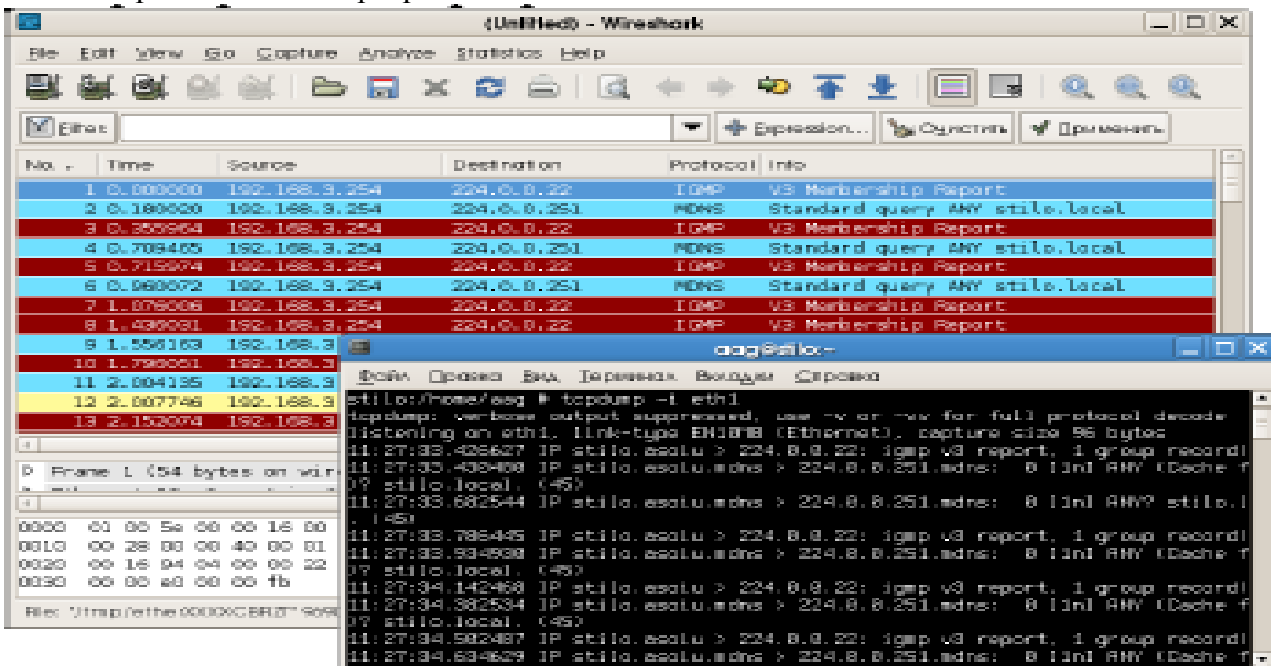


Рис. 1. Програми аналізу трафіка. Головне вікно програми Wireshark з результатами захвата й програма tcpdump (у консолі).

1.2. Wireshark Network Analyzer

Wireshark (практично повний аналог **Ethereal Network Analyzer**)- це мережевий аналізатор із графічним інтерфейсом. Він дозволяє в інтерактивному режимі переглядати пакети, передані за мережею або аналізувати раніше захоплені пакети, завантаживши їх зі збереженого файлу. Основний формат файлу Wireshark такий же, як в libpcap, але підтримується й інші формати. Wireshark може читати/імпортувати наступні формати:

libpcap, tcpdump і інші, що використовують формат tcpdump
snoop і atmsnoop
shomiti/Finisar Surveyor captures
novell Lanalyzer captures

microsoft Network Monitor captures
AIX's iptrace captures
cinco Networks Netxray captures
network Associates Windows-based Sniffer captures
network General/Network Associates Dos-based Sniffer (compressed or uncompressed) captures
AG Group/Wildpackets Etherpeek/Tokenpeek/Airopeek/Etherhelp/Packet-Grabber captures
RADCOM's WAN/LAN analyzer captures
network Instruments Observer version 9 captures
lucent/Ascend router debug output
files from Hp-Ux's nettl
Toshiba's ISDN routers dump output
the output from i4btrace from the ISDN4BSD project
traces from the Eyesdn USB S0.
the output in Iplog format from the Cisco Secure Intrusion Detection System
pppd logs (pppdump format)
the output from VMS's Tcpiptrace/Tcptrace/UCX$TRACE utilities
the text output from the DBS Etherwatch VMS utility
visual Networks' Visual Uptime traffic capture
the output from Cosine L2 debug
the output from Accellent's 5Views LAN agents
endace Measurement Systems' ERF format captures
linux Bluez Bluetooth stack hcidump -w traces
catapult DCT2000 .out files
Головне вікно програми (рис. 2)

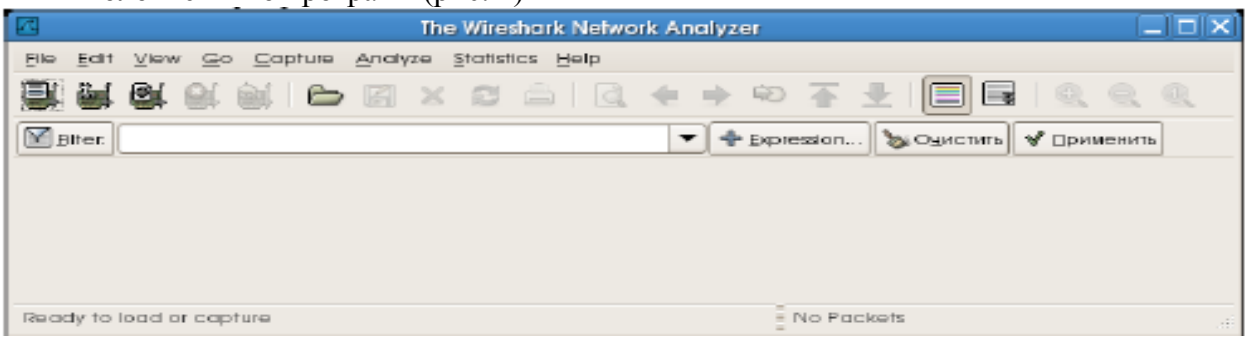


Рис. 2 Головне вікно програми

Захват пакетів

Усі опції захвата доступні через меню Capture

1. Вибір інтерфейсу (Capture/Interfaces) (рис. 3)

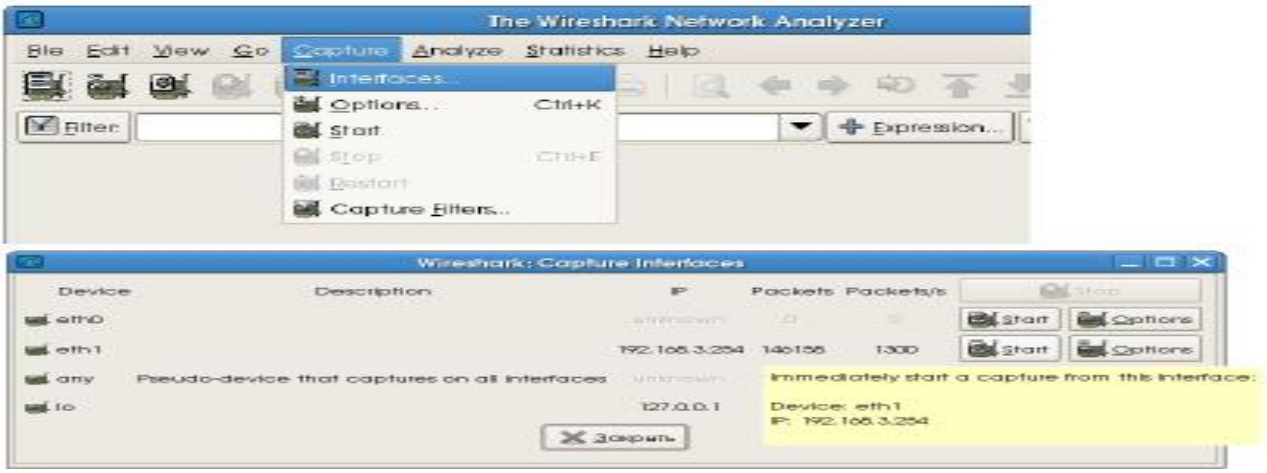


Рис. 3. Вибір інтерфейсу

2. Вікно процесу (рис. 4)

Рис. 4. Вікно процесу

3. Зупинка захоплення і отримання результатів (рис. 5).

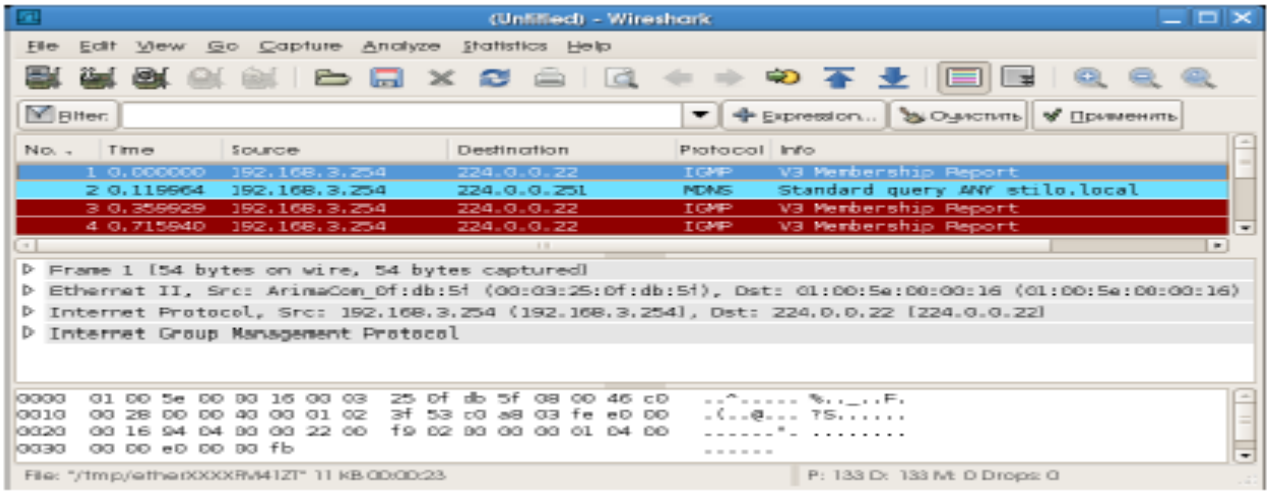


Рис. 5. Отримання результатів

Статистика

Типові звіти про використання мережі доступні через меню Statistics. Нижче наведені приклади відображення різних звітів.

1. Вибір звіту (Statistics) (рис. 6).

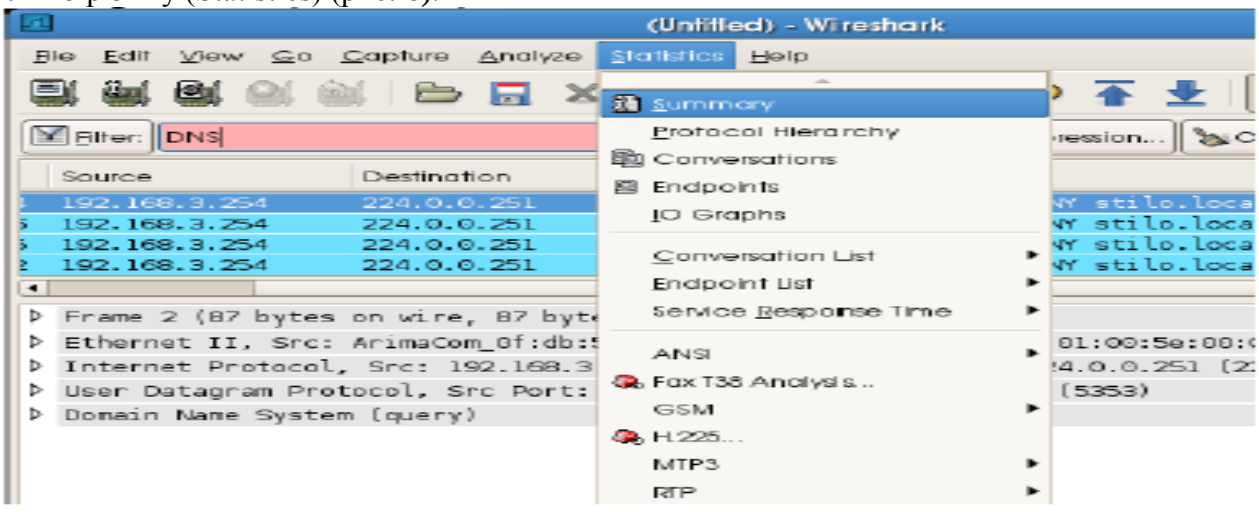


Рис. 6. Вибір звіту

2. Загальна статистика (рис. 7).

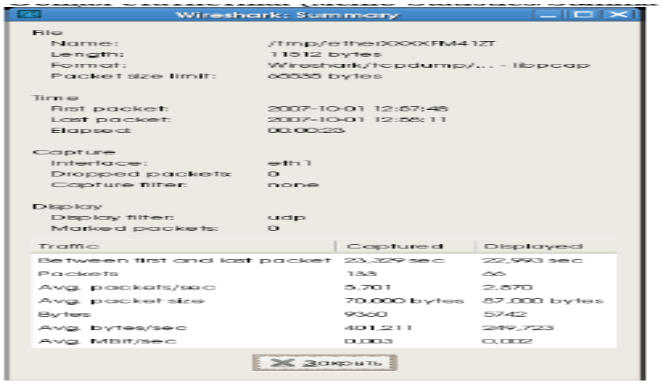


Рис. 7. Загальна статистика

3. Статистика за протоколами (меню Statistics/Protocol Hierarchy) (рис. 8).

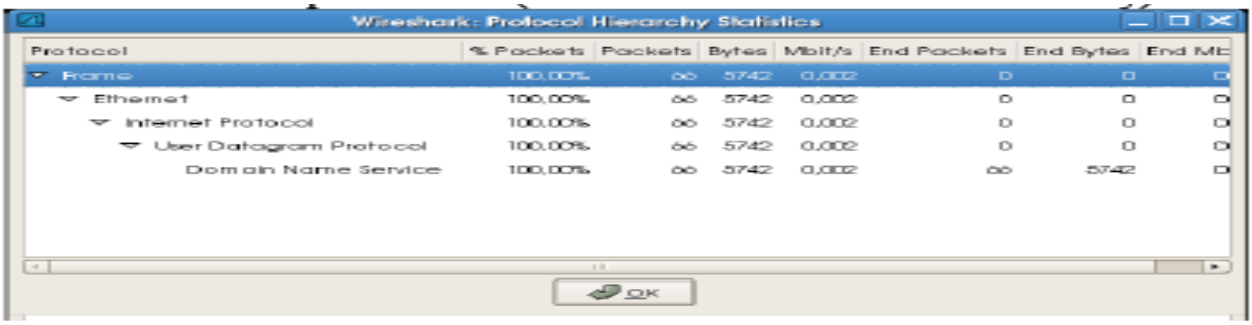


Рис. 8. Статистика за протоколами

4. Статистика за інтерфейсами (меню Statistics/Endpoints/Ethernet) (рис. 9).

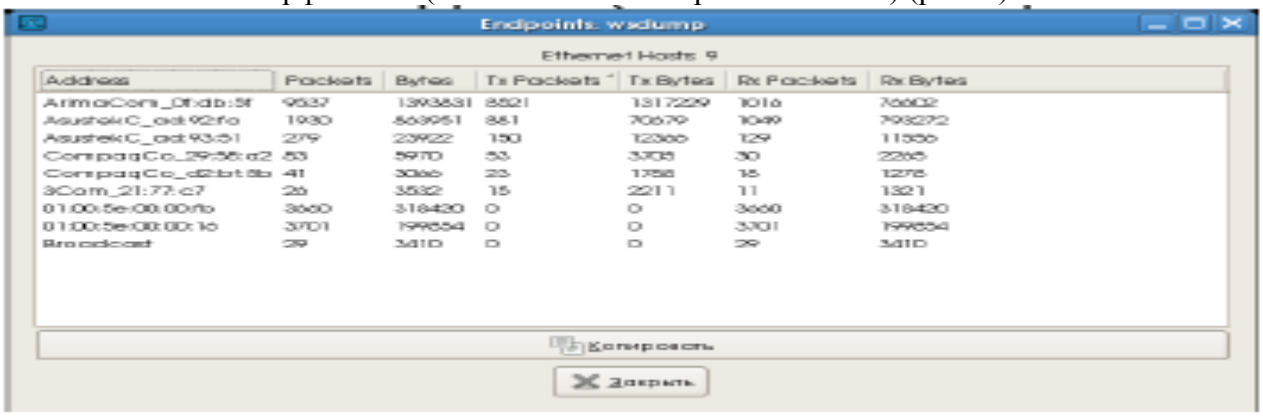


Рис. 9. Статистика за інтерфейсами

2. Хід роботи

Для виконання цієї роботи рекомендується використовувати програми Ethereal Network Analyzer або Wireshark (версії для UNIX/Linux, Windows-Версія працює не стабільно).

Ці програми практично ідентичні як за можливостями, так і за використанням.

Вказівки до роботи

Установіть (якщо не встановлена раніше) програму аналізу трафіка Ethereal Network Analyzer for Windows (Winena) + бібліотека Winpcap для Winena

Ethereal Network Analyzer(.rpm) Запустіть програму (потрібні права адміністратора) і ознайомтеся з користувацьким інтерфейсом і основними пунктами меню.

Завдання до роботи

1. Запустити ENA у режимі захвату трафіка, що проходить через інтерфейс, підключений до локальної мережі (звичайно це eth0). Перейти до наступного завданню.

2. Емулювати мережну активність у плині 10-15 хвилин. Для цього можна виконати, наприклад, деякі із зазначених дій (на вибір):

- Відкрити сайт http://rtos.asoiu;
- Підключитися до сервера ftp://telecom.asoiu;
- Виконати пінг будь-яких вузлів;
- Підключитися до одному з доступних мережевих дисків Windows (якщо такі ресурси представлені в мережі)
- Відкрити сайт http://telecom.asoiu;
- Виконати інші дії, що вимагають мережевого підключення.

3. Зупинити захват.

4. Заповнити таблицю 1. Вихідні дані для таблиці представлені у звіті Statistics/Summary. При заповненні таблиці зверніть увагу на дотримання розмірності величин (кб, Мб, Мбіт).

Таблиця 1

Параметр	**Значення**
Час захоплення, хв	
Кількість захоплених пакетів	
Обсяг, Мб	
Средній розмір пакета, Кб	
Середня швидкість, пакетів/сек	
Середня швидкість, Мбіт/сек	

5. Скласти таблицю розподілу трафіка по протоколах (табл. 2). Вихідні дані для таблиці можна одержати зі звіту Statistics/Protoc ol Hierarchy.

Таблиця 2

Протокол	**Трафік, Мбт**	**Трафік, %**
HTTP		
FTP		
Всього		100%

6. Скласти таблицю розподілу Ethernet-Трафіка за вузлами мережі (табл. 3). Вихідні дані для заповнення таблиці одержати з звіту Statistics/Endpoint list/Ethernet.

MAC - адреса	IP - адреса	Трафік					
		вхідний		вихідний		загальний	
		Мб	%	Мб	%	Мб	%
Всього			100		100		100

7. За даними табл. 1 визначити *відносне завантаження* мережі (в %) за контрольний період часу за формулою:

$$\text{Завнтаження} = \frac{(Трафік, Мбіт / Час, сек) * 100}{(Пропускназдатність, Мбіт / сек)}$$

8. За даними табл. 2 зробити виводи про якісний склад трафіка, тобто про співвідношення прикладних і службових протоколів.

9. За даними табл. 3 визначити, які з вузлів є найбільш завантаженими з урахуванням напрямку трафіка (вихідний, вхідний, загальний).

3. Контрольні питання

1. Що розуміють під поняттям моніторинг мережі?
2. Призначення програми WIRESHARK NETWORK ANALYZER.
3. Режими роботи програми WIRESHARK NETWORK ANALYZER.
4. Як вибрати режим статистики?
5. Як вибрати режим захоплення трафіку?

ЛАБОРАТОРНА РОБОТА 28. СКАНУВАННЯ МЕРЕЖ

Мета роботи: отримати практичні навички сканування мережі

Зміст

1. Теорія
1.1. Опис програми
1.2. Початок роботи із програмою
1.3. Створення списку хостів мережі
1.4. Робота зі списком хостів
1.5. Завершення роботи віддаленого комп'ютера
1.6. Включення комп'ютерів за мережею
1.7. Інформація про систему
1.8. Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP
1.9. Робота з папками
1.10. Пінг
1.11. Трасування маршруту
1.12. Мережевий трафік
2. Хід роботи
3.Контрольні питання

1. Теорія

1.1. Опис програми

Програма «10-страйк: Сканування Мережі» (Network Skanner) – зручна безкоштовна програма, яка допоможе вам одержати деяку інформацію про будь-яку локальну мережу. Вона просканує мережу, знайде всі доступні мережеві пристрої й одержить від них максимально доступний обсяг інформації. Програма може бути використана без попередньої установки на комп'ютер, тобто ви з легкістю можете записати її з флешки в будь-якій версії Windows, починаючи з Win2k. Крім одержання інформації програма дозволить виконувати вам деякі дії для керування комп'ютерами в мережі: пінгувати, трасувати маршрут, перезапускати, виключати й включати їх, управляти службами й реєстром на віддалених комп'ютерах. Крім усього, "Сканування Мережі" уміє взаємодіяти з мережевими пристроями за протоколом SNMP і одержувати будь-яку інформацію через нього. Програма є відмінним засобом для починаючого системного адміністратора або просто допитливого користувача.

1.1.1 Основне призначення програми:

Програма сканує локальну мережу, автоматично одержує перелік доступних хостів, формує список хостів, дозволяє виконувати наступні операції з ними:

Одержувати інформацію: IP-, Mac-Адреси, Dns-Ім'я, виробник адаптера, поточний користувач, домен, сервер, тип ОС, дата й час, час роботи, список локальних дисків, загальні ресурси, список активних підключень, облікові записи, групи, параметри реєстру, служби й пристрої, відкриті Tcp-Порти, запущені процеси, журнали подій, установлені програми, Snmp-Інформація.

- Пінгувати за протоколом ICMP
- Трасувати маршрут до віддаленого хосту
- Включати й виключати комп'ютери за мережею
- Відкривати в Провіднику (як у Мережевім оточенні)
- Порт на комутаторі
- Переглядати статистику використання локального вхідного й вихідного трафіка
- Управляти локальними папками загального доступу
- Управляти службами на віддаленому комп'ютері: зупиняти, запускати, відключати і т.д.
- Змінювати, додавати й видаляти параметри в реєстрі віддаленого комп'ютера.

1.1.2 Можливості програми:

- Швидке, багатопотокове сканування локальної мережі за заданими діапазонами Ip-Адрес;
- Одночасне застосування декількох способів виявлення мережевих пристроїв: ICMP-Пінг, сканування списку Tcp-Портів, Arp-Пінг (перетворення IP- в Mac-Адресу);
- Інтелектуальний алгоритм розпізнавання типу мережевих пристроїв. Визначення мережевих і локальних принтерів, серверів, серверів БД, роутеров, комутаторів, хабов, Wifi-пристроїв і т.д.;
- Одержання додаткової інформації про пристрої через Netbios;
- Пошук пристроїв, що підтримують протокол SNMP (комутатори, принтери, відеокамери, роутери і т.д.);
- Пошук пристроїв, що підтримують протокол UpnP (медіаплеєри, роутери і т.д.);
- Збереження результатів сканування в Csv-Форматі (підтримується Microsoft Excel);
- Автоматичне формування списку хостів для подальшої роботи;
- Автоматичне збереження всіх змін списку, параметрів хостів і перевірок;

Програма повністю працездатна під ОС WINDOWS NT4/2000/XP/2003/Vista/2008/7/8.

У локальній мережі повинен бути дозволений протокол ICMP або сканування TCP-Портів. Для повного функціонування повинні бути дозволені протоколи SNMP, Netbios.

Для успішного виконання програми необхідно запускати її тільки із правами адміністратора.

При використанні методу сканування мережі TCP-Пінг слід ураховувати, що в ОС Windows XP і вище не допускається більш 10 одночасних Tcp-Підключень. Це може позначитися на продуктивності програми

1.2. Початок роботи із програмою

1. Запустіть програму. Якщо ви запустили програму перший раз, то побачите на екрані головне вікно програми **" 10-страйк: Сканирование Сети"** і вікно **Майстра сканування мережі (рис. 1).**

Дотримуючись вказівок **Майстра...** можна швидко й легко виявити хости в мережі і додати їх у список.

Майстер... пропонує 2 способу пошуку хостів у мережі:

Сканування діапазону Ip-Адрес.

Даний спосіб дозволяє виявити максимальну кількість пристроїв, має наступні переваги:

- висока швидкість сканування діапазону (при оптимальному (див. нижче) виборі параметрів сканування й налагодження мережі);
- дозволяє визначати різні види пристроїв: принтери (локальні й мережеві), комутатори, хаби, сервера, сервера баз даних, роутери, Wifi крапки доступу і т.д.;
- застосовує відразу кілька ефективних способів пошуку пристроїв у мережі (ICMP-Пінг, сканування списку Tcp-Портів, Arp-Запити);
- дозволяє одержувати інформацію із пристроїв за SNMP;
- автоматично одержує багато іншої інформації про знайдені хостах (IP, Mac-Адреси, виробника мережевого адаптера, Dns-Ім'я, тип ОС, підключені принтери, описи);
- дозволяє сканувати відразу кілька діапазонів Ip-Адрес;

Якщо у вас більша мережа, що комутирується, то рекомендується використовувати цей спосіб сканування.

Оптимальність вибору параметрів випливає з конфігурації вашої мережі, наявності й функціонування необхідних протоколів. Зокрема, у невеликий 100 Мбіт локальної мережі для виявлення хостів досить буде 2-х пакетів пінга, і 100-500 мс секунд відгуку. У випадку сканування Tcp-Портів треба зрозуміти, що чим більше ви вкажете портів у списку, тем довше буде відбуватися процедура пошуку**.** Оптимальним варіантом отут є завдання

2-3 загальнопоширених портів, за якими можна знайди Windows-Станції або сервера – це 139, 21 і 80й порти (Netbios, FTP, HTTP). Слід урахувати вбудоване обмеження (затримка) на одночасне сканування декількох Tcp-Портів в ОС Windows XP і вище.

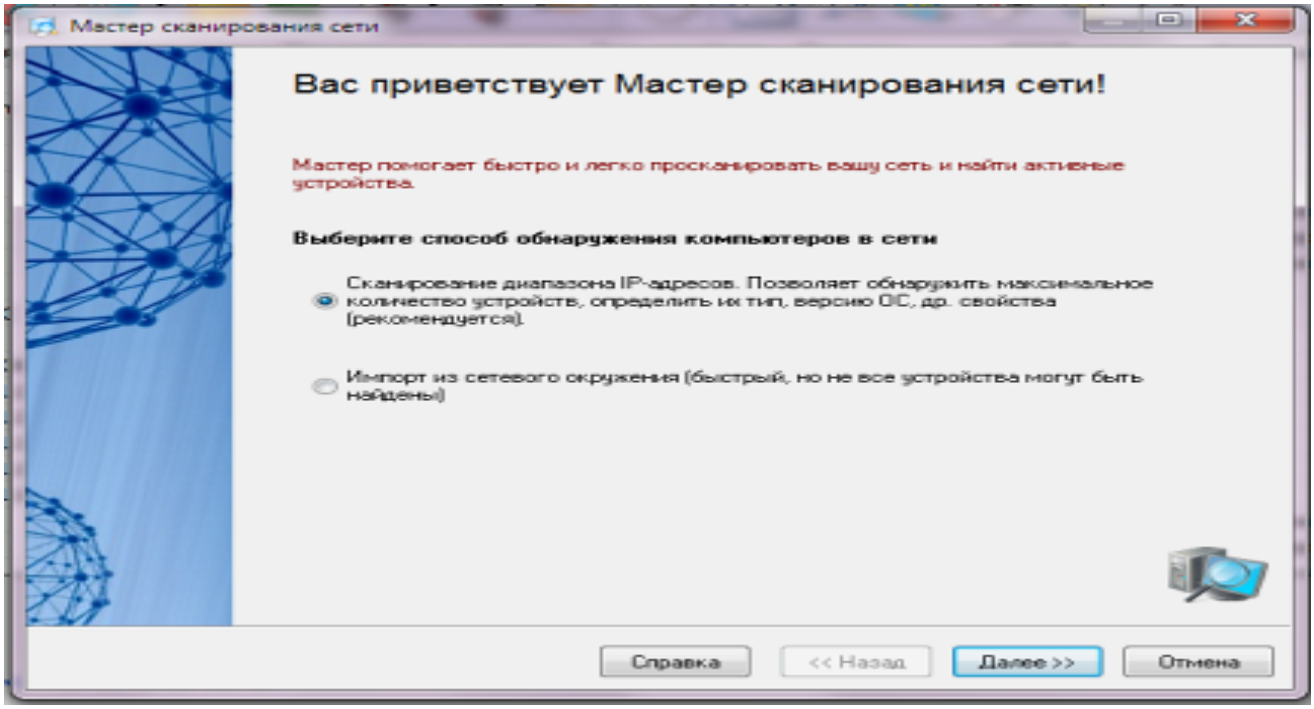


Рис. 1. Вікно майстра сканування мережі

У більшій мірі варто сказати про пошук мережевих принтерів. Дана процедура займає досить тривалий час, тому її не варто використовувати, якщо ви точно знаєте, що таких принтерів у вашій мережі немає. Інакше необхідно дочекатися закінчення цієї процедури, про що буде свідчити поява у вікні майстра індикатору ходу сканування мережі. Справа в тому, що пошук мережевих принтерів проводиться до запуску основної процедури сканування (яка виконується більшою кількістю паралельно працюючих потоків, на відміну від пошуку принтерів). Це відноситься й до можливості одержання додаткової інформації про хости через Netbios.

Якщо у вашій мережі заборонений протокол Netbios, то ніяка **додаткова інформація** не може бути отримана, і програма затратить досить багато часу на цю спробу (звідси відчуття, що програма "зависла").

Пошук пристроїв з SNMP здійснюється в багатопоточному режимі. Однак якщо ви вкажете досить велику кількість можливих community string, то це так само сповільнить процес сканування.

Виходячи із усього сказаного, випливає порада, що якщо ви вибрали параметри, і програма повільно сканує й взагалі "зависла" – слід відключити деякі параметри (у першу чергу пошук мережевих принтерів, потім одержання додаткової інформації через Netbios) і спробувати просканувати знову.

Імпорт із мережевого оточення.

Даний спосіб працює трохи швидше, але не всі мережеві пристрої можуть бути знайдені (тільки комп'ютери й деякі сервера).

Якщо **Майстер...** виявив не всі хости, ви можете добавити їх в список вручну.

2. Використовуйте контекстне, головне меню й панель інструментів для доступу до функцій програми. Усі функції програми доступні через контекстне меню, панель інструментів, головне меню, і будуть описані далі.

1.3. Створення списку хостів мережі

Створення списку хостів мережі здійснюється за допомогою Майстра сканування мережі. Список хостів створюється в кілька етапів:

1. Виклик Майстра сканування мережі.

Для цього потрібно вибрати пункт головного меню **Файл**, потім **Сканирование сети**.

2. Вибір способу сканування мережі.

Для пошуку мережевих пристроїв **Майстер** використовує 2 способи сканування мережі (рис.1):

- **Сканування діапазону Ip-Адрес** Даний спосіб дозволяє виявити максимальну кількість пристроїв, має наступні переваги:
  - багатопоточність, що забезпечує високу швидкість сканування діапазону;
  - дозволяє визначати різні види пристроїв: принтери (локальні й мережеві), комутатори, хаби, сервера, сервера баз даних, роутери, Wifi крапки доступу і т.д.;
  - застосовує відразу кілька ефективних способів пошуку пристроїв у мережі (ICMP-Пінг, сканування списку TCP-Портів, Arp-Запити);
  - дозволяє одержувати інформацію із пристроїв за SNMP (комутатори, принтери, Wifi і т.д.);
  - дозволяє сканувати відразу кілька діапазонів Ip-Адрес;

Якщо у вас велика мережа, що комутується, то рекомендується використовувати цей спосіб сканування.

- **Імпорт із мережевого оточення** Даний спосіб працює трохи швидше, але не всі пристрої можуть бути знайдені.

При імпорті з мережевого оточення необхідно на наступних кроках Майстра просто слідувати його підказкам. Процес сканування діапазону адрес потребує детального опису.

3. Крок 1. Завдання діапазону Ip-Адрес (рис. 2).

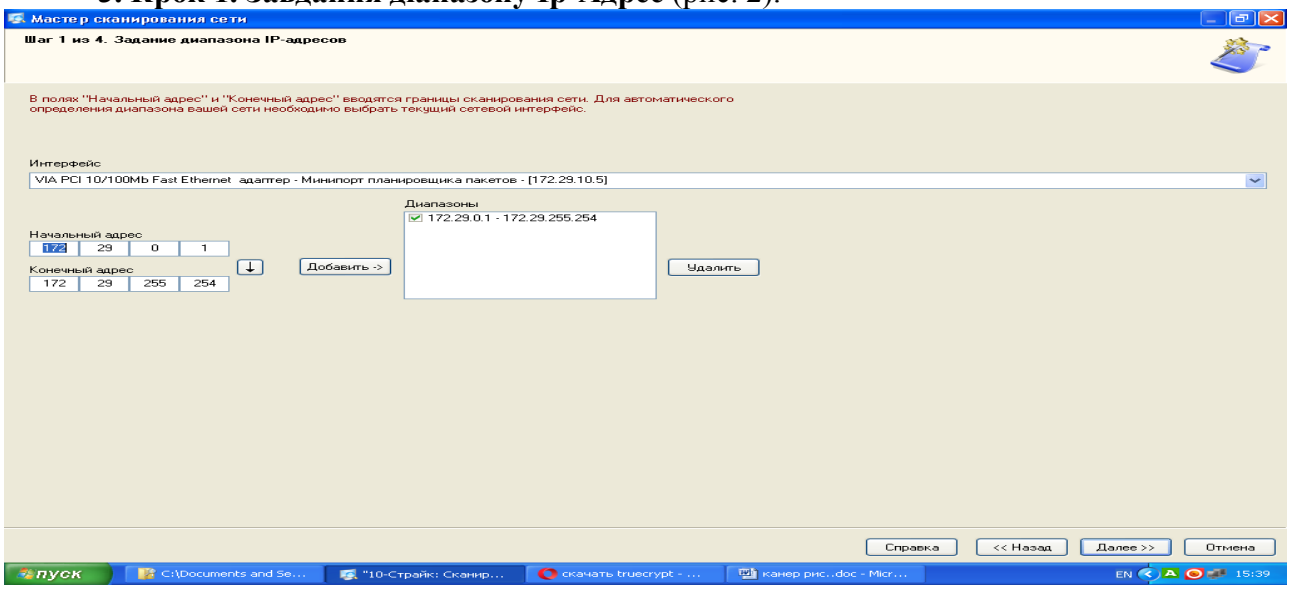


Рис. 2. Вікно задання діапазону **Ip-Адрес**

На першому кроці задаються діапазони сканування. Процедура виконується в кілька етапів:

1. У полях **Початкова адреса** й **Кінцева адреса** вводяться границі сканування мережі. Для автоматичного визначення діапазону можливих адрес вашої мережі необхідно вибрати поточний мережевий **Інтерфейс**.

2. Після заповнення полів адреси необхідно нажати кнопку **Добавить**, після чого обраний діапазон занесеться в список скануємих діапазонів. Вилучити діапазон зі списку можна натисканням відповідної кнопки **Удалить**, щоб діапазони в списку були просканові, необхідно виділити їх галочкою.

3. Нажати кнопку **Далее.**

4. Крок 2. Завдання способу й параметрів сканування (рис. 3).

Майстер надає для вибору три способи пошуку пристроїв у мережі:

- **ICMP-Пінг**;

Параметр **Кількість пакетів** відповідає за число ICMP-Пакетів, що відправляються програмою за кожною скануємою адресою. У мережах з високим трафіком одного пакета може бути недостатньо для одержання відгуку від існуючого хосту. У цьому випадку рекомендується задавати не менш 3-4 пакетів.

- **сканування списку TCP-Портів;**

Для сканування TCP-Портів необхідно задати **список портів**, за якими пристрої можуть бути знайдені в мережі. Найпоширенішими відкритими портами в мережах Microsoft є 139 (Netbios), 21 (FTP), 80 (HTTP).

ВАЖЛИВО! При виборі методу сканування портів необхідно враховувати, що ваші дії в більшості випадків можуть розцінюватися брандмауерами як атака й спричинити відповідні наслідки.

Крім цього, ОС Windows XP і вище не дозволяють одночасного сканування групи Tcp-Портів і на рівні драйверів штучно гальмують процес .

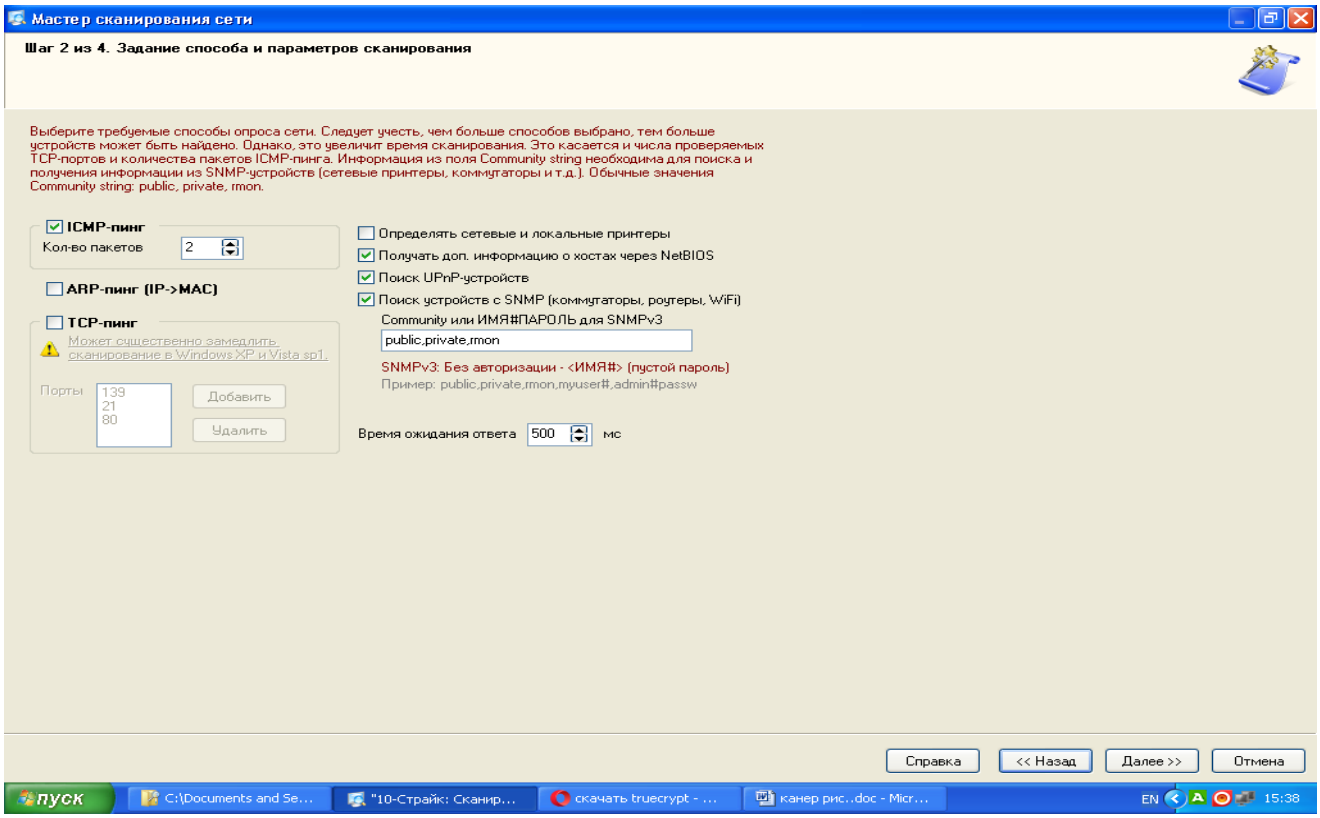


Рис. 3. Завдання способу й параметрів сканування

- **ARP-Пінг (IP->MAC) .**

ARP-Запити полягають у спробі визначення Mac-Адреси хосту за його Ip-Адресою. Якщо Mac-Адреса може бути отримана, Майстер поміщає даний хост у список результатів пошуку. Існує ймовірність, що програма може знайти неіснуючі хости. Справа в тому, що на комутаторі, в адресній таблиці можуть залишатися застарілі або зарезервовані записи. У цьому випадку, слід просто зняти з них галочки у вікні результатів.

Для всіх способів сканування необхідно задати **Час очікування відповіді** – час, у плині якого Майстер буде чекати відповідь від хосту, що сканується.

Якщо у вашій мережі є сервери друку або **мережеві принтери**, можна задати їхній пошук. Функція також може знайти локально-підключені до комп'ютерів принтери.

Майстер може автоматично знайти всі сервера, сервера БД у мережі, одержати іншу корисну інформацію про знайдені комп'ютери (тип ОС, коментар і т.д.). Для цього необхідно вибрати опцію **Одержувати дод. інформацію через Netbios**. Функція буде працювати тільки в тому випадку, якщо протокол Netbios дозволений політикою безпеки на вашім комп'ютері й комп'ютерах вашої мережі.

Якщо у вашій мережі є пристрої, на яких активний SNMP-Агент, то Майстер проінформує вас про це, відобразить опис цих пристроїв. Наявність активного SNMP-Агента допомагає Майстрові визначати більш широкий спектр типів пристроїв. Так, наприклад, за отриманою **SNMP** інформацією Майстер може ідентифікувати комутатори (switch), хаби, роутери, принтери, Wifi крапки доступу, радіороутери і т.д. При пошуку пристроїв з активним SNMP-Агентом, Майстер намагається підключитися до чергової адреси, використовуючи задані імена співтовариств (**Community**). Ці імена можуть бути перераховані через кому в поле **Community strings**. Найпоширенішими іменами, що задаються за ***замовчуванням, співтовариств, є public***, private, rmon. Якщо ви впевнені, що на ваших пристроях задані інші імена, необхідно вказати їх у списку.

Після завдання всіх параметрів, Майстер переходить безпосередньо до сканування мережі. Для перехід до кроку сканування мережі потрібно нажати кнопку **Далі >>.**

5. Крок 3. Пошук і відбір комп'ютерів для приміщення в список.

Процес сканування стартує негайно. Спочатку здійснюється спроба виявлення мережевих і локальних принтерів. Ця процедура може забирати тривалий час, протягом якого програма може не відповідати на запити й буде недоступної кнопка **Остановить.** Після цього проводиться пошук пристроїв за Netbios, що також може зайняти якийсь час. Після виконання двох підготовчих процедур, програма починає безпосередній перебір усіх Ip-Адрес заданих діапазонів. Про хід процесу сигналізує індикатор прогресу й напис у нижньому лівому куті Майстра – **"Сканування діапазону адрес...".**

Хід процесу сканування можна зупинити, нажавши кнопку **Остановить.**

Знайдені в процесі сканування хости поміщаються в список результатів. Існує можливість зміни типу знайденого пристрою прямо з вікна результатів. Для цього необхідно виділити необхідний запис (допускається множинний вибір) і викликати контекстне меню. У цьому меню необхідно вибрати встановлюваний тип пристрою.

Для того, що б помістити в список хостів не всі знайдені пристрої, пропонується відзначити бажані пристрої галочками. Кнопки **Відзначити всі**, **Виділені**, **Інвертувати** допомагають проводити множинний вибір пристроїв. Можна оперативно вивантажити всю отриману інформацію в CSV-**Файл**. При цьому, у звіт будуть поміщені й параметри сканування мережі. Для вивантаження інформації необхідно нажати кнопку **Отчет.**

Даний звіт може допомогти розроблювачам програми, якщо ви зіштовхнетеся із проблемами формування списку хостів мережі.

Після завершення процесу сканування потрібно перейти на завершальний крок, нажавши кнопку **Далее.**

6. Крок 4. Розміщення хостів у списку (рис. 4).

Перед поміщенням знайдених хостів у список можна задати додаткові параметри:

- Можна вказати, що **використовувати в якості імені (адреси) хоста** - Ip-Адресу пристрою або його DNS-Ім'я. Для мереж, з динамічним розподілом Ip-Адрес необхідно вибрати DNS -Ім'я, тому що цей атрибут у цьому випадку буде постійним. У мережах зі статичними Ip-Адресами можна вказати в якості імені Ip-Адреса пристрою.
- **Відкидати DNS Суфікс в імені хоста**. У якості імені хосту Майстер може використовувати певні Dns-Імена пристроїв. Часто, такі імена мають суфікс, наприклад: *mary.dep1.orgname.com*. При виборі даного параметра ім'я хосту буде *mary*.

Для додавання тільки нових хостів, яких ще немає в списку, включіть відповідний параметр.

Після натискання кнопки **Готово** знайдені хости поміщаються в список (рис. 5).

1.4. Робота зі списком хостів

Додавання хоста

Для додавання нового хосту в список необхідно виконати наступні дії:

1. Вибрати пункт головного меню **Хости | Додати хост**;

2. У вікні, що з'явилося, увести необхідні параметри. Обов'язковим параметром є **Ім'я або адреса хоста**;

Опис параметрів хосту:

Ім'я або адреса хоста Ім'я комп'ютера в мережі або його Ip-Адреса. Значення даного поля є вхідним параметром для функцій програми.

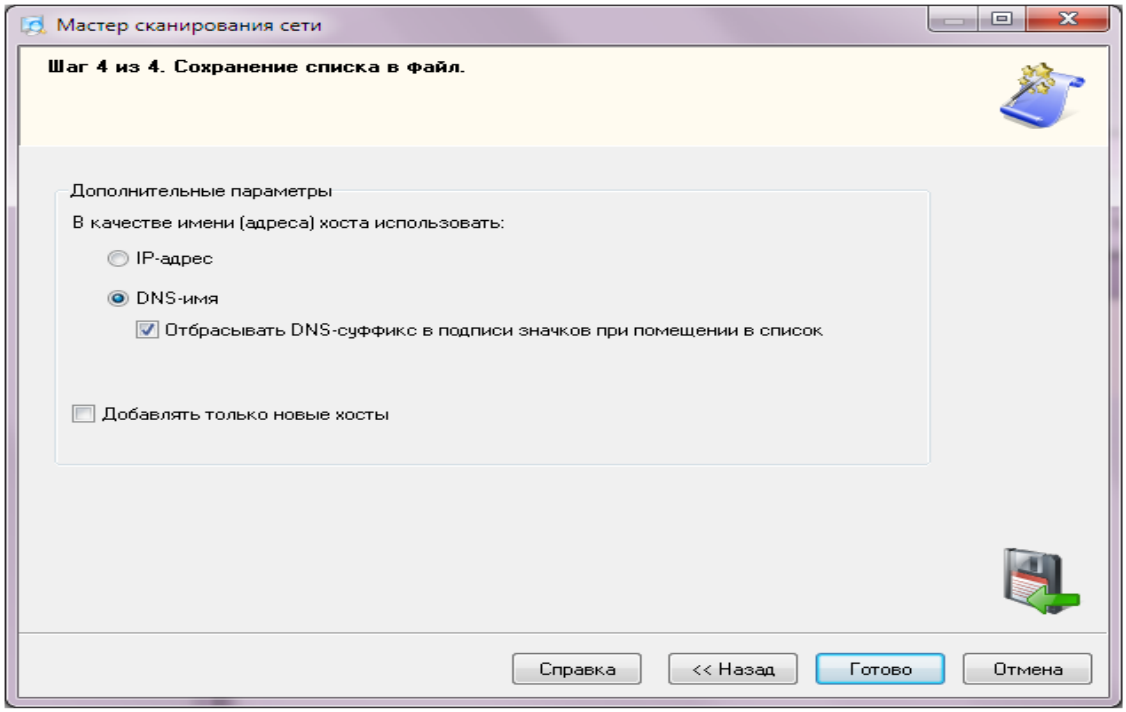


Рис. 4. Вікно налагодження програми

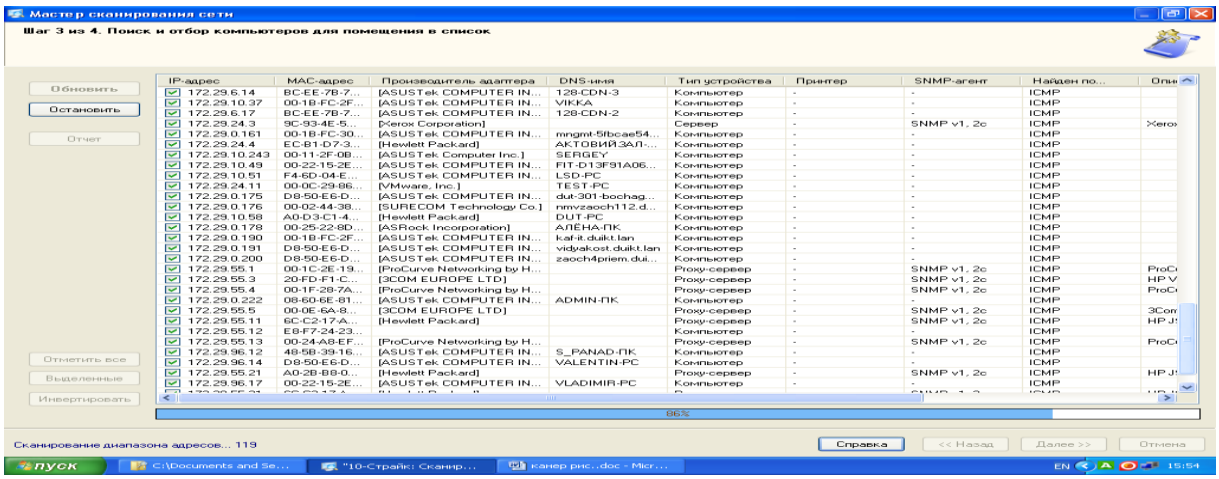


Рис. 5. Розміщення хостів у списку

Назва в списку За замовчуванням, у якості назви хосту в списку виступає його адреса або мережеве ім'я. Його можна змінити, задавши будь-яке бажане ім'я в цьому полі.

Тип Тип пристрою служить для візуального поділу хостів у списку. Кожний тип супроводжується умовним значком-піктограмою.

Мас-Адреса Для успішної роботи функції включення комп'ютера за мережею (Wake on LAN) необхідно для кожного хосту один раз задати Мас-Адресу мережевого адаптера (рис. 6). Мас-Адреса можна одержати автоматично у включених хостів або ввести її вручну.

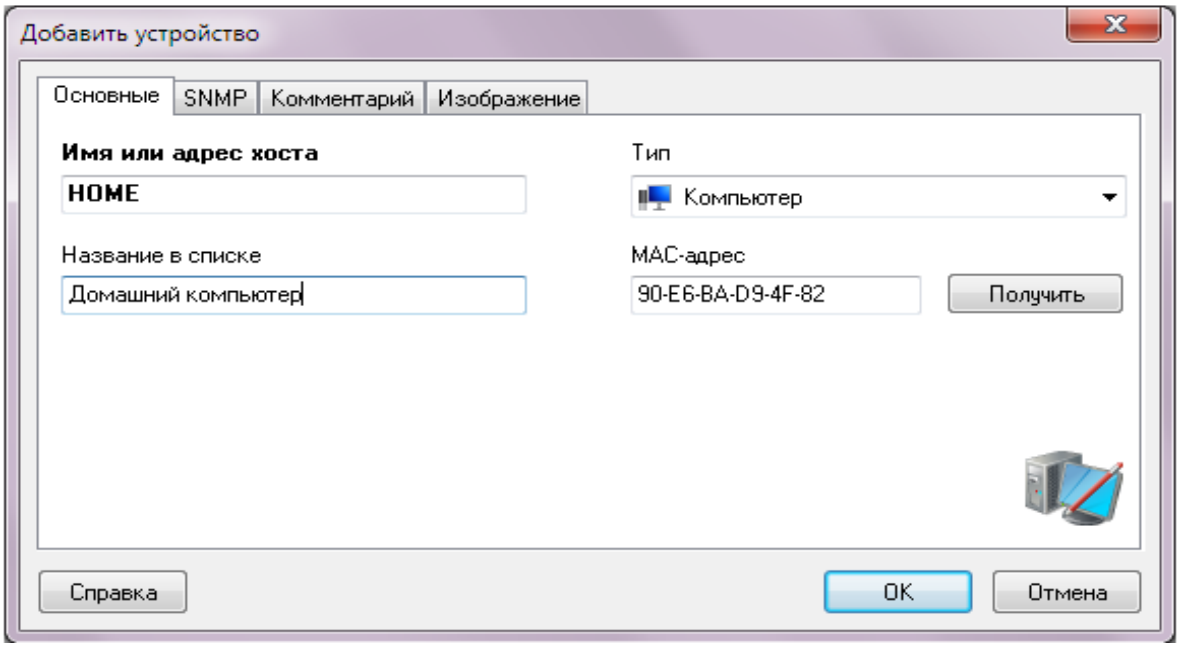


Рис. 6. Введення **Мас-Адреси**

SNMP **Для одержання SNMP-Інформації про хост необхідно знати його** Community**. Можна задати цей параметр, включивши галочку** Агент є (рис. 7)**. Уведене значення буде автоматично підставлятися там, де це необхідно.**

Коментар: Кожний хост можна супроводити користувацьким коментарем. У цьому полі можна зберігати інформацію про користувача комп'ютера, складові його системи, список ПЗ і т.д. Для зручності й швидкості введення коментаря передбачений механізм вибору атрибутів зі списку. Список атрибутів може бути доповнений (рис. 8).

Зображення **Кожному хосту можна прив'язати яке-небудь зображення, яке допоможе простіше й швидше ідентифікувати його (фото користувача, приміщення і т.д.). Включіть галочку** Файл зображення **(рис. 9) й виберіть його файл.**

Після завдання параметрів потрібно нажати кнопку **ОК.** Новий хост поміститься в список. Збереження нової інформації у файл відбувається автоматично.

Зміна параметрів хоста

Для зміни параметрів хосту необхідно виконати наступні дії:

1. Виділити в списку хост;

2. Викликати контекстне меню, вибрати пункт **Изменить хост**;

3. Змінити необхідні параметри у вікні, що з'явилося. Нажати кнопку **ОК** для збереження змін.

Зміни зберігаються у файлі й набувають чинності негайно.

1.5 Видалення хосту

Для видалення хосту необхідно виконати наступні дії:

1. Виділити в списку хост;

2. Викликати контекстне меню, вибрати пункт **Удалить хост**. Підтвердити дію, нажавши кнопку **ОК** у запиті, що з'явився;

Обраний хост віддаляється зі списку й файлу.

1.4 Завершення роботи віддаленого комп'ютера

При відповідних правах у мережі ви можете завершити роботу віддаленого комп'ютера.

При цьому можливі наступні варіанти:

- Виключити комп'ютер, при цьому програми з незбереженими даними запросять підтвердження на вихід без збереження;
- Виключити комп'ютер, ігноруючи незбережені дані;
- Перезавантажити комп'ютер;

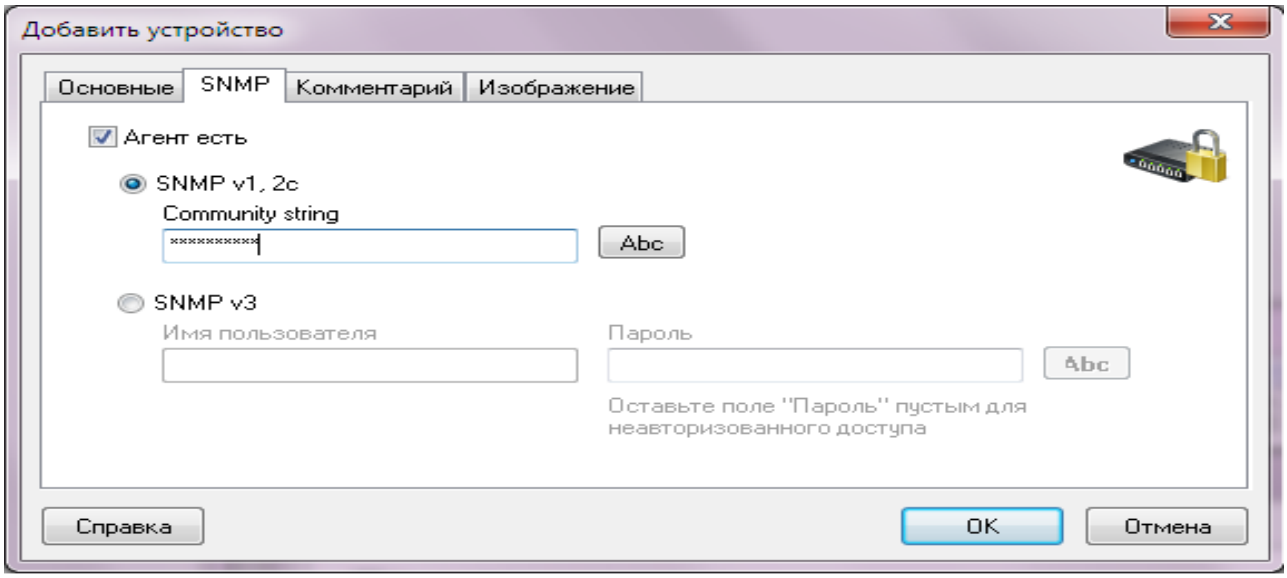


Рис. 7. Вікно **SNMP**

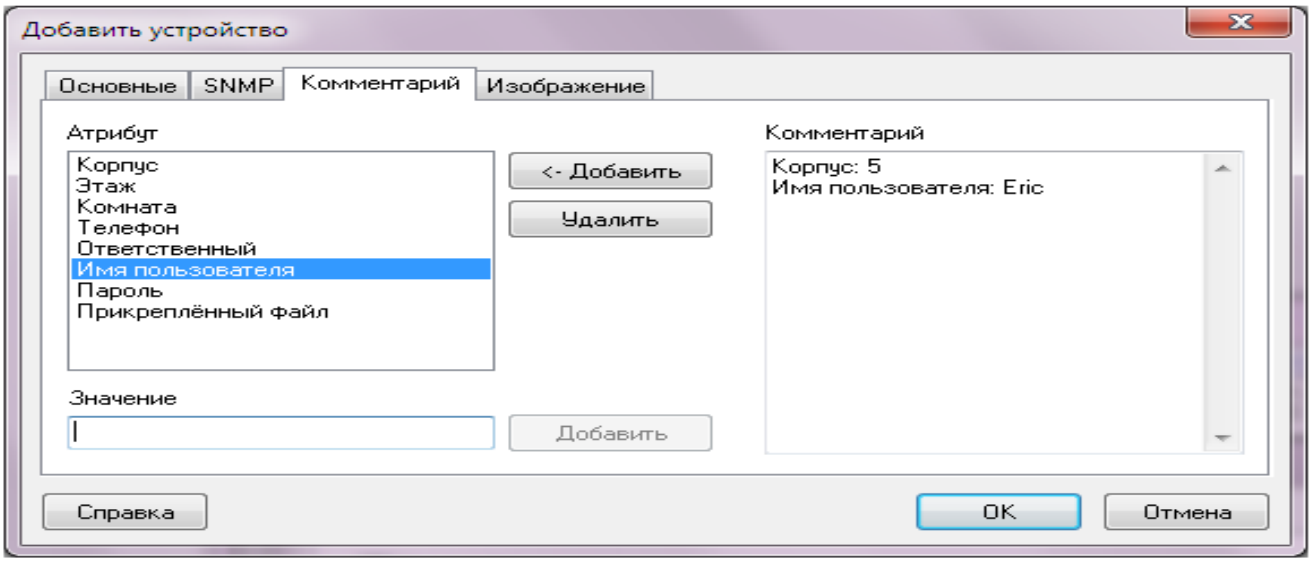


Рис. 8. Вікно коментарів

Рис. 9. Вікно відбору зображення

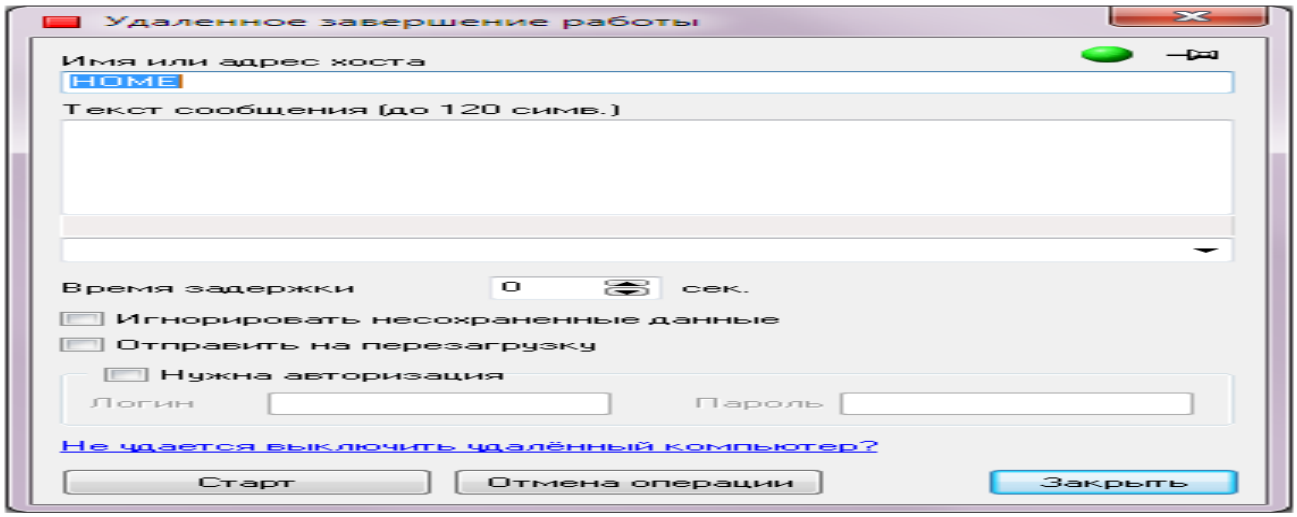


Рис. 10. Вікно управління віддаленим ПК

- Скасувати операцію завершення роботи, якщо час затримки перевищує 0 секунд. Після закінчення заданого часу скасування операції буде неможливе.

Можна завершити роботу відразу декількох комп'ютерів. Для цього необхідно перелічити в полі **Ім'я комп'ютера** імена комп'ютерів, що вимикаються, розділяючи їх символом ";". Після натискання кнопки **Старт** в, список будуть додаватися найменування й результати виконуваних операцій.

Якщо користувач, під яким працює програма, не має прав адміністратора на комп'ютері, що вимикається, то для успішного виконання вимикання або перезавантаження необхідно задати ім'я й пароль користувача з необхідними повноваженнями. Для завдання імені й пароля необхідно включити параметр **Потрібна авторизація** й заповнити поля **Логін** і **Пароль**.

Перед завершенням роботи на екран віддаленого комп'ютера буде виведене повідомлення, яка інформує про завершення роботи й залишок часу перед цим (рис. 11). Також, у це повідомлення можна додати будь-який текст (поле **Текст повідомлення**). У рядку стану буде відображатися повідомлення про залишок часу до виконання операції.

Якщо мережеві адаптери й BIOS'и ваших машин підтримують функцію **Wakeuponlan**, то ви можете за певних умов включати комп'ютери за мережею.

Для успішного виконання цієї функції повинні бути дотримано кілька умов:

- Мережевий адаптер повинен бути PCI2.2-compatible, або більш старий, але з кабелем, за яким з материнської плати подається живляча напруга в 5В;
- Режим Wakeonlan повинен підтримуватися й бути включений в Biose (Wakeon - Netcard);
- Комп'ютер попередньо повинен бути "правильно" виключений – це називається "Soft-Off", лампочки на клавіатурі й мережевій карті повинні горіти.

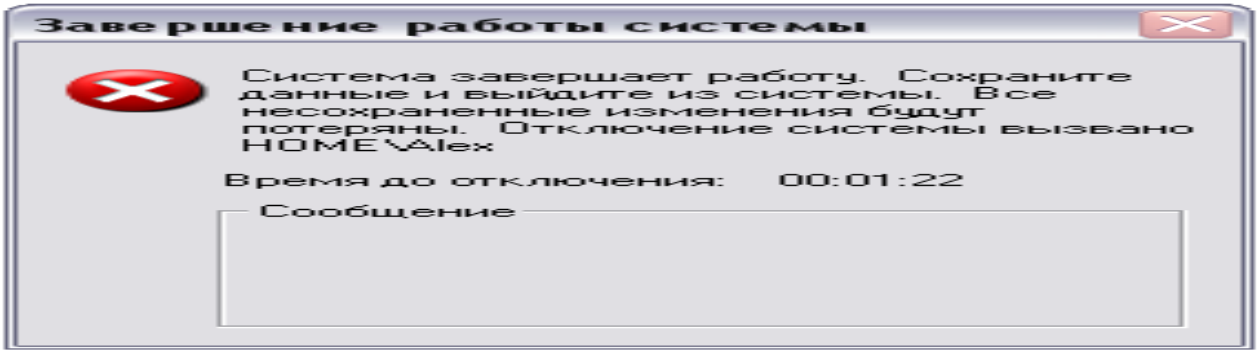


Рис. 11. Вікно попередження

1.5. Включення комп'ютерів за мережею

Для включення за мережею одного або декількох комп'ютерів необхідно виділити їх у списку й вибрати пункт контекстного меню **Включить/Выключить/Включить.** У вікні нажати кнопку **Старт**. Після цього всім комп'ютерам, у яких визначилася Mac-Адреса, буде відправлений сигнал на включення. Для відправлення цього сигналу необхідно, щоб ваш firewall пропускав вихідні UDP-Пакети.

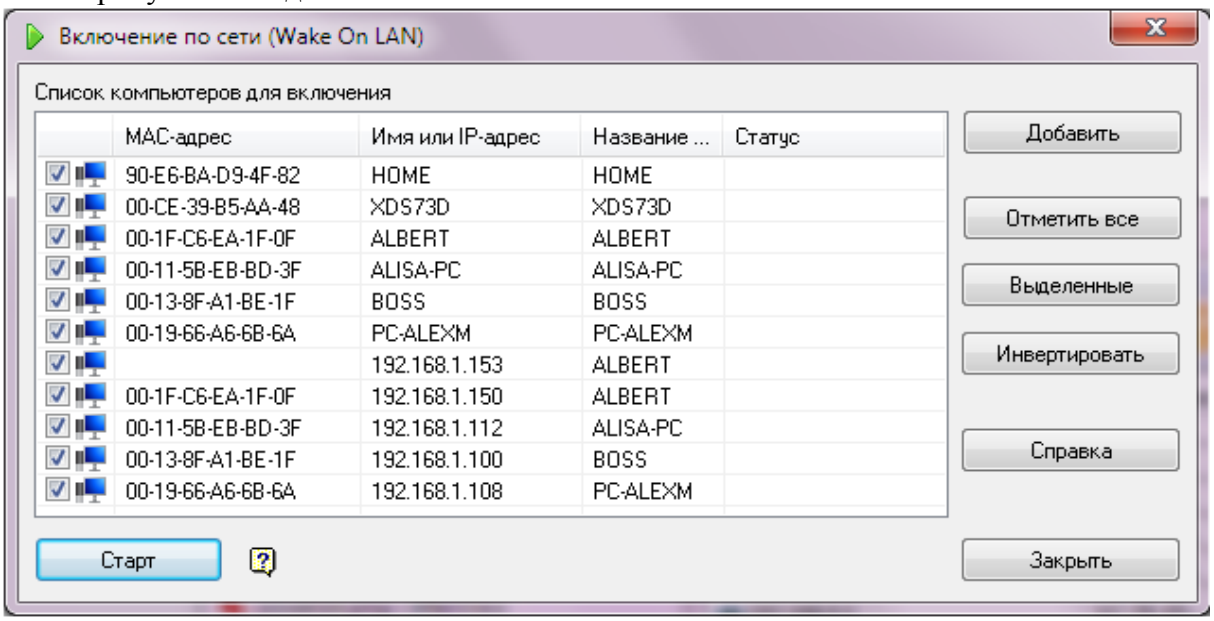


Рис. 12. Вікно включення ПК

Тому що для доставки пакета-сигналу на включення використовується протокол UDP, немає гарантії, що комп'ютер обов'язково одержить цей сигнал і ввімкнеться. Якщо таке відбулося, необхідно повторити процедуру включення ще раз.

1.6 Інформація про систему

У вікні **Інформація про систему** зібрані відомості про віддалену машину. Якщо користувач, під яким працює програма, не має прав адміністратора на віддаленому комп'ютері, то для успішного одержання інформації про журнал подій, списку процесів, установлених програм, керування службами й реєстром, необхідно задати ім'я й пароль користувача з необхідними повноваженнями. Для встановлення з'єднання з віддаленим комп'ютером від імені адміністратора необхідно нажати кнопку на панелі інструментів (рис. 13) із зеленою піктограмою або викликати пункт головного меню **Сервис / Подключиться с логином и паролем...**, у діалоговім вікні, що з'явилося, увести ім'я й пароль, нажати кнопку **ОК**. У випадку успішного підключення програма видасть відповідне повідомлення, або повідомлення про помилку. Після встановлення з'єднання всі запити за одержанням або зміні інформації на віддаленому комп'ютері будуть іти від цього користувача. За завершенням роботи з інформацією віддаленого комп'ютера необхідно розірвати з'єднання (з метою безпеки, тому що їм можуть скористатися інші програми), нажавши кнопку із червоною піктограмою, або викликавши пункт головного меню **Сервис /Разорвать соединение.**

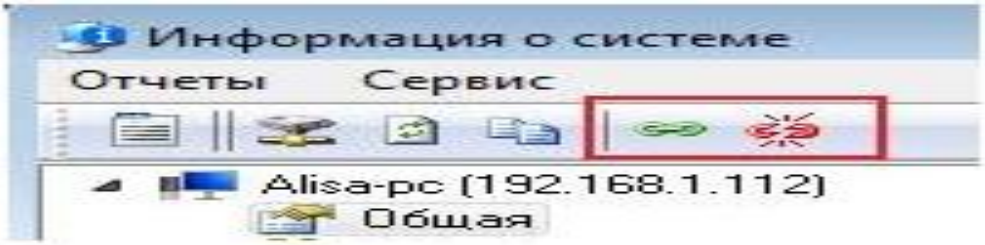


Рис. 13. Панель інструментів

Ви можете скопіювати отриману в розділах інформацію в буфер, а потім вставити в будь-який текстовий файл або аркуш Microsoft Excel. Для цього викличте контекстне меню списку властивостей і виберіть пункт **Копировать в буфер**.

1.7. Загальна інформація

У цьому розділі відображається узагальнена інформація про віддалений комп'ютер: Ip-Адреси, Dns-Ім'я, Mac-Адреси адаптерів, їх виробники користувач, домен/робоча група, сервер, тип операційної системи установки, , дата й час, час роботи без перезавантаження, список дисків (рис.14).

Одержання деяких властивостей віддаленого комп'ютера займає якийсь час, тому можлива затримка (тривалість – від 0 до 20 сек., залежно від розташування комп'ютера в мережі і її швидкодії).

Частина властивостей може виявитися недоступною з ряду причин, пов'язаних з організацією мережі й правами користувача.

Якщо в системі встановлено кілька мережевих адаптерів (фізичних або віртуальних), то будуть знайдені всі їх IP і Mac-Адреси.

Для одержання додаткової інформації про домен натисніть ярлик біля імені домену.

Для одержання списку дисків віддаленого комп'ютера потрібні права адміністратора домену (роб.групи).

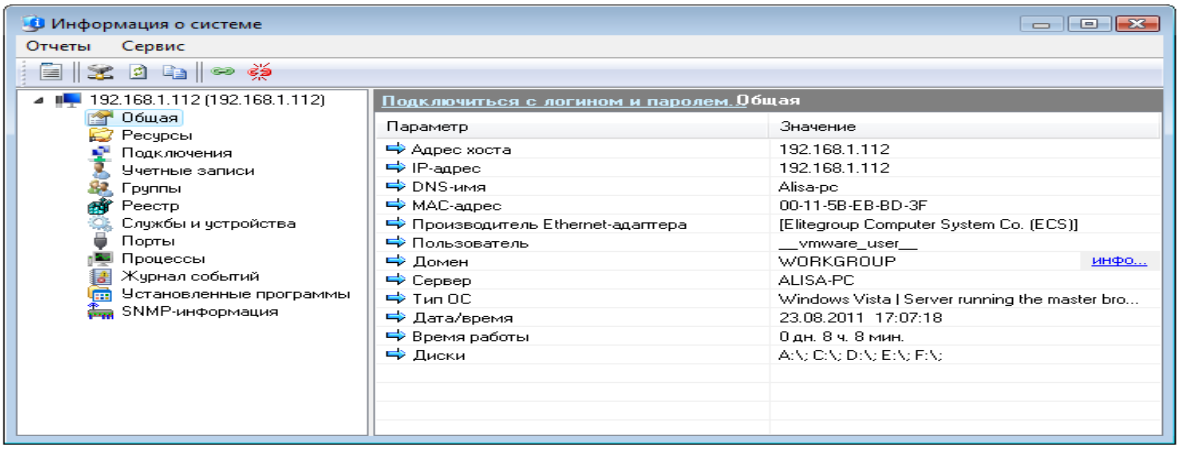


Рис. 14. Інформація про систему

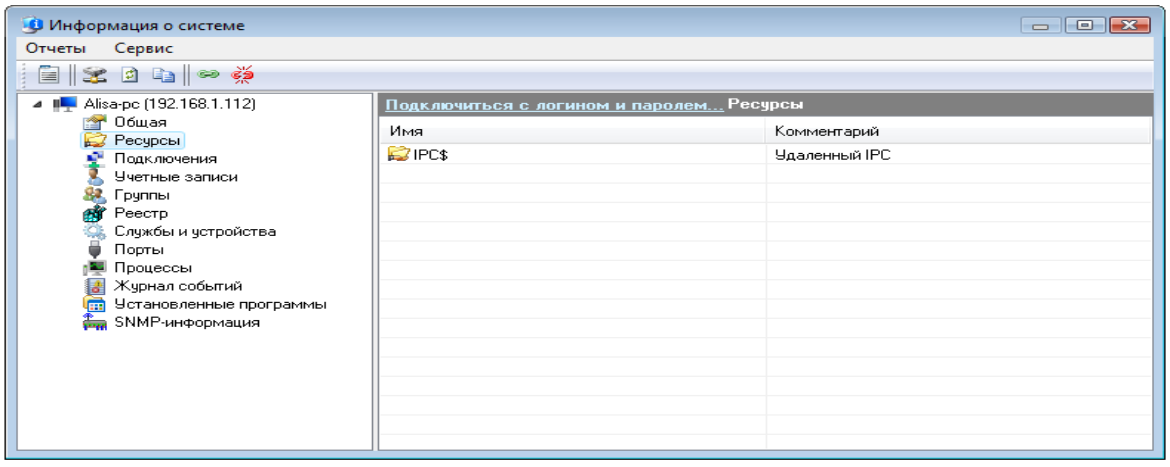


Рис. 15. Список ресурсів віддаленого ПК

Ресурси

У цьому розділі ви можете подивитися список відкритих ресурсів віддаленої машини (рис. 15). У списку можуть бути показані й так звані сховані ресурси (зі значком $). Зі списку ресурсів ви можете легко відкрити їх у Провіднику (подвійним кличем миші на рядку).

Для підключення мережевого диска виділіть ресурс у списку й виберіть пункт контекстного меню **Подключить сетевой диск...** Після підключення диска, автоматично відкривається вікно провідника.

Підключення

У цьому розділі ви можете одержати інформацію про поточні підключення до віддаленої машини, або відстежити, хто в цей момент використовує мережеві ресурси на будь-якій машині мережі (рис. 16).

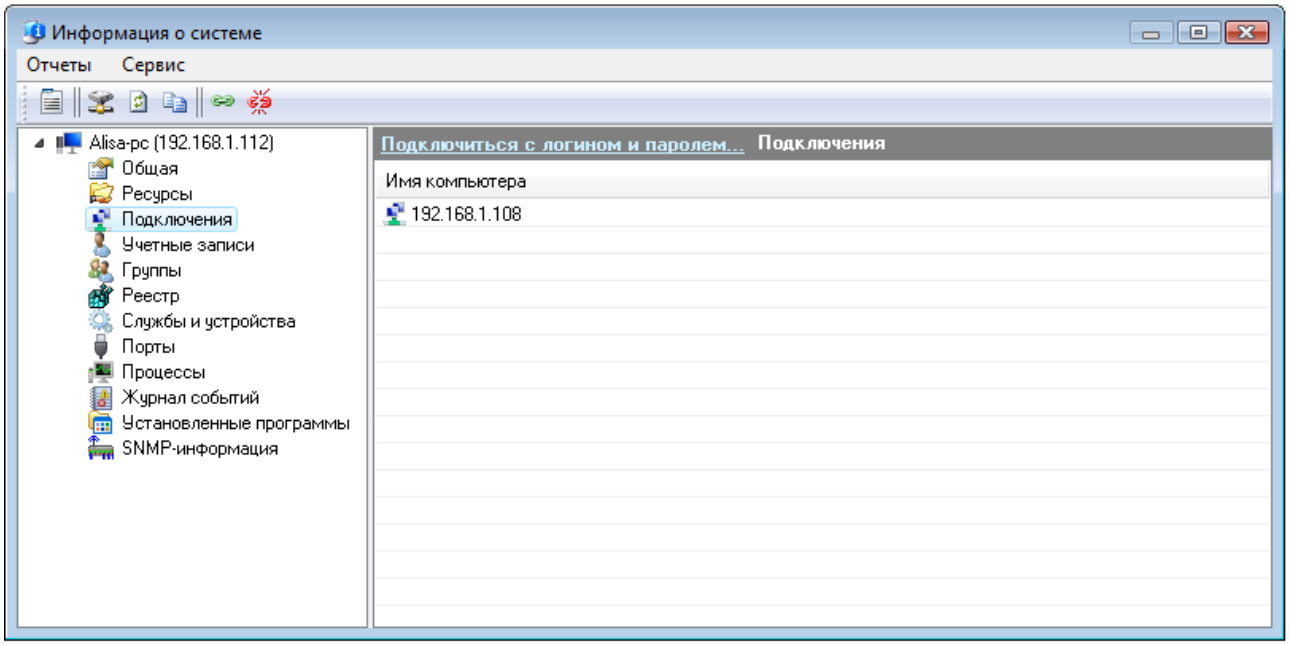


Рис. 16. Вікно підключення на віддаленому ПК

Облікові записи

У цьому розділі ви можете переглянути список облікових записів віддаленої машини (рис. 17) й вибрати тип відображуваних записів (фільтр).

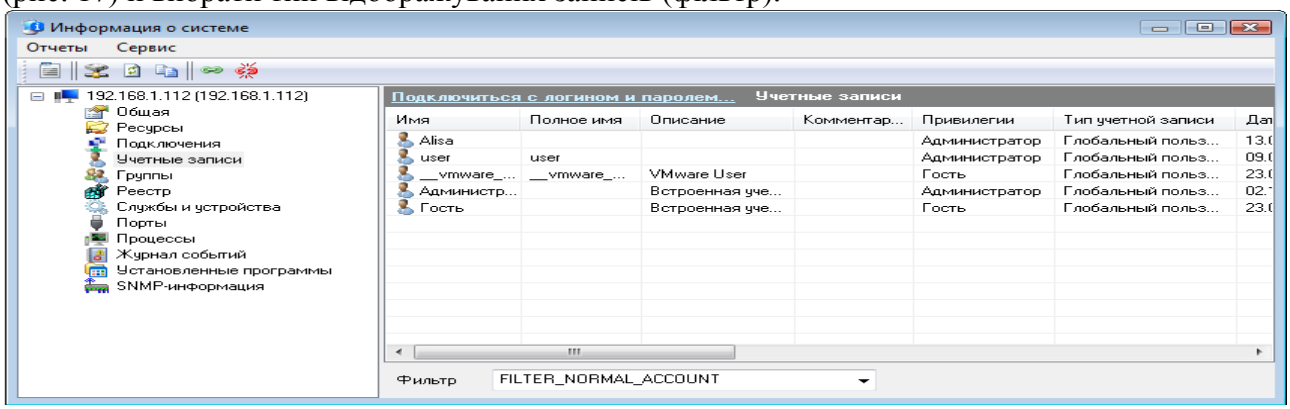


Рис. 17. Вікно облікових записів на віддаленому ПК

Групи

Список локальних і глобальних груп користувачів віддаленої машини (рис. 18).

Реєстр

У цьому розділі ви можете переглядати реєстр на віддаленій машині (рис. 19).

Одержання інформації про зміст реєстру виконується динамічно, через що можлива деяка затримка при розкритті вузлів. Не всі відображувані дерева реєстру можуть бути розкриті, як і не всі розділи можуть бути доступні. Це визначається налагодженням політики безпеки на віддаленій машині.

Через контекстне меню дерева ключів доступне копіювання їх імен у буфер.

За подвійним кликом на виділеному рядку параметра з'являється вікно з полями, у яких відображаються параметр і значення, які також можна скопіювати в буфер.

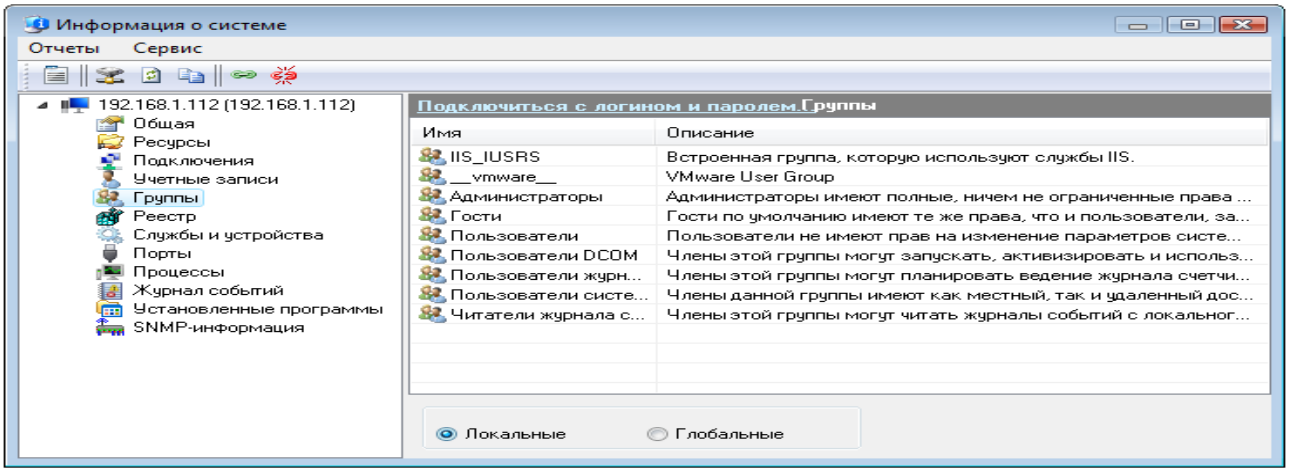


Рис. 18. Список груп користувачів на віддаленому ПК

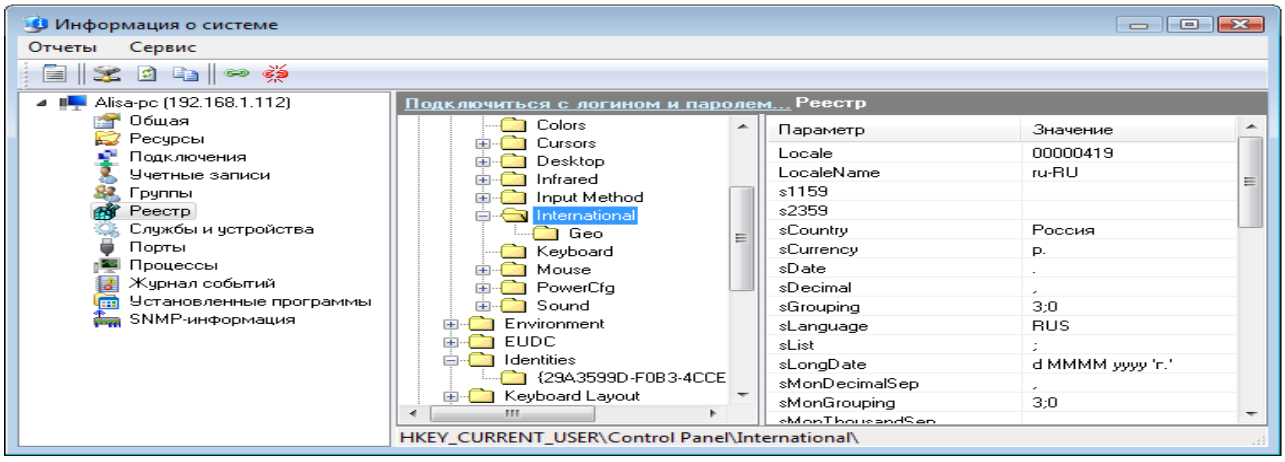


Рис. 19. Реєстр на віддаленому ПК

Через контекстне меню списку параметрів доступна зміна, додавання, видалення параметрів і їх значень. Однак операції зі зміни реєстру віддаленого комп'ютера вимагають повноважень адміністратора..

Служби й пристрої

Програма дозволяє одержати список усіх служб і пристроїв віддаленого комп'ютера (рис. 20). Можна відображати тільки ті служби, тип яких відповідає обраному значенню поля **Тип**. Також можна відображати/не відображати активні/не активні служби (список **Состояние**).

При наявності повноважень адміністратора на віддаленому комп'ютері доступне керування службами: пуск, зупинка, перезапуск. Для керування виділеної в списку службою необхідно вибрати відповідний пункт контекстного меню.

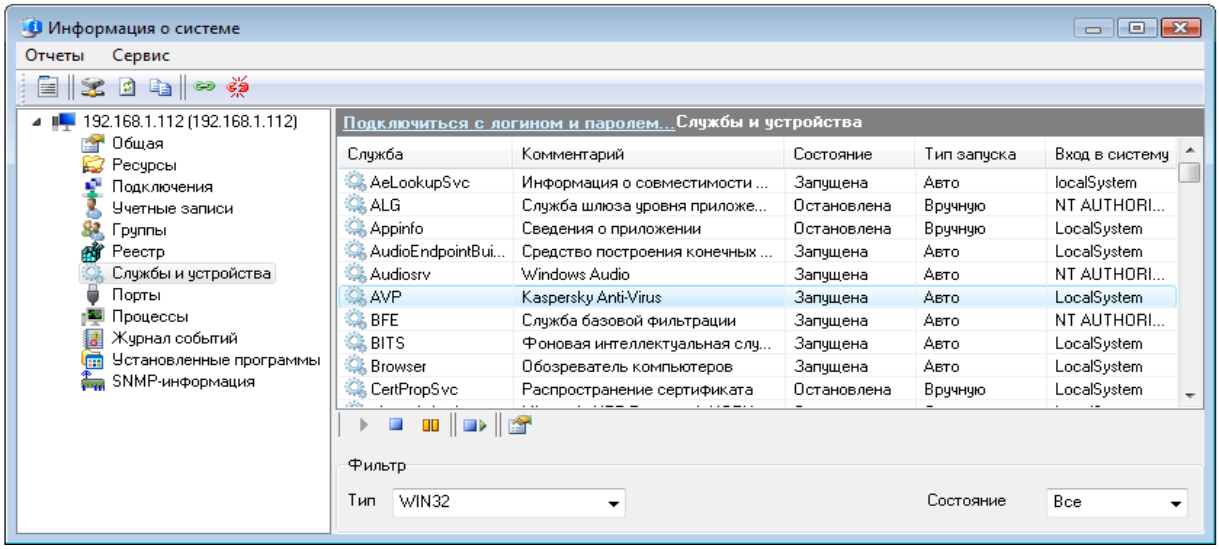


Рис. 20. Служби та пристрої на віддаленому ПК

Порти

За допомогою сканера портів можна одержати інформацію про відкриті порти вашої й віддаленої машини (рис. 21). Функція визначає як TCP, так і UDP порти. Можна вказати інтервал сканування й затримку – час, протягом якого програма буде чекати відповіді від віддаленого комп'ютера.

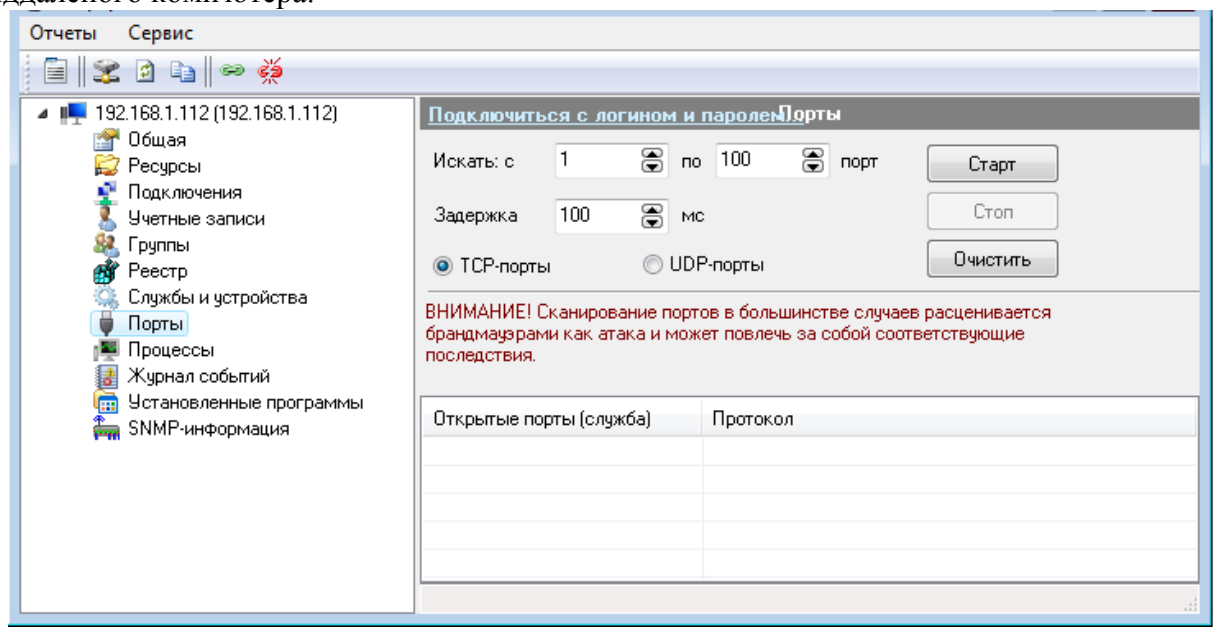


Рис. 21. Порти на віддаленому ПК

ВАЖЛИВО!: Сканування портів у більшості випадків розцінюється брандмауерами віддалених хостів як атака, що може викликати відповідні наслідки.

Процеси

У цьому розділі (рис. 22) ви можете подивитися список активних процесів на віддаленій машині.

Журнал подій

Програма дозволяє читати журнали подій (рис. 23) з віддалених машин. Доступні журнали системних, прикладних подій і, при певних правах у домені (роб. групі), подій служб безпеки. При цьому доступно докладний опис події (помилки, повідомлення, попередження). Для перегляду події необхідно подвійним клацанням на виділеному записі журналу відкрити вікно **События** (рис. 24)**.** Кнопки навігації (продубльовані "гарячими клавішами" Left, Right Arrow) дозволяють швидко переходити до наступного або попередньому запису журналу.

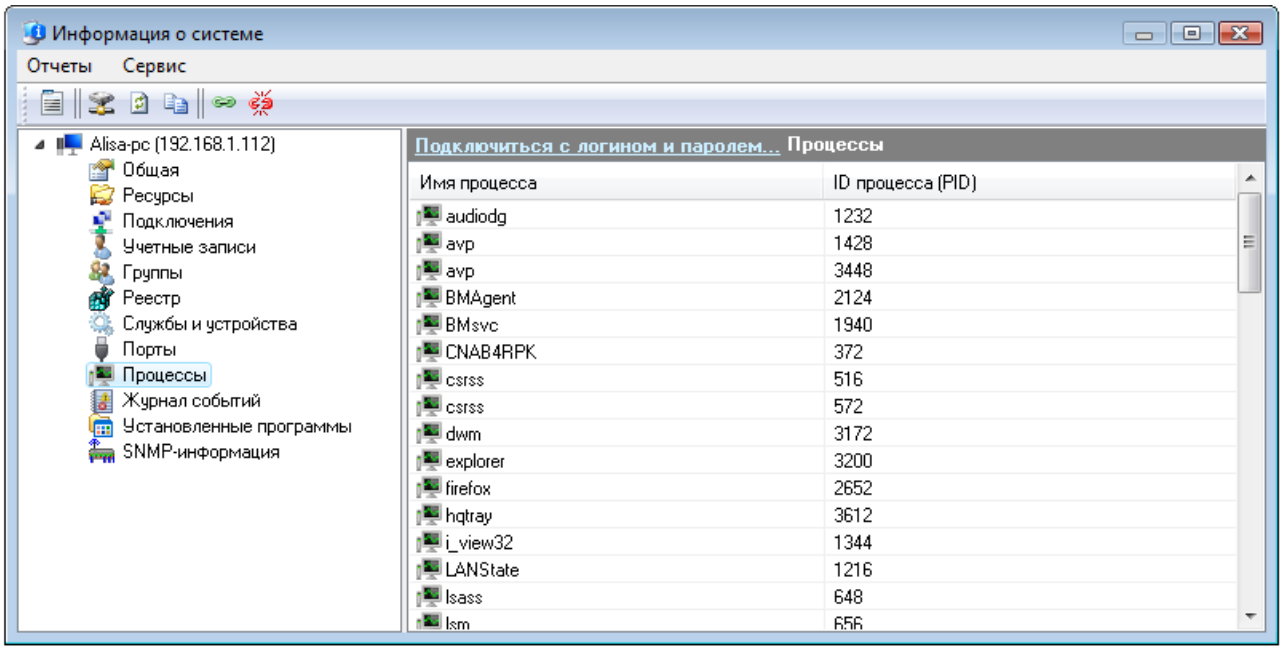


Рис. 22. Процеси на віддаленому ПК

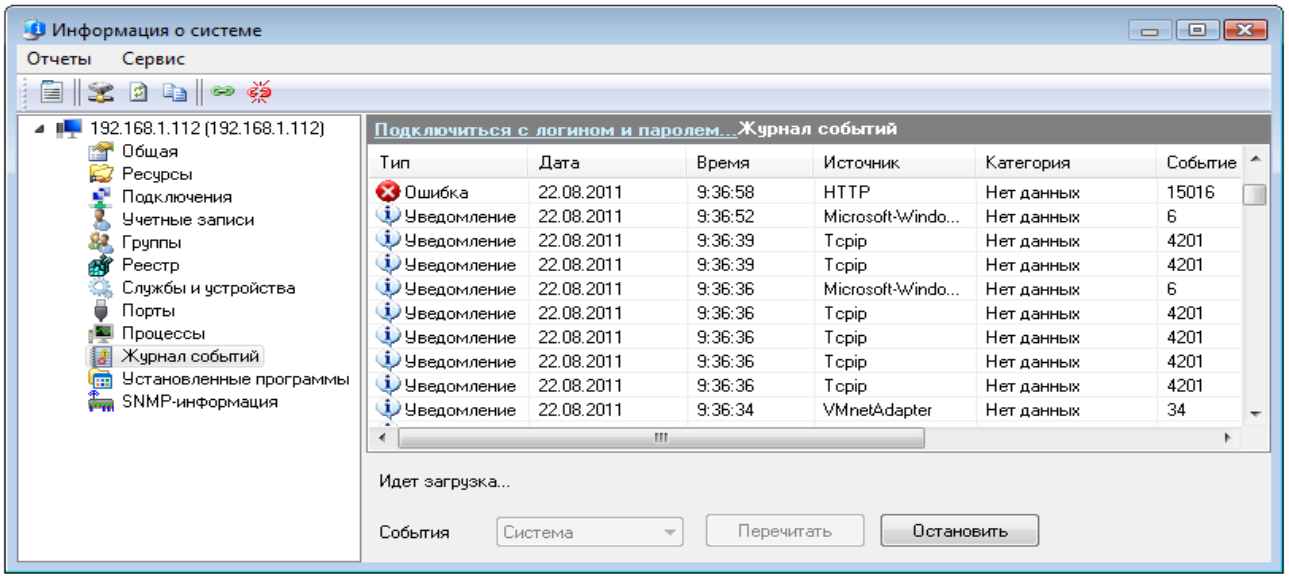


Рис. 23. Журнали на віддаленому ПК

Установлені програми

У цьому розділі ви можете одержати список установлених на віддаленому комп'ютері програм. Для успішної роботи функції необхідно мати:

- Наявність прав адміністратора на віддаленому комп'ютері;
- Запущену на віддаленому комп'ютері службу ***"Вилучене керування реєстром"***.

SNMP-Інформація

Програма може одержувати масу корисної інформації з комутаторів, роутерів і інших мережевих пристроїв, що підтримують SNMP-Протокол. Кожний комп'ютер при наявності активного SNMP-Агента може віддавати програмі інформацію із протоколу SNMP. В операційній системі Windows 2000/XP/2003/Vista SNMP-Агент реалізований у вигляді служби **"Служба SNMP"**.

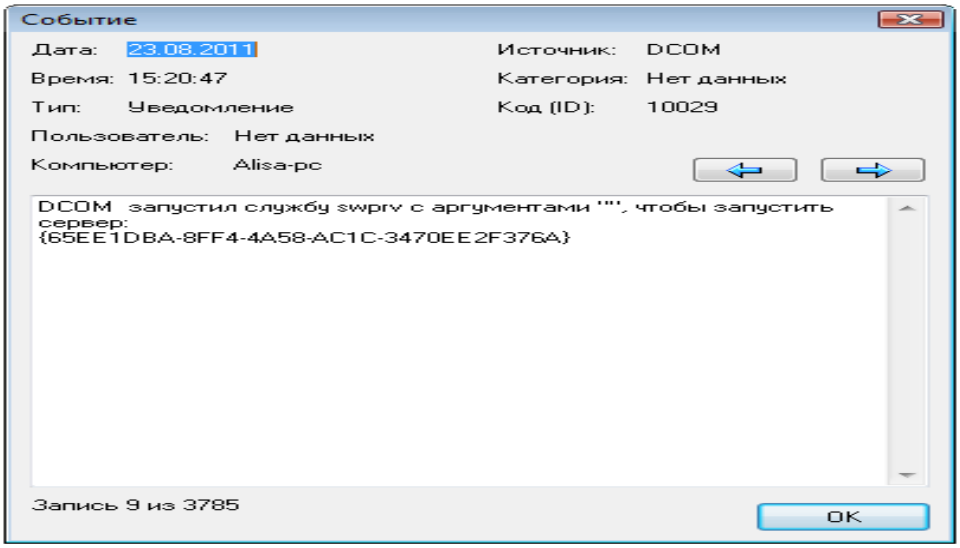


Рис. 24. Подія на віддаленому ПК

1.8. Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP

Увага! Уважно вивчіть проблеми безпеки перед установкою служби SNMP на комп'ютер. Змініть community за замовчуванням, налагодьте обмеження в брандмауерові.

Часто в деяких мережевих пристроях (таких, як роутери, комутатори, мережеві принтери і т.д.) SNMP- Агент присутній, але не запущений. Для його запуску звичайно виконують наступні дії: звертаються до налагодження пристрою через Web-Інтерфейс, шукають параметр типу **"SNMP Agent (Disable/Enable)"** і встановлюють перемикач у позицію **Enable**, при цьому попутно звернувши увагу на параметр Community.

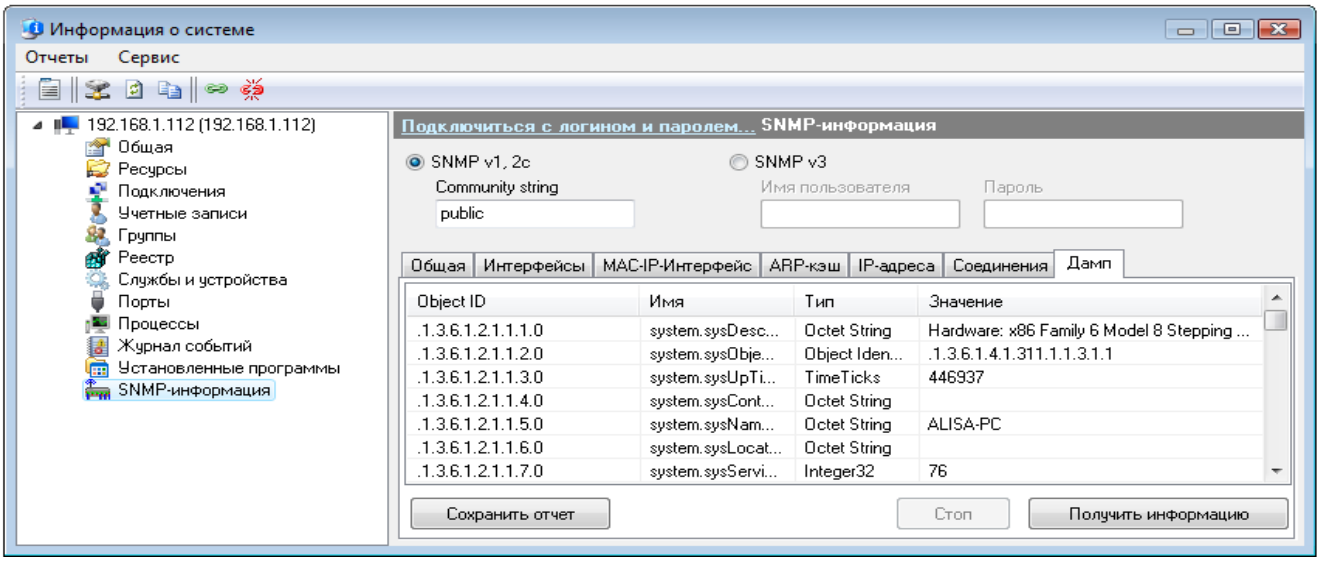


Рис. 24 SNMP-інформація на віддаленому ПК

Community (співтовариство) - це свого роду пароль доступу до інформації в пристрої. Даний пароль необхідно вказувати в поле SNMP Read Community string (рис. 24). Для одержання інформації необхідно вибрати, вкладку й нажати кнопку **Получить информацию**. На всіх вкладках, крім **Общая,** є кнопка **Сохранить отчет**, що дозволяє вивантажити отриману інформацію в CSV-Файл.

На вкладці **интерфейсы** можна одержати інформацію про існуючі у пристрої мережеві інтерфейси з докладною інформацією про кожний з них. Крім цього, доступна мережева статистика за вхідними і вихідними пакетами, що дозволяє відслідковувати мережевий трафік на віддалених пристроях.

На вкладці **Mac-Ip-Интерфейс** можна одержати інформацію про таблицю з'єднань.

На вкладці **Соединение** можна одержати інформацію про поточні TCP і UDP з'єднання хосту. Приводиться інформація про стан з'єднання, номер віддаленого/локального порту, віддаленої/локальної Ip-Адреси.

На вкладці **ДАМП** можна одержати всю доступну за SNMP-Протоколом інформацію від віддаленого пристрою. Одержання інформації може забрати тривалий час (залежить від пристрою), протягом якого не можна буде одержати інформацію з інших вкладок.

Дані можуть бути збережені в CSV-Звіт. Для зручного перегляду інформації можна подвійним клацанням на будь-якому записі відкрити вікно **Детальный просмотр** (рис. 25). Можна переходити до наступного / попереднього запису, натискаючи кнопку **След. >>/<< Пред.**

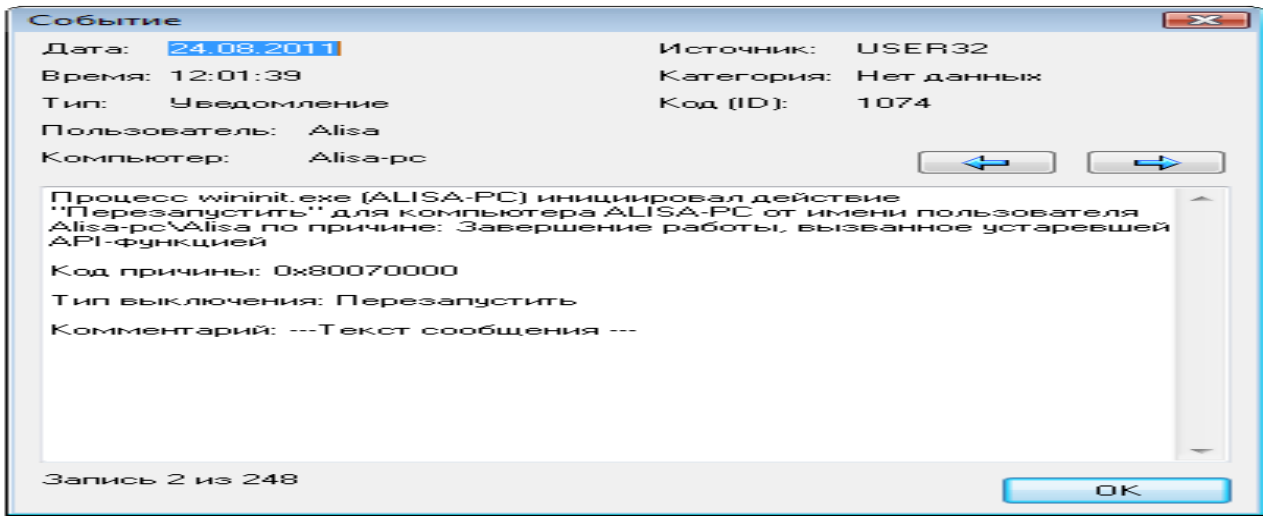


Рис. 25. Подія на віддаленому ПК

Інформація про домен

У вікні **Інформація про домен** зібрані відомості про домен або робочу групу. Доступна наступна інформація:

- Ім'я контролера домену;
- DNS-Ім'я контролера домену;
- Список довірених доменів;
- Користувачі, робочі станції, групи.

Одержання інформації може забрати тривалий час. Необхідно дочекатися закінчення роботи функції.

1.8. Робота з папками

У вікні відображаються папки вашого комп'ютера, до яких у даний момент призначений загальний доступ. (рис. 26)

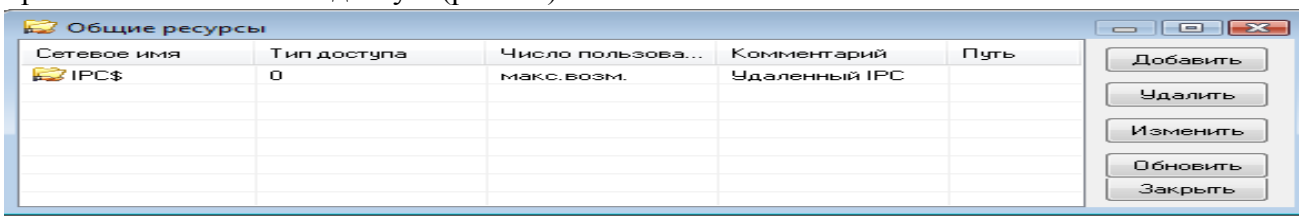


Рис. 26. Вікно папок

Ви можете:

- Змінити тип доступу до папок, вибравши в контекстному меню пункт **Изменить** й замінивши відповідні значення полів у вікні **Доступ** (рис. 27)**;**
- Закрити доступ, нажавши кнопку **Удалить;**
- Відкрити доступ до нової папки, нажавши кнопку **Добавить** й вибравши в дереві каталогів необхідну папку.

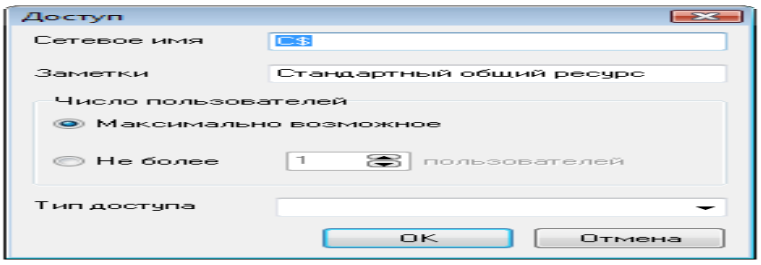


Рис. 27. Вікно доступу

1.9. Пінг

Функція **Пінг** подібна команди Winows - ping, але більш зручна (рис. 28). Можливе завдання параметрів:

- Розмір пакета даних;
- Число запитів;
- Час очікування.

Результати пінга, як і повідомлення про помилки, помістяться у вікно **Результат.**

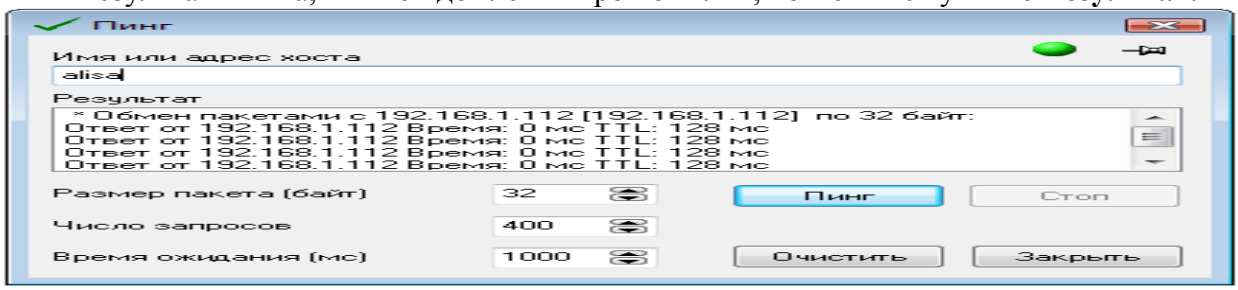


Рис. 28 Вікно пінг

Індикатор у верхньому правому куті повідомляє про готовність (зелений) або зайнятості (червоний).

Процес пінга можна зупинити натисканням кнопки **Стоп.**

1.10. Трасування маршруту

Функція **Трасувати маршрут** подібна команди Winows ***tracert***, але більш зручна (рис. 29). Можливе завдання параметрів:

- Число переходів**;**
- Час очікування**.**

Результати трасування помістяться у вікно **Результат**.

Індикатор у верхньому правому куті повідомляє про готовність (зелений) або зайнятості (червоний).

Процес трасування можна зупинити натисканням кнопки **Стоп**

1.11. Мережевий трафік

У цьому вікні бачимо статистику вхідного й вихідного локального трафіка (рис. 30), а також найменування й Мас-Адреса інтерфейсу, через який він проходить (рис. 31).

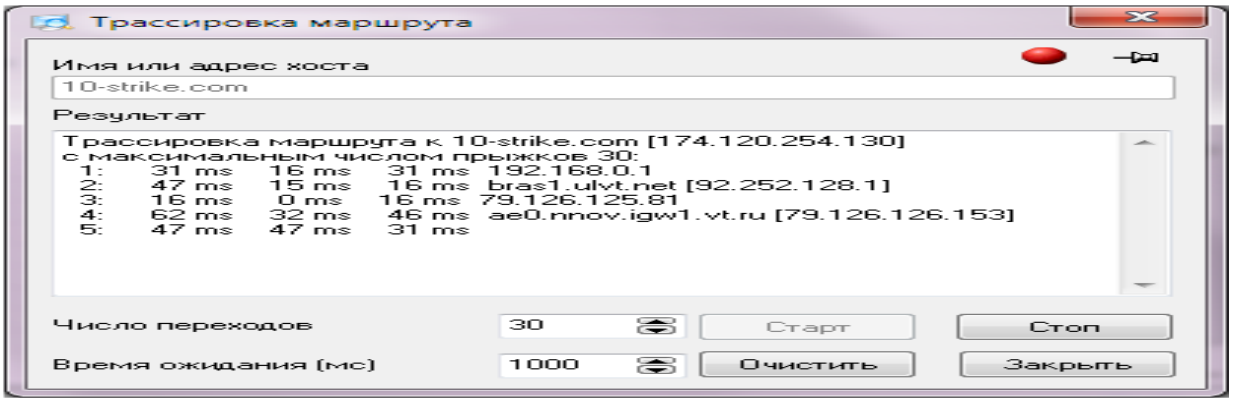


Рис. 29. Вікно трасування

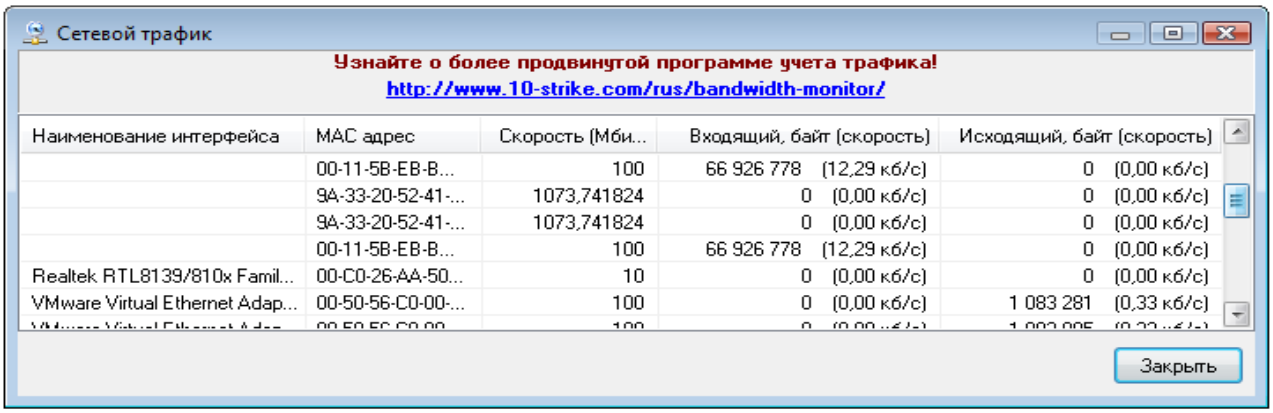


Рис. 30. Вікно мережевого трафіку

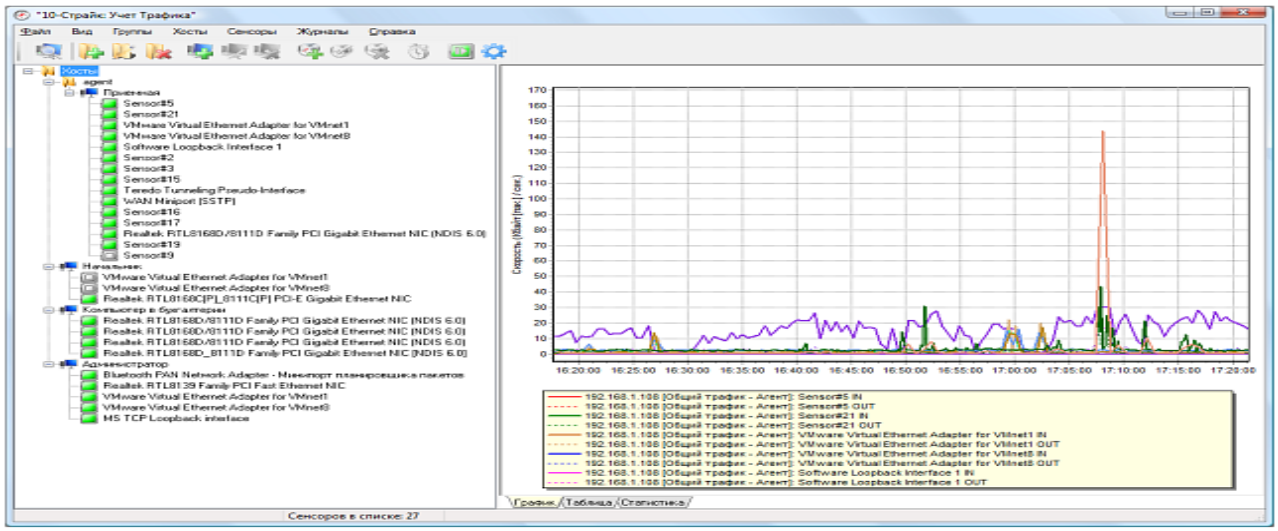


Рис. 31. Вікно графічного відображення мережевого трафіку

2. Хід роботи

Виконати роботи згідно п 1. Звіт представити в вигляді рисунків та пояснювального тексту. Сканування мережі провести трьома способами.

3. Контрольні питання

1. Призначення програми.
2. Можливості програми.
3. Як створити список хостів мережі?
4. Робота зі списком хостів.
5. Як завершити роботу віддаленого комп'ютера?
6. Як включити комп'ютери за мережею?
7. Як отримати інформацію про систему.
8. Установка підтримки SNMP на ПК з Windows Налаштування властивостей безпеки SNMP .
9. Робота з папками.
10. Як провести пінг мережі?
11. Як трасувати маршрут до віддаленого хосту?
12. Як отримати мережевий трафік?

ЛАБОРАТОРНА РОБОТА 29.
ЗНАЙОМСТВО З ПРОГРАМАМИ КОНТРОЛЮ ТРАФІКУ МЕРЕЖ

Мета роботи: уміти користуватися програмами контролю трафіку локальних та глобальних мереж; формувати відповідні команди; аналізувати отримані дані.

Зміст

1. Теорія
1.1. Поняття трафіку мереж
1.2. Лічильники трафіку
1.3. Приклади програмного забезпечення контролю трафіка
1.3.1 ProxyInspector
1.3.2. NetWorx
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Поняття трафіку мереж

Трафік це основний і єдиний ресурс будь – якого типу мережі, в тому числі мережі Internet, з погляду протоколів транспортного рівня. Як відомо, будь-яка інформація в мережі Internet передається у вигляді окремих пакетів – блоків даних порівняно невеликого розміру, кожний з яких має адреса відправника й одержувача й подорожує за мережею самостійно. Отож, трафік це сумарний обсяг пакетів, що пройшли через крапку спостереження. Якби Internet був транспортною компанією, то трафік це сумарна вага вантажів, перевезених пакетами – вантажівками незалежно від конкретного змісту вантажів. Коли ми працюємо із трафіком, ми абстрагуємося від умісту пакетів, оскільки в цьому контексті нас цікавить не що саме передане, а скільки й звідки. З іншої сторони, для кінцевого користувача мережі Internet інтерес представляє не тільки скільки й звідки даних було отримано, тобто кількість, але і якість, а саме що містилось у цих отриманих даних. У загальному випадку завдання обліку трафіка для операторів і для кінцевих споживачів відрізняється саме тим, що останнім необхідно контролювати не тільки кількість, але і якість трафіка, тобто у певних межах його вміст.

Якщо говорити про облік трафіка при роботі компаній з Internet, то виникає поняття трафіка вхідного й вихідного. Вхідний трафік це всі пакети, які перетнули границю мережі між вашою організацією й будь-якою іншою мережею в напрямку « до вас». Це обсяг імпортованих вами з Internet даних. Вихідний – відповідно, обсяг експортованих вами даних.

Інформаційні технології є невід'ємною частиною життя сучасного суспільства. Чималу користь приносять вони й бізнесу. Однак дана «медаль» має й зворотний бік. Можливості всесвітньої павутини можуть використовуватися персоналом для вивчення кон'юнктури ринку, спілкування з потенційними й діючими клієнтами, пошуку нових можливостей для підвищення ефективності комерційної діяльності. Але нерідко трафік складається й з інших показників: спілкування співробітників у соціальних мережах, приємного часу проведення на інших тематичних, але, що не мають до трудової діяльності, порталах. І все це в робочий час, який оплачується компанією. Зрозуміло, подібний стан справ погано кореспондується з інтересами бізнесу й наносить йому істотні збитки.

Для усунення цієї проблеми й контролю над трафіком компанії використовують різні методи. Хтось перекриває доступ до соціальних мереж, хтось забороняє використання Internet зовсім. Існують також каральні заходи, застосовувані до недбайливих співробітників за результатами різних тотальних перевірок трафіка. Разом з тим, усі ці способи є малоефективними (співробітники цілком можуть обійти будь-які встановлені перешкоди) і не сприяють створенню здоровішої атмосфери в колективі. От чому, найбільш

ефективним методом, як з погляду звичайних користувачів, так і з погляду фахівців, є використання спеціальних систем для обліку трафіка (лічильників трафіка).

1.2. Лічильники трафіку

Лічильник трафіку корисна річ. Особливо, якщо у Вас обмежений доступ у мережу за часом або обсягу використаних мегабайтів. Не у всіх же безліміт, правда? У багатьох удома безлімит, а для ноутбука використовують 3G зв'язок або мобільний Internet поза будинком, наприклад. І такий вид зв'язку звичайно обмежений. Треба стежити за витратою трафіка, щоб не потрапити на гроші при перевитраті.

Цікаво деколи знаті активність свого ПК чи комп'ютерів інших користувачів у локальній мережі на рахунок споживання трафіку Internet-з'єднання. Для персонального використання це може бути необхідно, коли у Вас тариф з певним обмеженням за об'ємом трафіку або коли у Вашій локальній мережі присутній ще один комп'ютер. Для організацій – це може бути корисним для контролю за споживанням Internet мережі робочими ПК та інше. Ситуацій можна вигадати та змоделювати безліч.

Облік Internet трафіка користувачів локальної мережі забезпечує контроль трафіка користувачів і захист від перевитрати бюджету підприємства на зв'язок.

Існує ціла група програм Firewall та брандмауерів для точного обліку трафіка користувачів, пропонують зручні способи моніторингу й обмеження трафіка – відображення спожитого трафіка в режимі реального часу, різні квоти вихідного й вхідного трафіка, погодинний розклад роботи, блокування доступу в Internet для користувача або групи користувачів при вичерпанні квоти трафіка Internet і т.п. Вони розглядаються в навчальній дисципліні «Інформаційна безпека».

В даній лабораторній роботі ми розглянемо більш прості програмні засоби, такі як, наприклад, NetWorx 5.5.0, TMeter, NetWorx, BWMeter 6.11.2, Tmeter, NetBalancer 9.1.4, DU Meter 7.11.4757, NetworkTrafficView 2.01, Windows 10 Firewall Control 7.3.11.3, NetLimiter Pro 3.0.0.11 / 4.0.15.0, BWMeter 6.11.1, NetWorx 5.4.2, BitTally, Traffic Inspector 3.0, Speed-O-Meter 4.1, Traffic Monitor 1.1.4, BitMeter, ProxyInspector і т.п.

1.3. Приклади програмного забезпечення контролю трафіка

1.3.1. ProxyInspector

ProxyInspector – система обліку трафіка, впроваджена сьогодні на багатьох підприємствах. Дана програма призначена для обліку трафіка Internet й контролю над цільовим використанням мережі Internet співробітниками компанії.

Безумовно, однієї із кращих у цьому випадку є програма Proxyinspector. Переваги даної системи обліку трафіка очевидні.

По-перше, дана програма обліку трафіка може бути встановлена на будь-який офісний комп'ютер. По-друге, програма самостійно становить звіти про використання трафіка кожним зі співробітників. Формовані нею документи максимально прості для розуміння й сприйняття й дозволяють одержати об'єктивну картину про те, як використовує робочий час персонал. По-третє, підрахунок трафіка за допомогою Proxyinspector знімає навантаження з It-Кадрів: системний адміністратор може займатися розв'язком більш важливих завдань, ніж контроль за Internet-трафіком. Графічні приклади такого контролю наведеня на рис. 1.

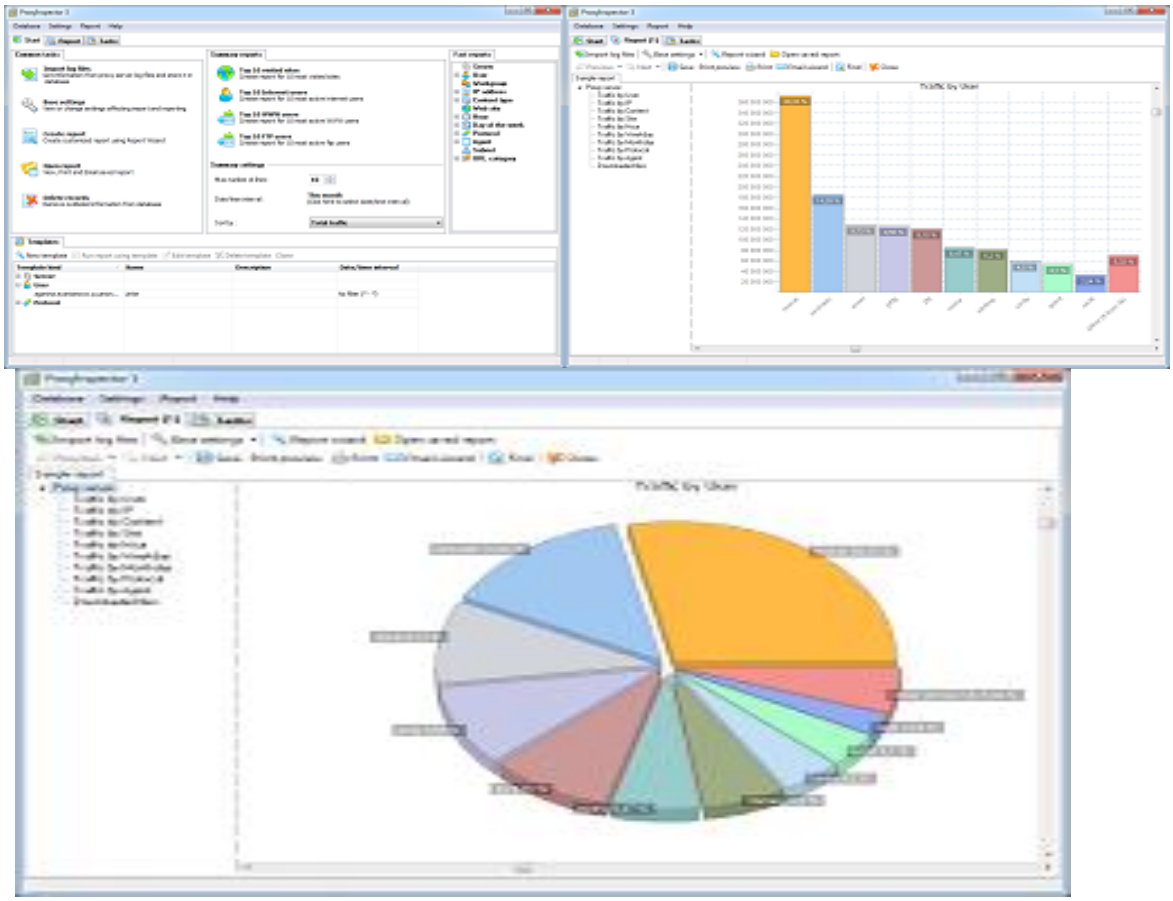


Рис. 1. Приклади результатів контролю

Однак було б неправильно обмежувати можливості системи обліку трафіка тільки контролем над раціональним використанням мережі Internet. Насправді, список переваг, якими має дана програма, куди ширше. Пропонована нами система обліку трафіка дозволяє боротися з комерційним шпигунством, запобігати витоку важливих відомостей на сторону й багато чого, багато чого іншого.

Установивши систему обліку трафіка, ви зможете:

- Довідатися, як саме ваші співробітники використовують можливості трафіка: які файли вони скачують, які сайти відвідують, чим цікавляться в пошукових системах.
- Здійснювати підрахунок трафіка за різними групами: користувачів, типу інформації, протоколам, робочим станціям, правилам firewall і т.д.

Система підрахунку трафіка Internet Proxyinspector сумісна з наступними ОС: Windows 2000/XP/2003/Vista/2008/7/8/2012.

Пропонована програма обліку трафіка підтримує такі Проксі-сервери, як:

- Eproxy/Eserv
- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Microsoft ISA Server 2006
- Squid
- Kerio Winroute Firewall
- Microsoft Forefront Threat Management Gateway 2010
- Kerio Control
- Qbik Wingate

У найпростішому варіанті запуск *Iperf* відбувається в такий спосіб:

iperf -s – на сервері (рис. 2).

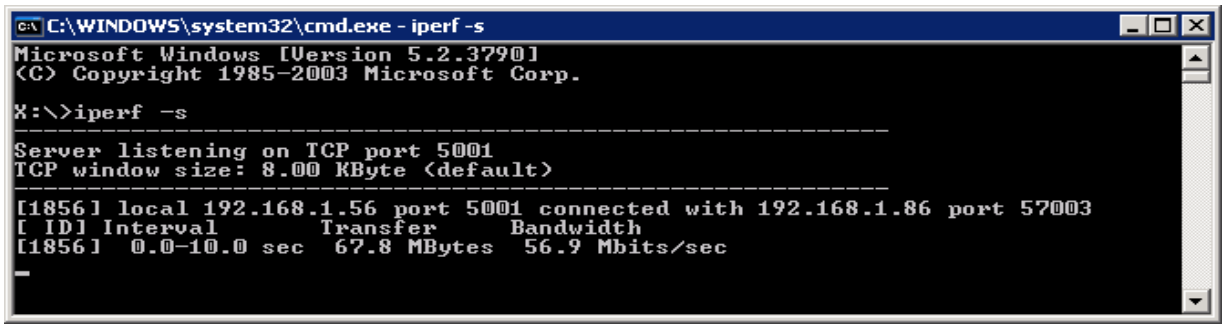


Рис. 2. I**perf -s** – на сервері

iperf –c 192.168.1.56 – на клієнтові, де 192.168.1.56 – Ip-*Адреса* сервера (рис. 3).

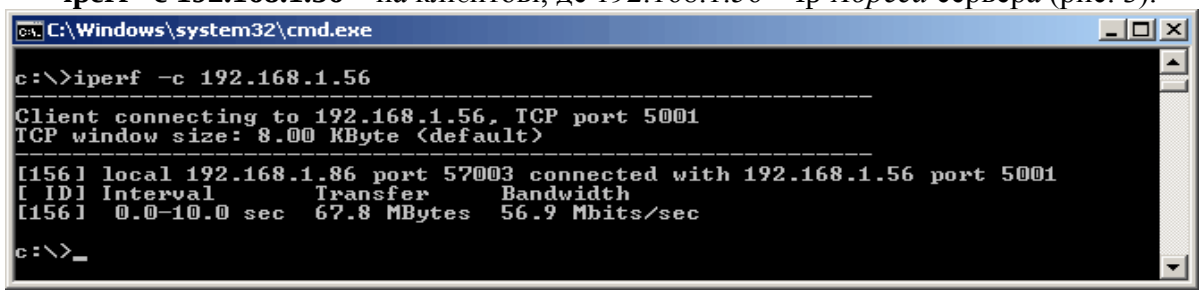


Рис. 3. I**perf -s** – на робочій станції

За замовчуванням використовується *TCP* порт 5001, тестування проходить протягом 10 секунд. Цього цілком достатньо для швидкої оцінки швидкості з'єднання, однак можливості *Iperf* цим не обмежуються. Наприклад: iperf -s -i10 -p80 – сервер прослуховує 80 порт і видає результат з інтервалом в 10 секунд (рис. 4).

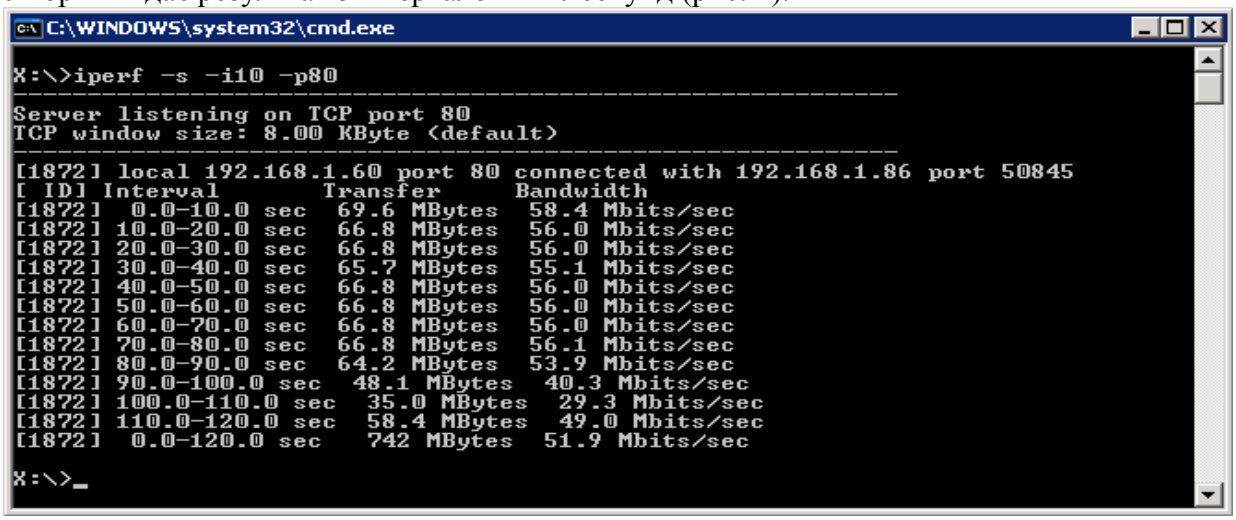


Рис. 3. Прослуховування 80-го порту

Наведемо список опцій програми:

- **-f** — у якому форматі показувати швидкість (*Kbits, Mbits, Kbytes, Mbytes*)
- **-i** — з якими інтервалами відображати проміжні результати
- **-l** — розмір буфера (за замовчуванням 8 *KB*)
- **-m** — показувати максимальний розмір *TCP* сегмента (*MSS*)
- **-p** — указати порт, за якими буде відбуватися з'єднання (за замовчуванням 5001)
- **-u** — використовувати *UDP* замість *TCP*
- **-w** — розмір вікна *TCP*
- **-B** — вказівка для сервера, на якому інтерфейсі ухвалювати трафік
- **-C** — режим сумісності зі старими версіями

- **-M —** дозволяє змінити максимальний розмір *TCP* сегмента (*MSS*)
- **-N —** міняє деякі опції *TCP* (відключення алгоритму Нахабна)
- **-V —** використовувати *IPV6*
- **-h** — вивід довідки

Опції для сервера:

- -s — запустити як сервер і відображати всю інформацію на екран;
- -D — запустити як сервіс (у фоновому режимі) і не відображати інформацію.

Опції клієнта:

- **-b** — використовувана смуга для *UDP* (за замовчуванням 1*Mbit/sec*)
- **-c** — запустити як клієнт і з'єднатися із сервером
- **-d —** тестувати лінію в обидва боки
- **-n —** установити розмір переданого трафіка (не можна використовувати с ключем **-t)**
- **-r** — робити тестування окремо для кожного
- **-t** — указати час тестування (за замовчуванням 10 сек.)
- **-F —** не генерувати трафік, а передавати готовий файл
- **-I —** введення даних, переданих з *STDIN* (стандартний потік уведення)
- **-L** — порт, на якім клієнт буде ухвалювати двонаправлений трафік
- **-P —** запуск декількох потоків паралельно
- **-T —** час життя пакета для групового розсилання (за замовчуванням 1)

Існує також версія програми з графічною оболонкою.

1.3.2 NetWorx

Для початку роботи треба розпакувати архів із програмою й запустити exe-файл. Слідуємо за майстром – натискаємо **Next** та відбираємо параметри (рис. 4-6).

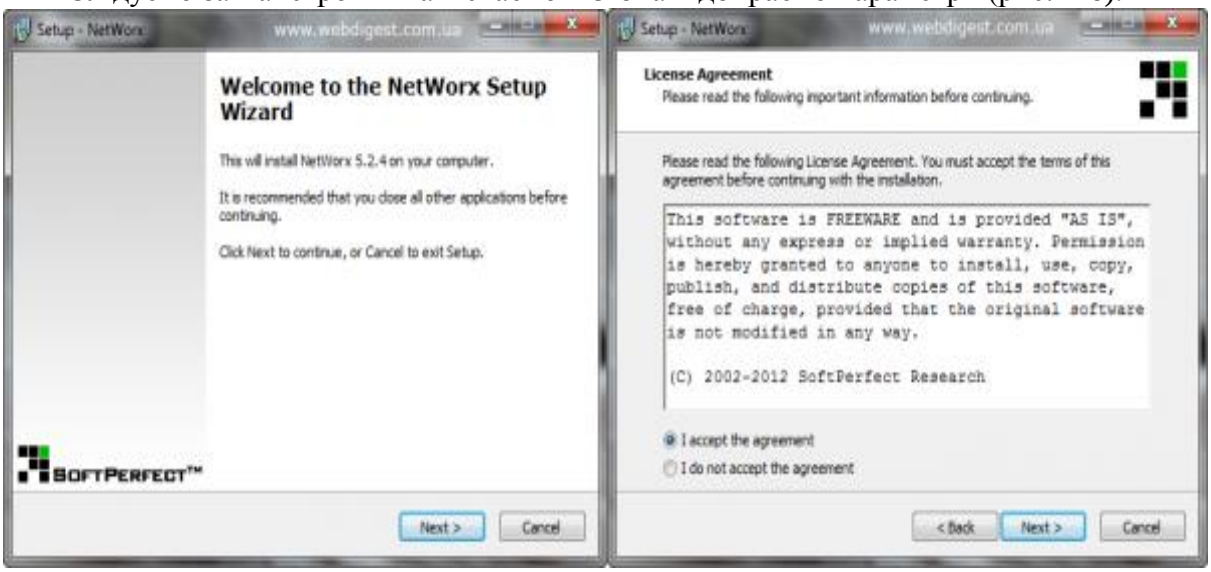


Рис. 4. Запуск установки програми та прийняття ліцензійної угоди

Шлях установки програми NetWorx – при бажанні можемо змінити і поставити програму в інше місце – **Next.**

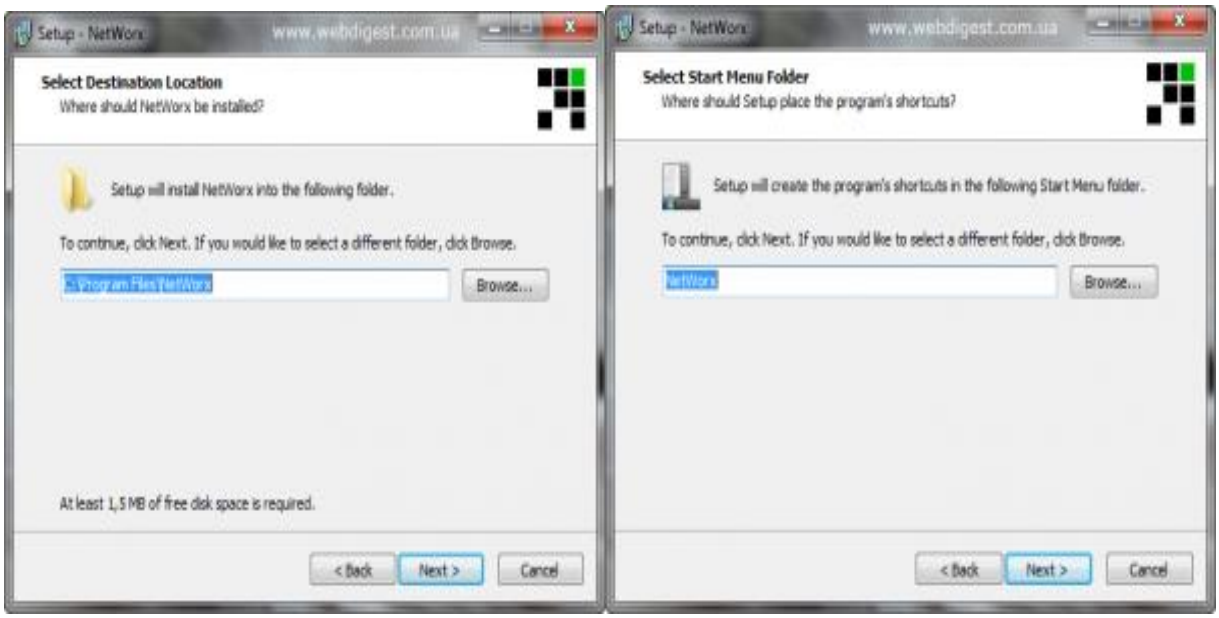


Рис. 5. Відбір місця встановлення програми

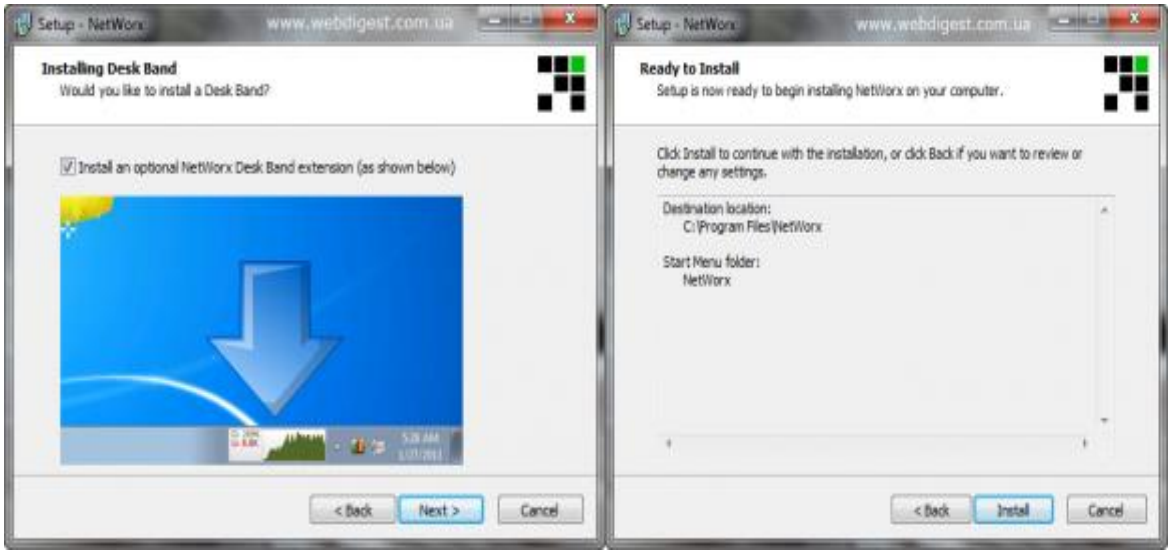


Рис. 6. Закінчення процедури інсталяції програми

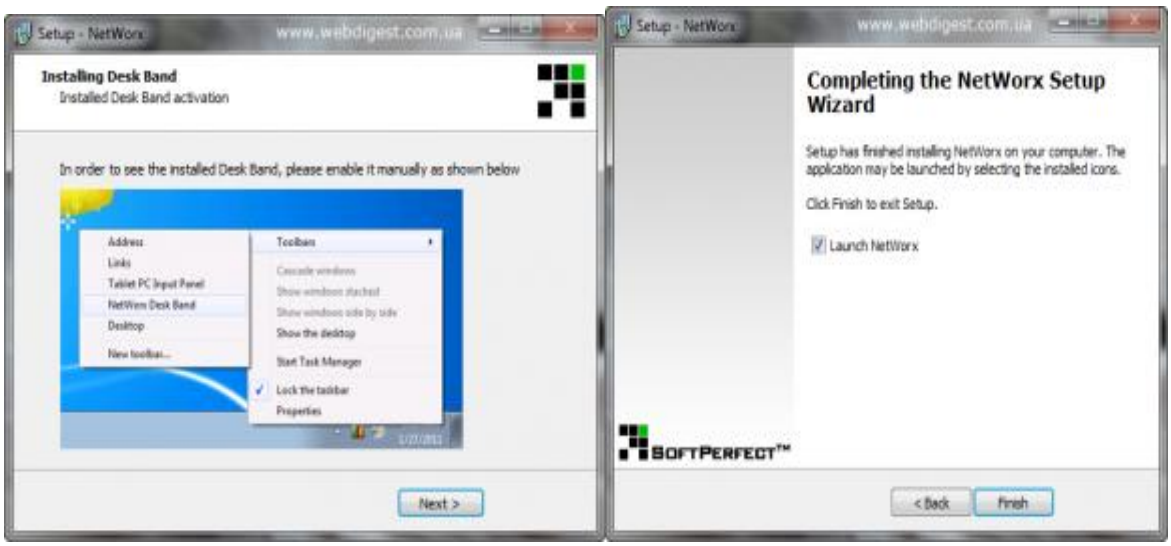


Рис. 6. Остаточний фініш установки програми

Після цього в треї (місце поруч із системним годинником) з'явиться значок програми (рис. 7), за допомогою якого ми й будемо нею управляти.

Рис. 7. Значок програми

Керування Networx буде відбуватися через контекстне меню, яке викликається правою клавішею миші (рис. 8,а). Далі проведемо налагодження параметрів програми (рис. 8,б).

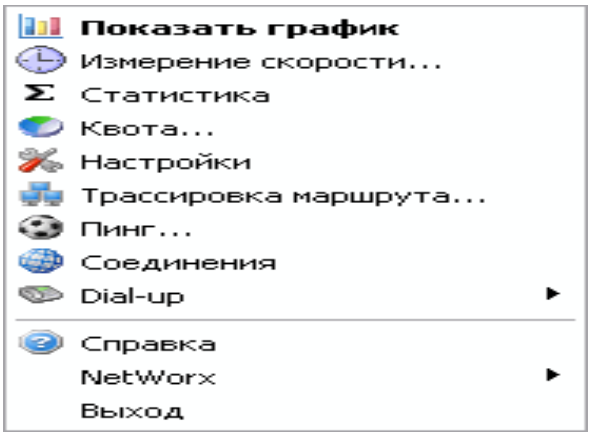


Рис. 8,а. Контекстне меню

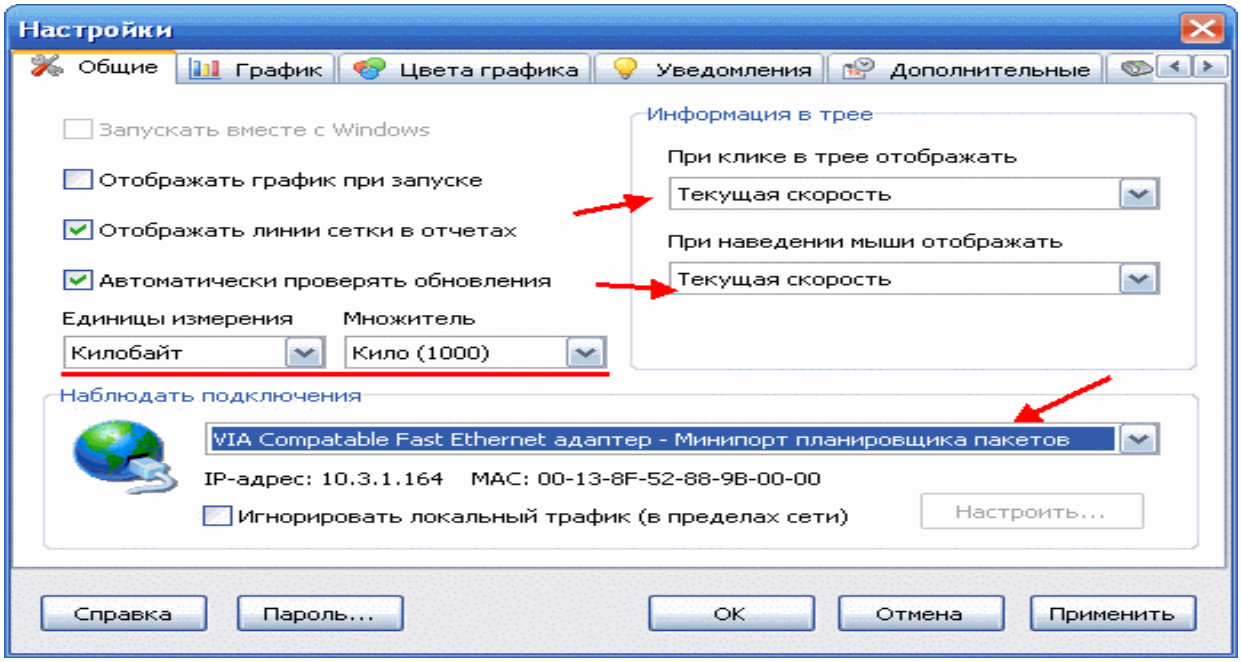


Рис. 8,б. Вікно **налаштування**, вкладка **общие**

В «Загальних» ми можемо налагодити одиниці виміру швидкості, інформацію, яка виводиться в треї, а також (найголовніше!), за яким із з'єднань вести спостереження (за замовчуванням підраховується весь трафік). Розділи «Графік» і «Кольори графіка» дозволяють нам самим налагодити зовнішній вигляд графіка вхідних/вихідних пакетів інформації. В «Повідомленнях» можна включити й налагодити сервісні повідомлення від програми, а в «Додаткових» ми маємо можливість зробити налагодження збору статистики. Сама остання вкладка – «Dial-up» – дозволяє встановити з'єднання за замовчуванням і додати додатки, які будуть запускатися разом з Networx. Після того, як Налагодження зроблені, натискаємо спочатку кнопку «**Применить**», щоб вони набули чинності, а потім «**Ok**. Монітор трафіка Тепер давайте пройдемося безпосередньо з інструментами Networx.

Перший і основний з них — монітор трафіка. Він представлений у вигляді графіка (рис. 9), який викликається кнопкою «**Показать график**».

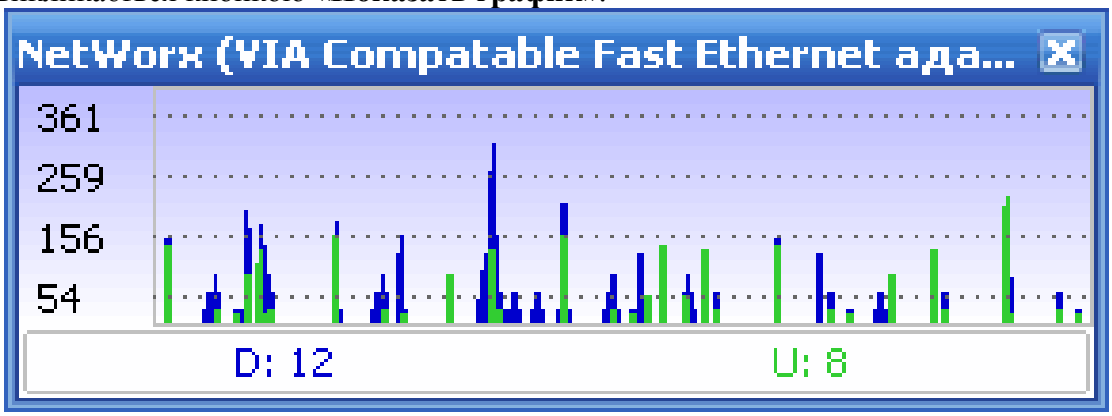


Рис. 9. Графік трафіка

Графік може представлятися у вигляді гістограми, кривих ліній або просто чисел (рис. 10). При цьому внизу завжди буде перебувати два числа. Число з індексом «D» (за замовчуванням синій колір) показує кількість вхідного трафіка (від англ. download), а «U» (зелений) відповідно вихідний (від англ. upload). Відповідними кольорами на графіку вимальовуються криві зміни швидкості, числове значення яких можна співвіднести зі шкалою ліворуч. Наступний кнопка – «**Измерение скорости**» – замірить, на жаль, не загальну швидкість Internet-підключення, а лише поточну швидкість фонової передачі пакетів. Це може знадобитися для порівняння (доступне збереження) результатів при повному навантаженні на канал.

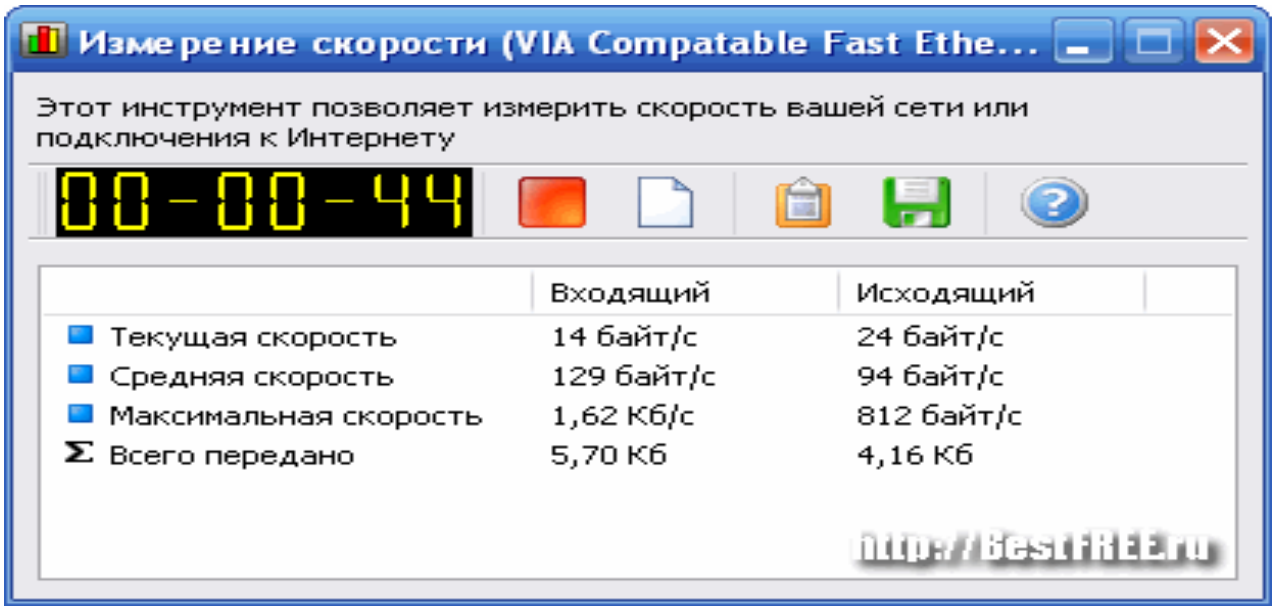


Рис. 10 Числові дані трафіка

Для запуску тесту досить нажати кнопку «**Старт**» і засікти певний проміжок часу. Потім результат можна зберегти в текстовий файл, а потім зрівняти з новими даними, отриманими при «завантаженні» каналу. Далі випливає кнопка «**Статистика**». Ця функція запускається також після подвійного клацання лівою кнопкою Миші по значкові Networx (рис. 11).

Найбільше ця функція сподобається системним адміністраторам, тому що можливо вести як загальний підрахунок трафіка, так і виводити докладну статистику за кожним з користувачів мережі. Результати можна експортувати у формат xls (електронні таблиці Excel) і зберігати на комп'ютері. Також присутні інструменти для зберігання статистики і її

подальшого відновлення (наприклад, якщо потрібно зберегти всі дані після переустановлення системи). Рухаючись далі, переходимо до розділу «Квота». Ця функція підійде найбільше користувачам з Dial-up підключенням або лімітованим трафіком (наприклад мобільний Internet). Вона дозволяє задати максимальна кількість отриманої або відправленої інформації й завжди попередить користувача про перевитрату заданого ліміту (рис. 12).

За замовчуванням квота задано в 0,00 Кб, тому якщо прагнете скористатися цією функцією, треба буде її спершу «Налагодити» (рис. 13).

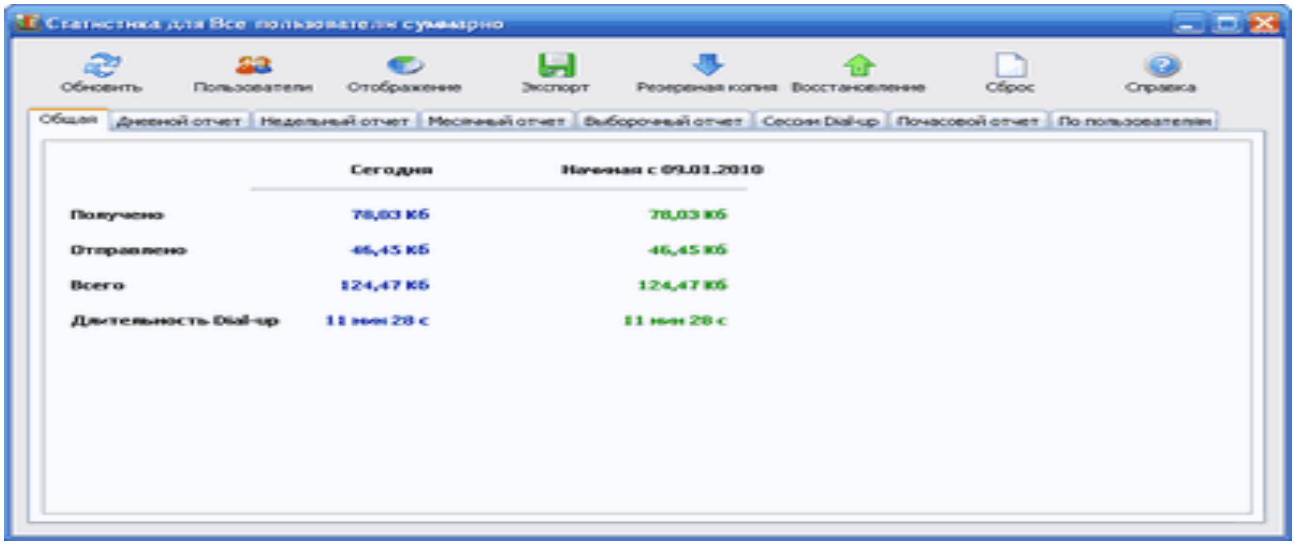


Рис. 11. Статистичні дані

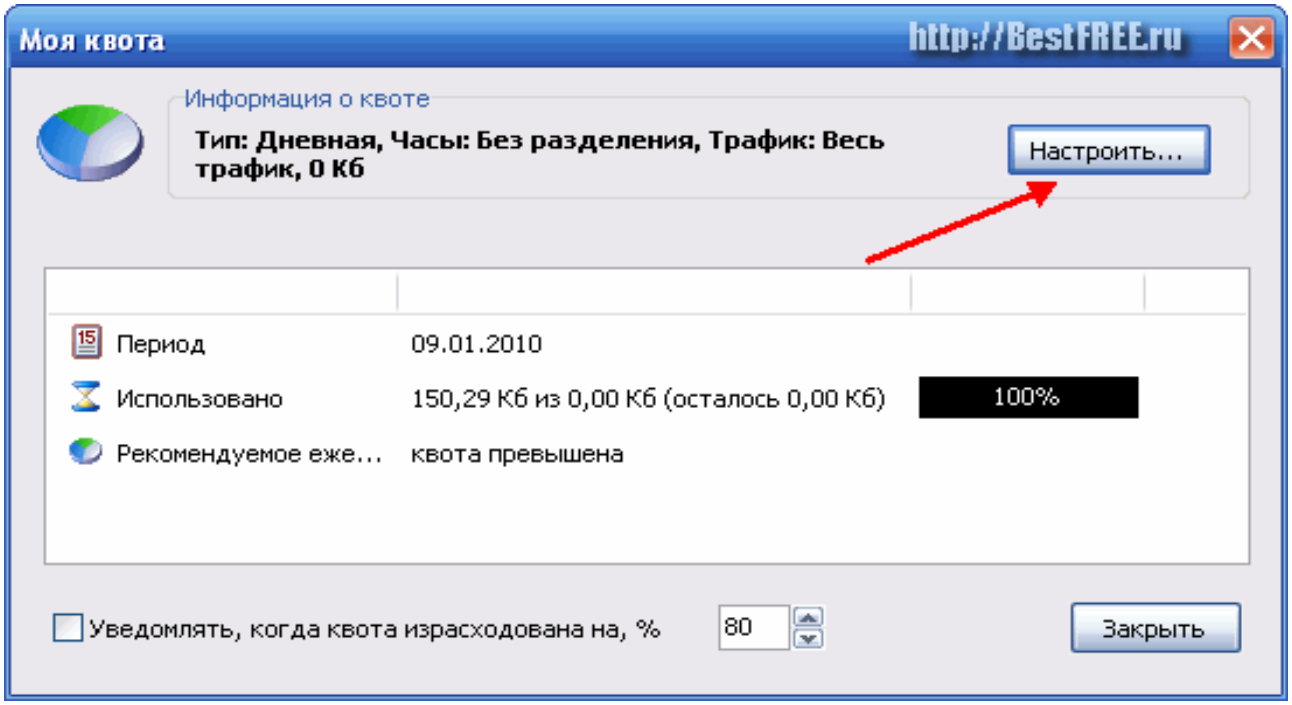


Рис. 12. Обмеження трафіку

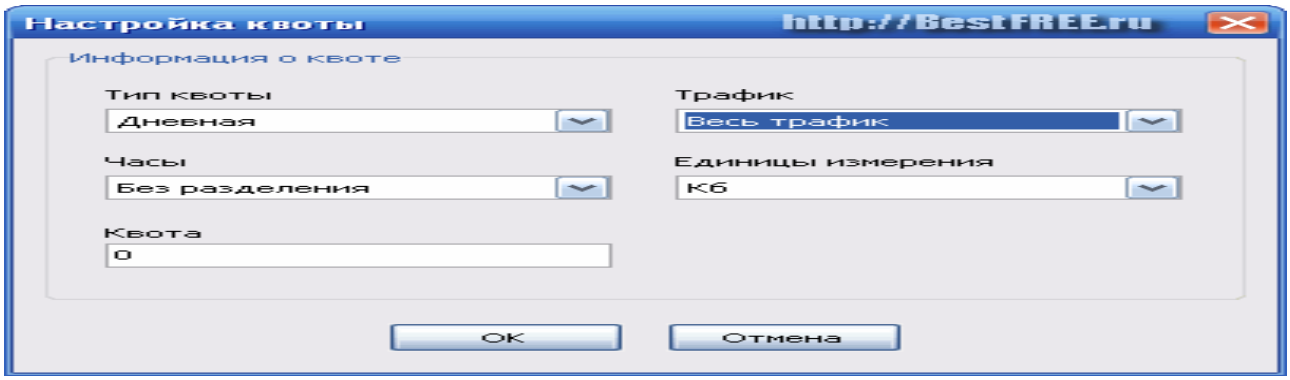


Рис. 13. Налагодження квоти

У налагодженнях вказуємо тип квоти (денна, тижнева, місячна, останні 24 години) і тип трафіка (вхідний вихідний або весь). Годинник можна залишити як є, а далі вказати одиниці виміру й властиво саму квоту. Для збереження налагодження натисніть «**Ok**», а у вікні моніторингу квоти не забудьте поставити галочку на пункт «Повідомляти, коли квота витрачена, на %», щоб вчасно одержувати інформацію про перевитрату.

Якщо раптом пропав доступ до якого-небудь Internet-ресурсу або треба довідатися, який шлях Ви проходите, перш ніж потрапите на той або інший сайт, спробуйте зробити трасування даного шляху. Це можна зробити й штатними можливостями Windows, однак з Networx виходить набагато простіше й наочніше (рис. 14).

Для початку трасування введіть ім'я сайту (комп'ютера) або його Ip-Адресу. Тепер можна задати час очікування відповіді (хоча найчастіше стандартного значення цілком достатньо) і можна натискати «**Старт**».

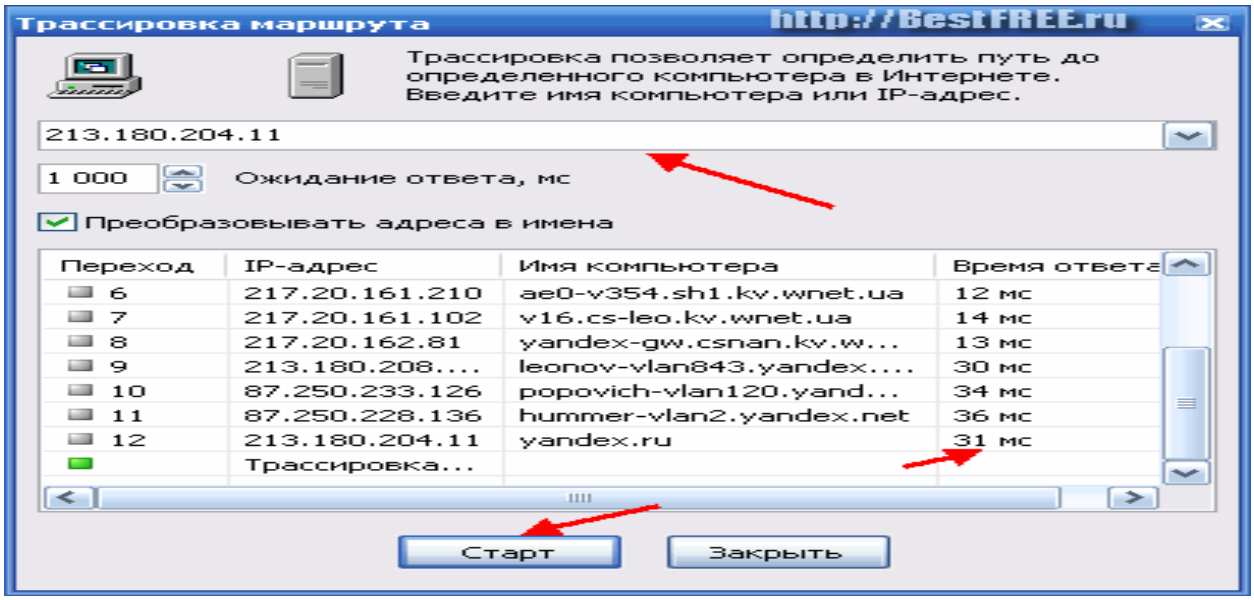


Рис. 14. Трасування маршруту

2. Хід роботи

Знайти дві довільні програми (лічильники трафіку), установити їх на комп’ютері, провести налагодження програм та трафіку мережі. Провести трасування сайтів, які переглядалися під час виконання роботи. Звіт представити у вигляді таблиці та зробити висновки.

Таблиця для звіту за лабораторною роботою.

Назва програми тестування трафіку		
Результати трасування сайтів		
IP адреса сайту		
IP адреса сайту		
Швидкість передачі даних		
Швидкість приймання даних		
Загальна швидкість		
Максимальна швидкість передачі даних		
Максимальна швидкість приймання даних		
Всього байт відправлено		
Всього байт отримано		
Всього байт відправлено і отримано		
Швидкість підключення		
Середня швидкість передачі даних		
Середня швидкість приймання даних		
Локальна IP адреса комп'ютера		
IP адреса сайту		

3. Контрольні питання

1. Поняття трафіку мереж.
2. Для чого необхідний контроль трафіку різним групам користувачів?
3. Програми лічильники трафіку, їх можливості.
4. Як встановити програми лічильники трафіку?
5. Які результати контролю трафіку можна отримати?
6. Як підібрати програми контролю трафіку для різних груп користувачів?

ЛАБОРАТОРНА РОБОТА 30.
УСТАНОВЛЕННЯ MICROSOFT OFFICE 2016 ЗА ГЛОБАЛЬНОЮ МЕРЕЖЕЮ

Мета роботи: отримати практичні павички в установленні Microsoft Office 2016 за глобальною мережею

Зміст

1. Хід роботи
1.1. Закачування установочних файлів
1.2. Встановлення компонентів Microsoft Office 2016
1.3. Перевірка працездатності компонентів Microsoft Office 2016
1.4. Активування компонентів
2. Контрольні питання

1. Хід роботи

1.1. Закачування установочних файлів

1. В мережі Internet знаходимо установочний файл для закачування, наприклад, на сайті ycutube.com (рис. 1).

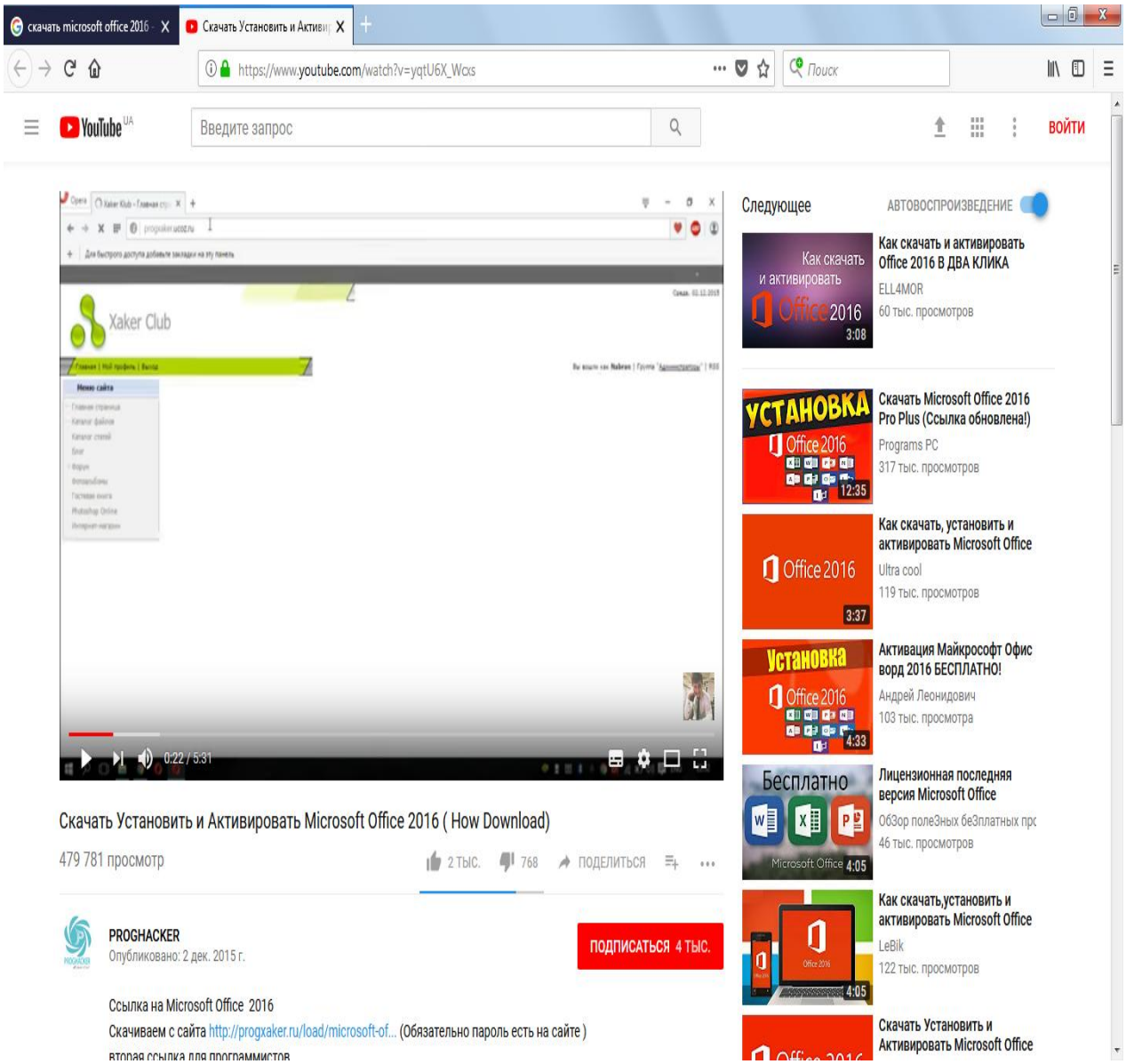


Рис. 1. Сайт для скачування файлів установки

2. Входимо до каталогу Microsoft Office 2016 (рис. 2).

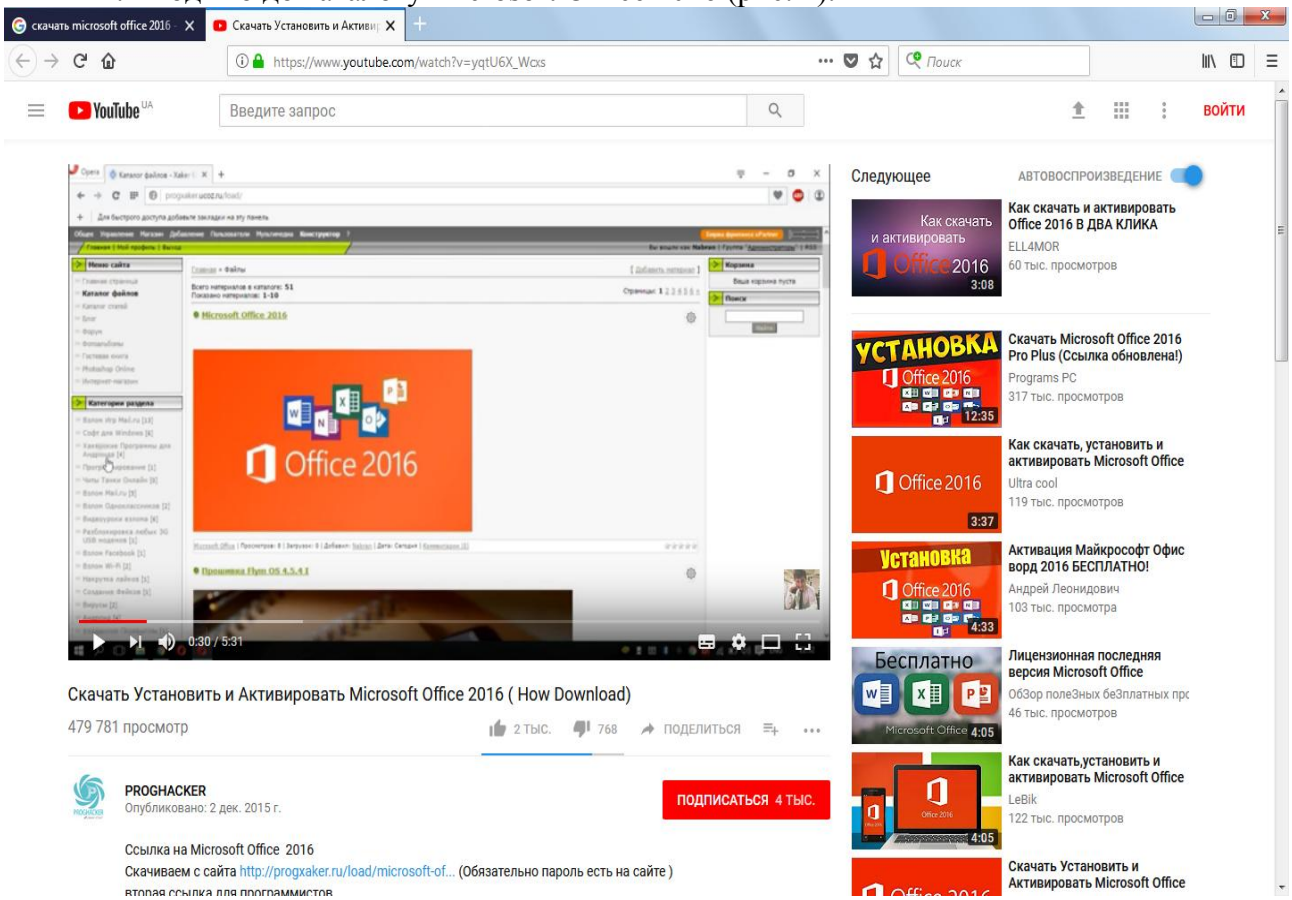


Рис. 2. Каталог Microsoft Office 2016

3. Входимо до розділу категорії (рис. 3).

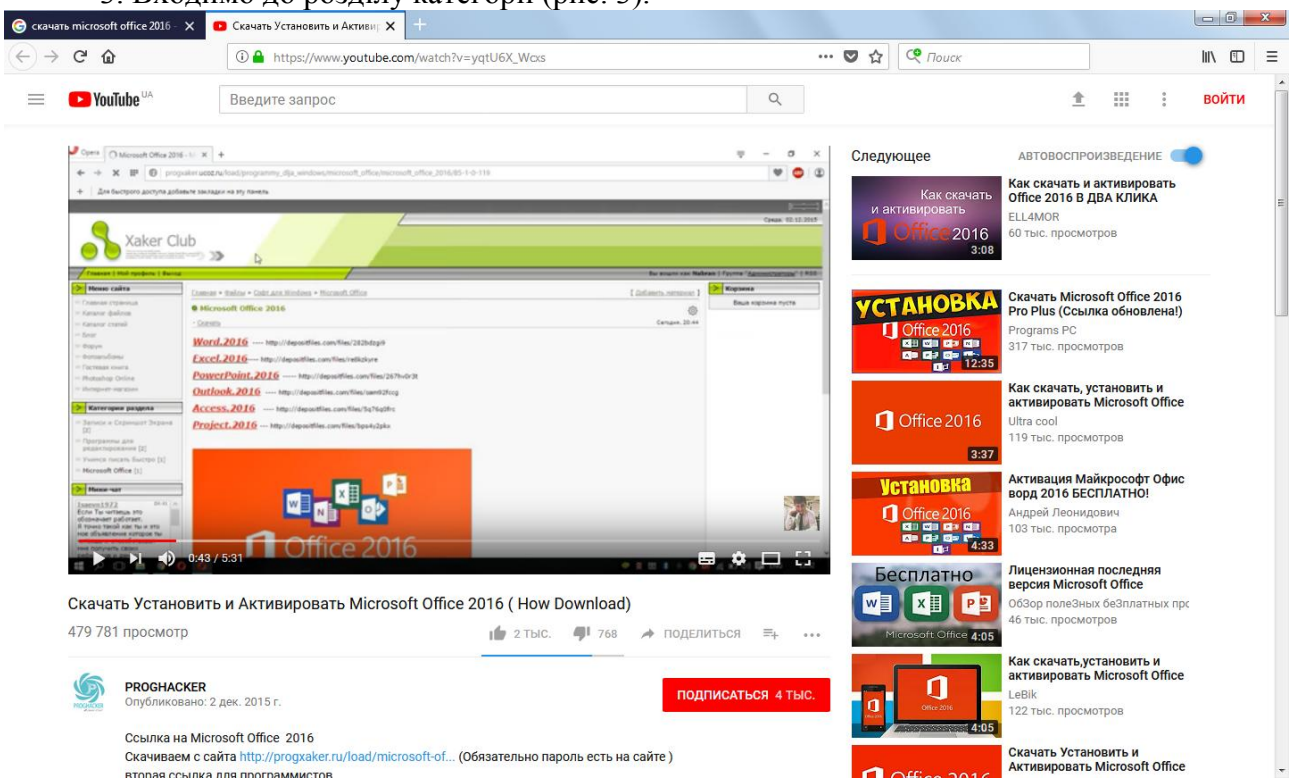


Рис. 3. Розділ категорія

4. Копіюємо почергово посилання біля компонентів Microsoft Office 2016 (рис. 4), наприклад, біля Word 2016.

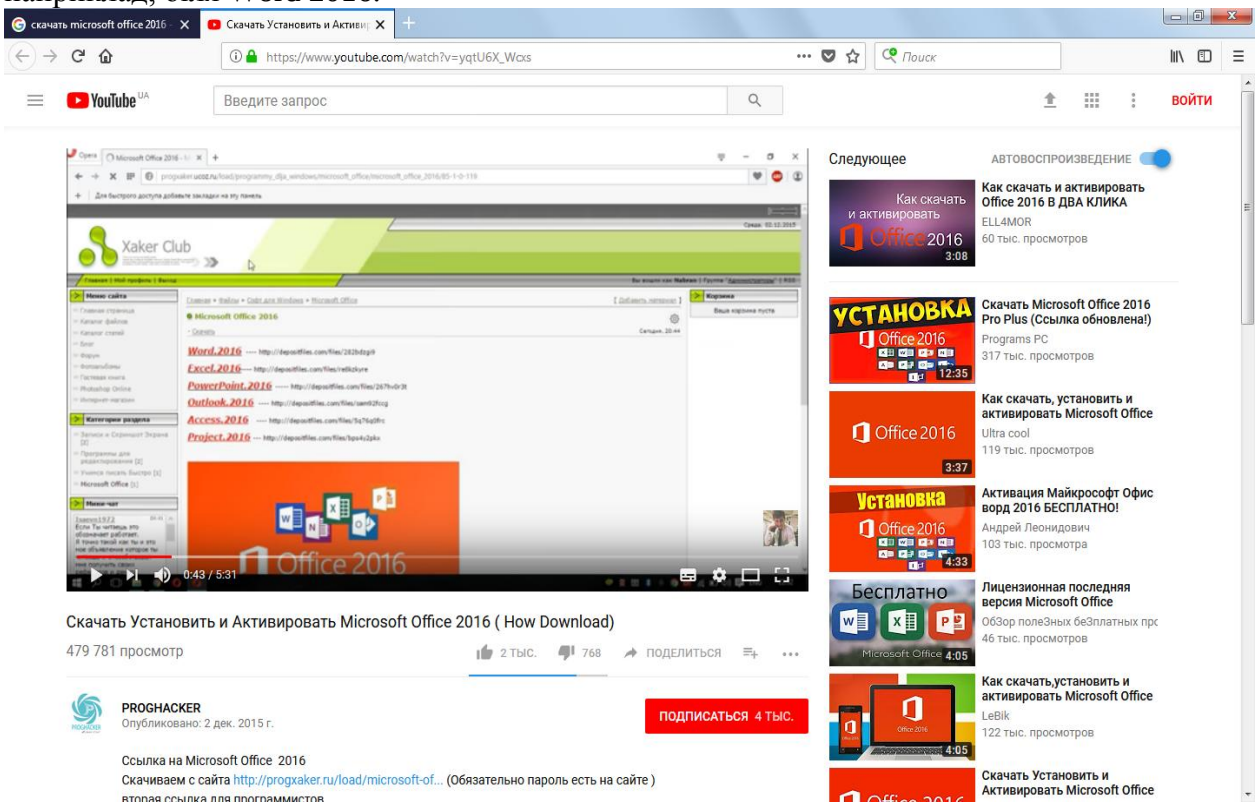


Рис. 4. Копіювання посилання біля компонентів Microsoft Office 2016

5. Вставляємо почергово посилання в адресний рядок, натискуємо **Enter,** та переходимо почергово до скачування файлів рис. 5 - 7. Відбувається закачування тільки частини файлів, інша більша частина для установки компонента закачується за глобальною мережею після активації установки компонента-програми.

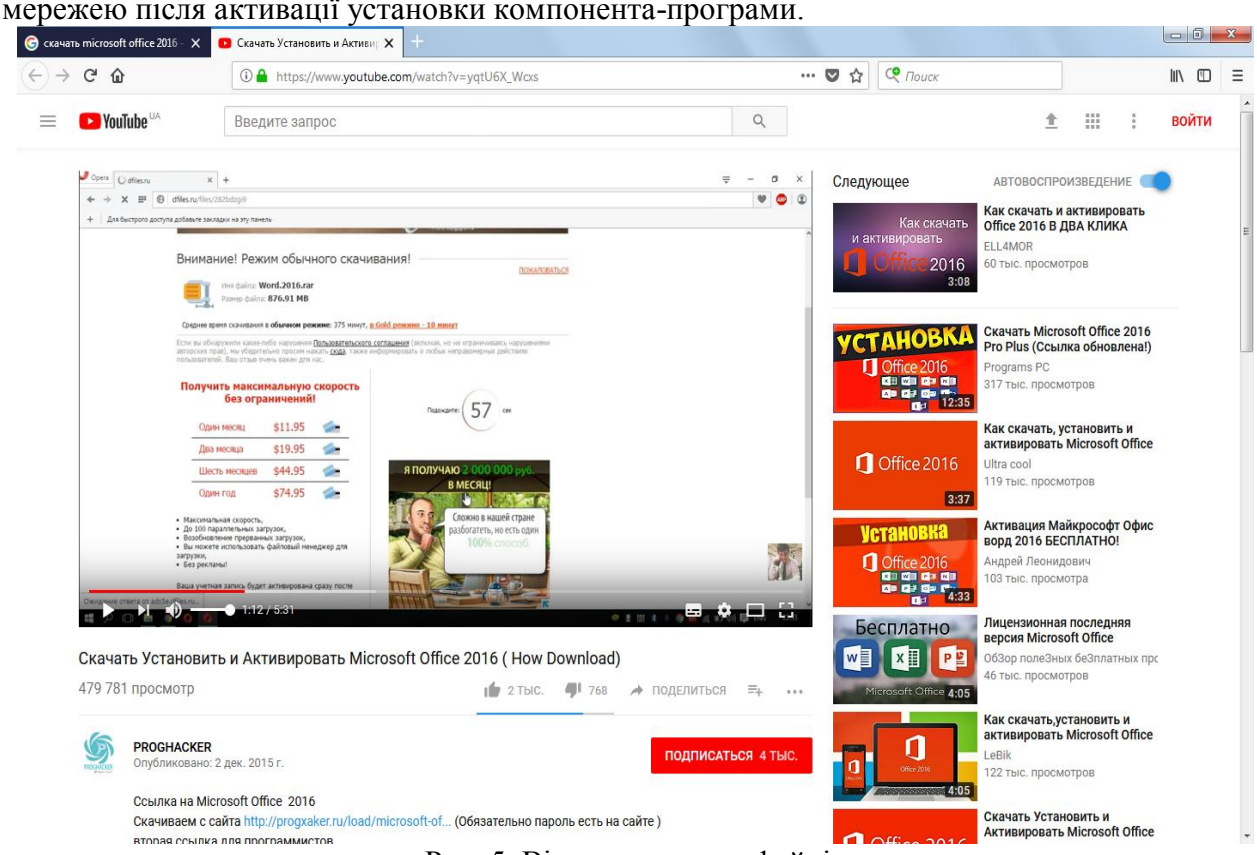


Рис. 5. Віко скачування файлів

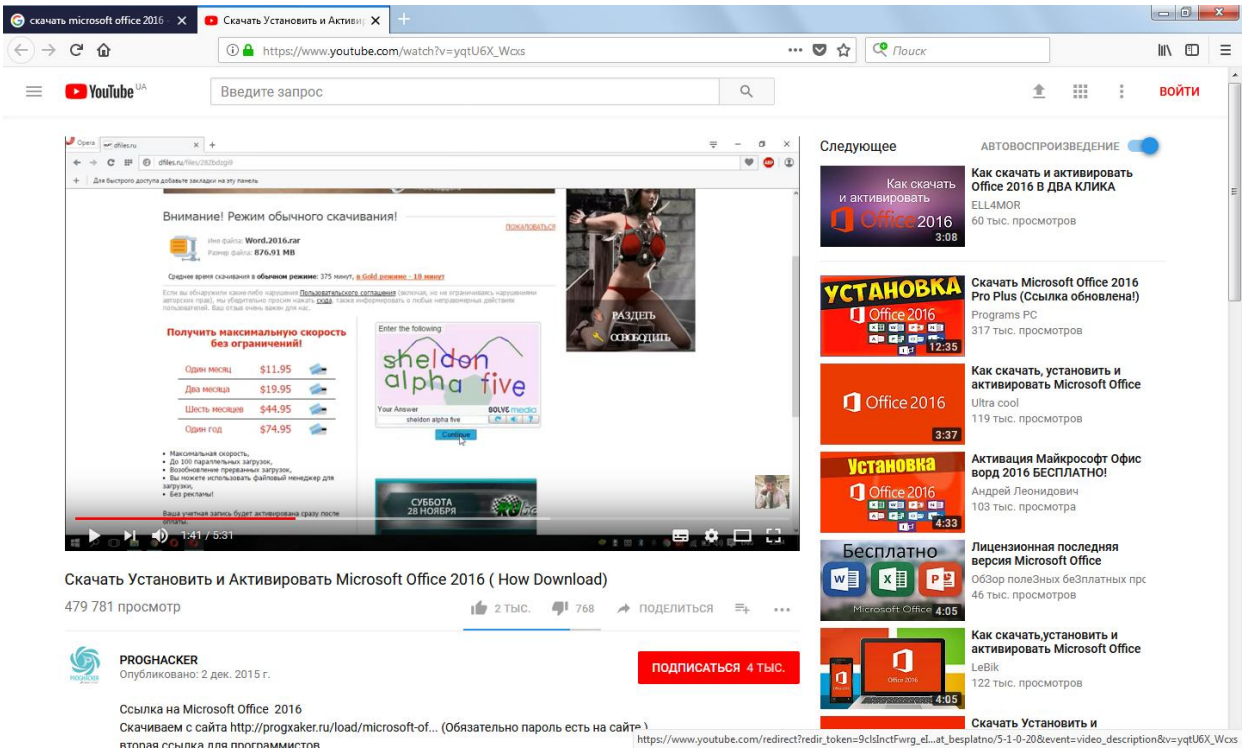


Рис. 6. Заповнення поля запиту

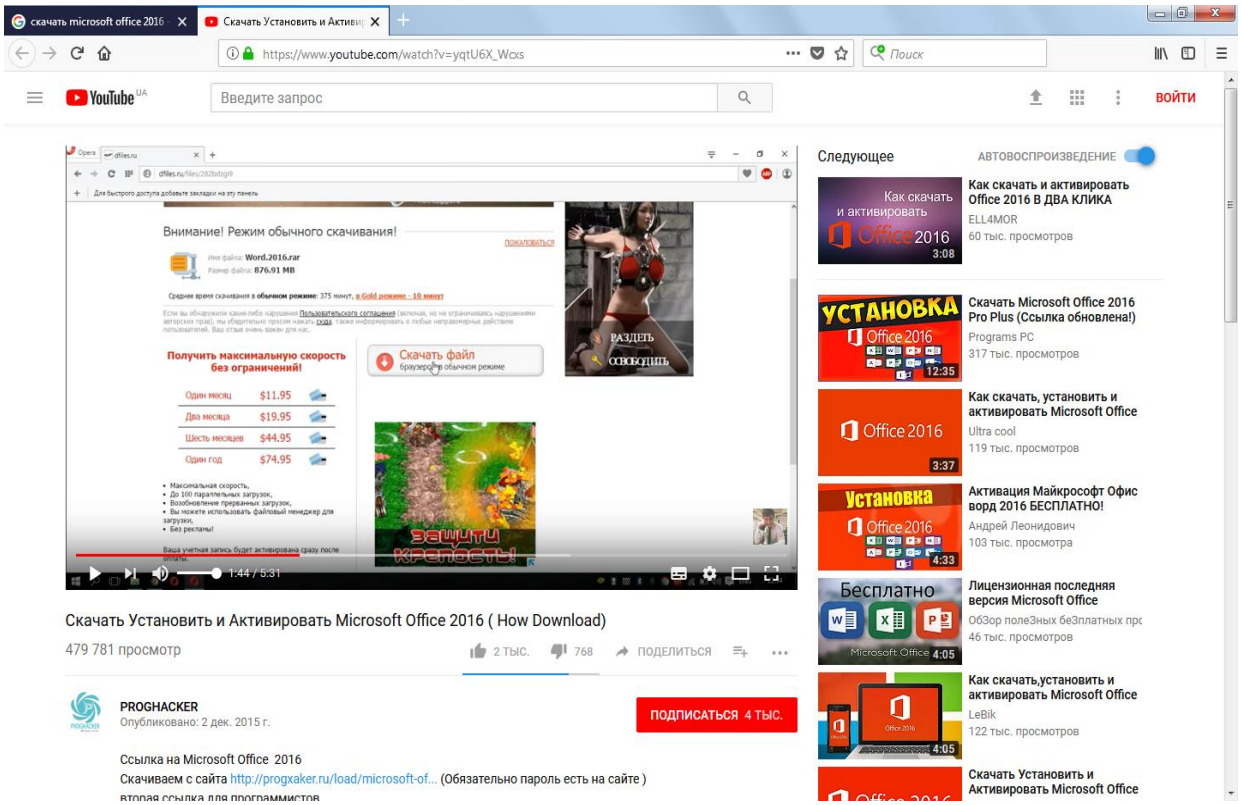


Рис. 7. Скачування файлів

1.2. Встановлення компонентів Microsoft Office 2016

6. Після закінчення закачування компонентів файлів починаємо активізацію установлення кожного компонента окремо, почергово (рис. 8). Для чого проводимо клацання лівою клавішею маніпулятора типу «миш» по одному з файлів установки та проводимо встановлення компонентів (рис. 9). Далі проводимо вібір розрядності Microsoft Office 2016 (рис. 10) в залежності від встановленої операційної системи. Та закінчуємо встановлення програми (рис. 11).

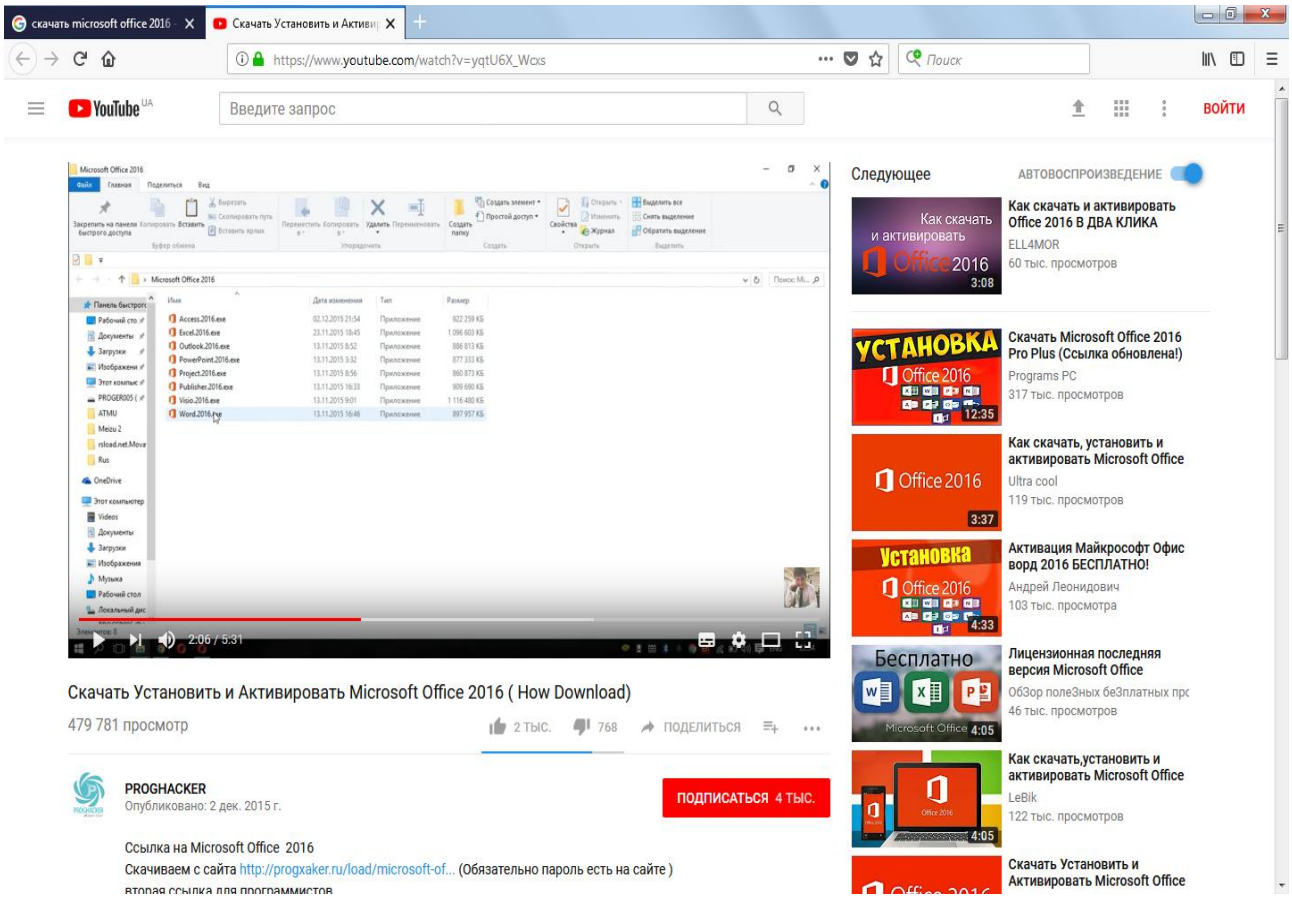


Рис. 8. Запуск файлу на виконання

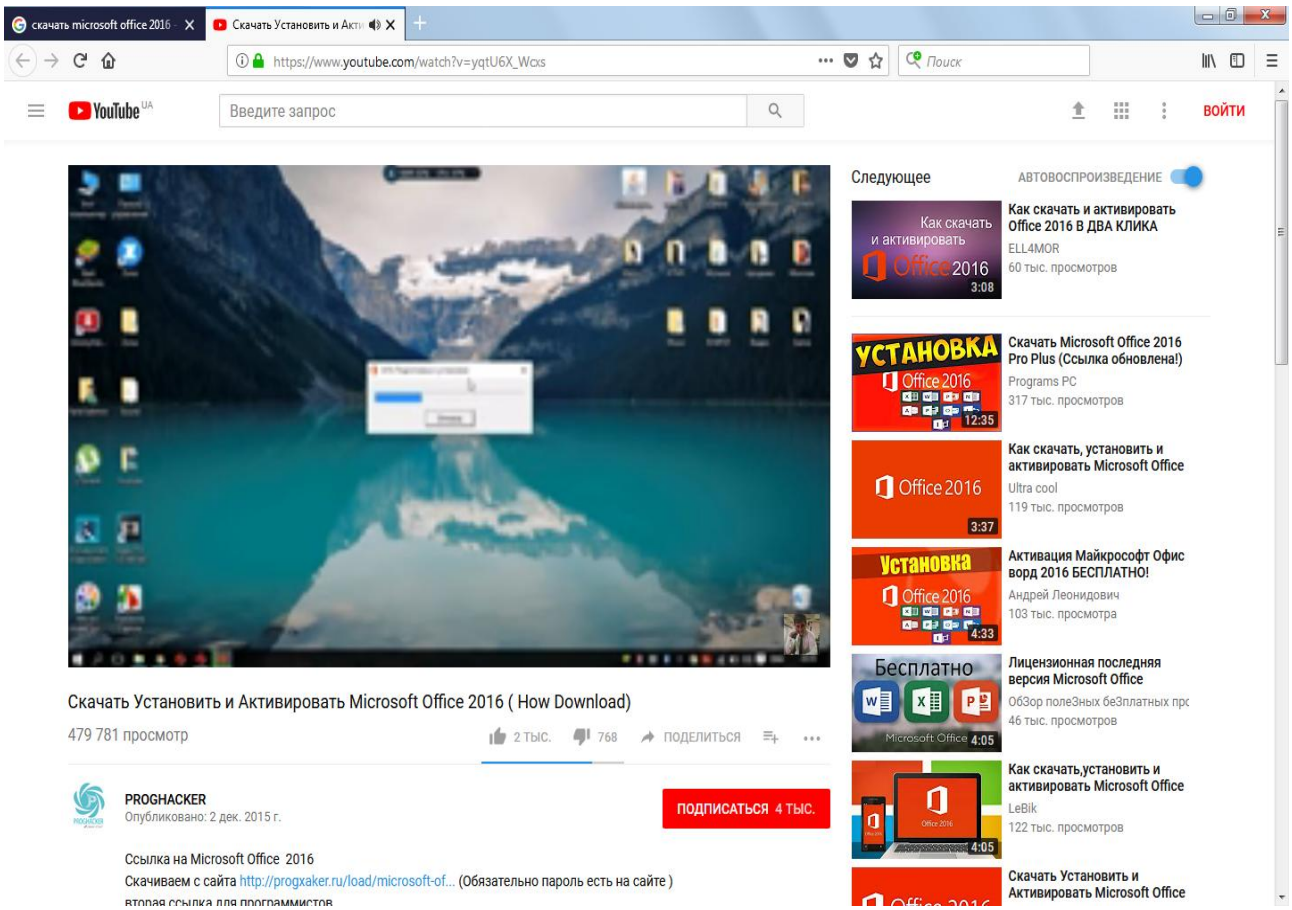


Рис. 9. Процес установки програми та закачування файлів за глобальною мережею

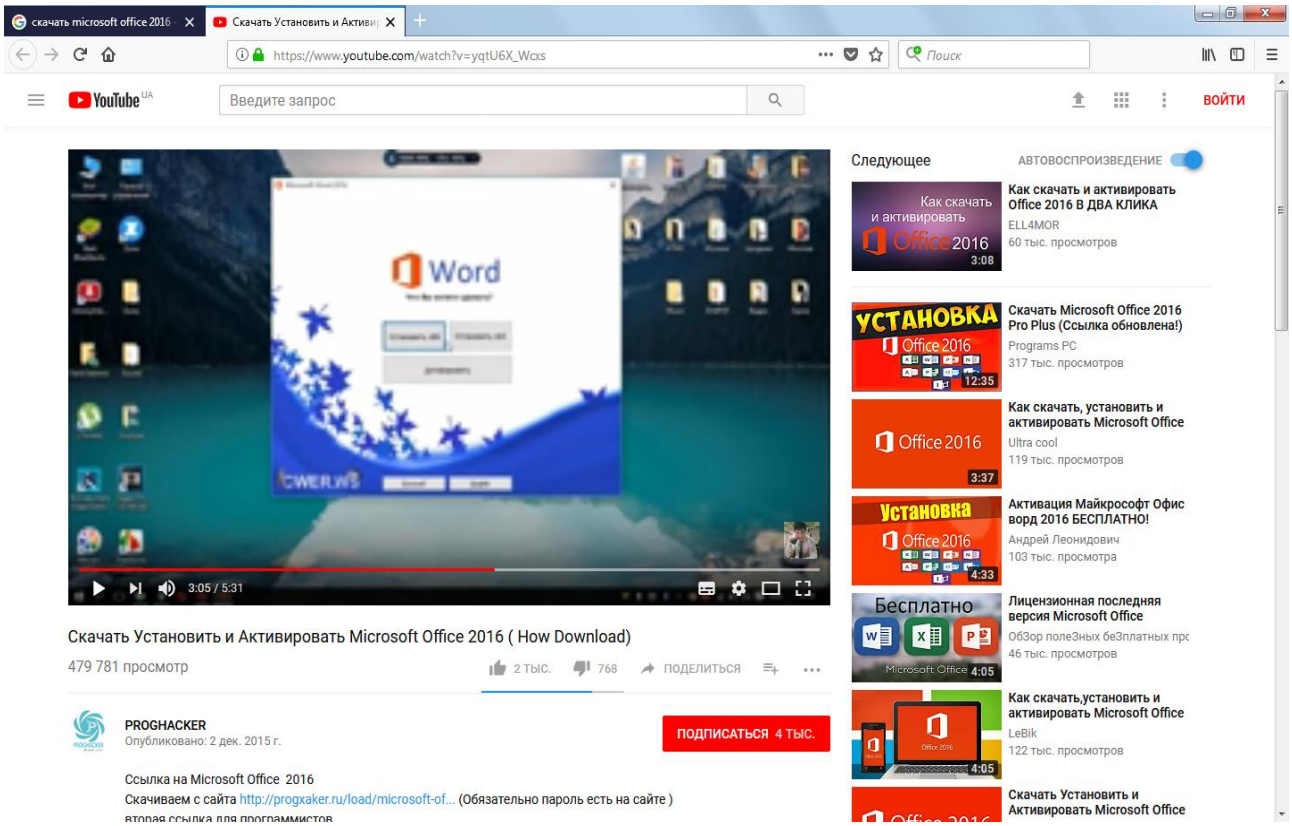


Рис. 10. Закінчення установки програми, вибір розрядності офісу

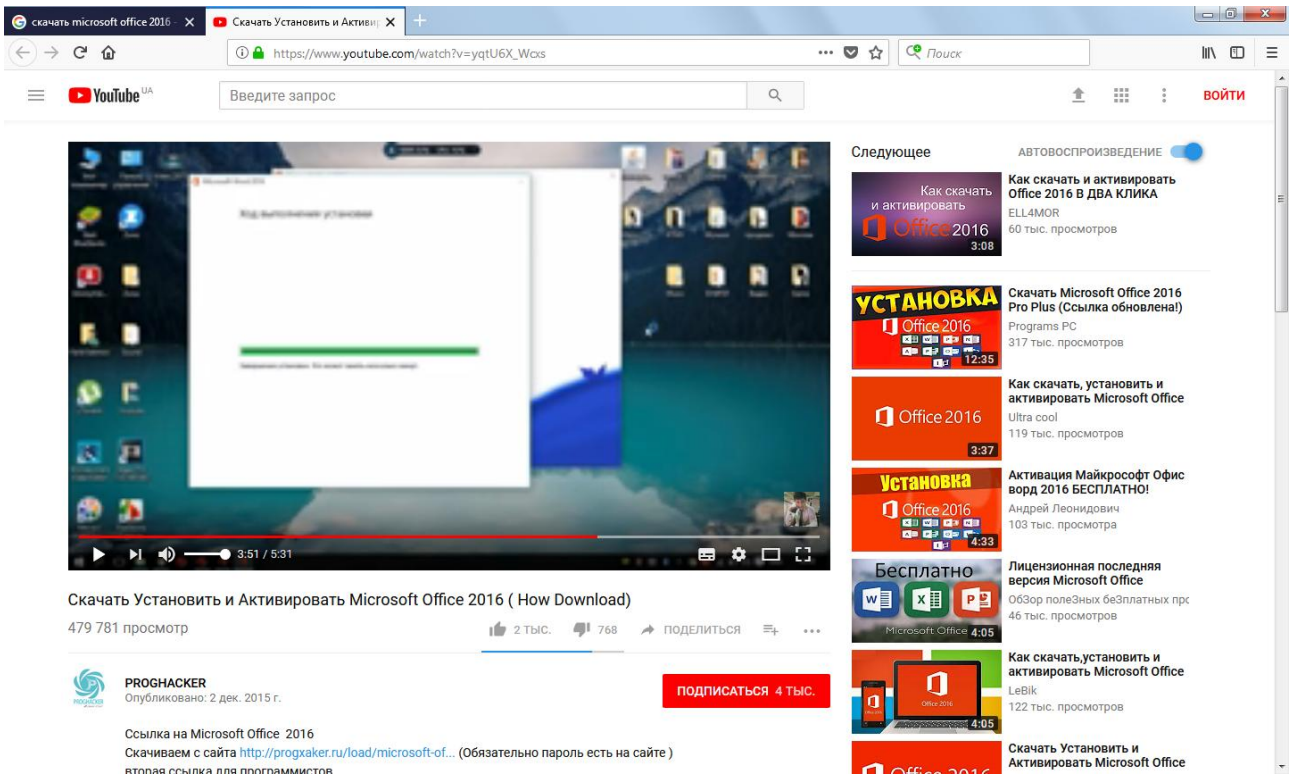


Рис. 11. Закінчення установлення програми

1.3. Перевірка працездатності компонентів Microsoft Office 2016

7. Почергово відкриваємо програми-компоненти (рис. 12 – 16). Після відкриття вікна відмовляємося від активації програми (рис. 17).

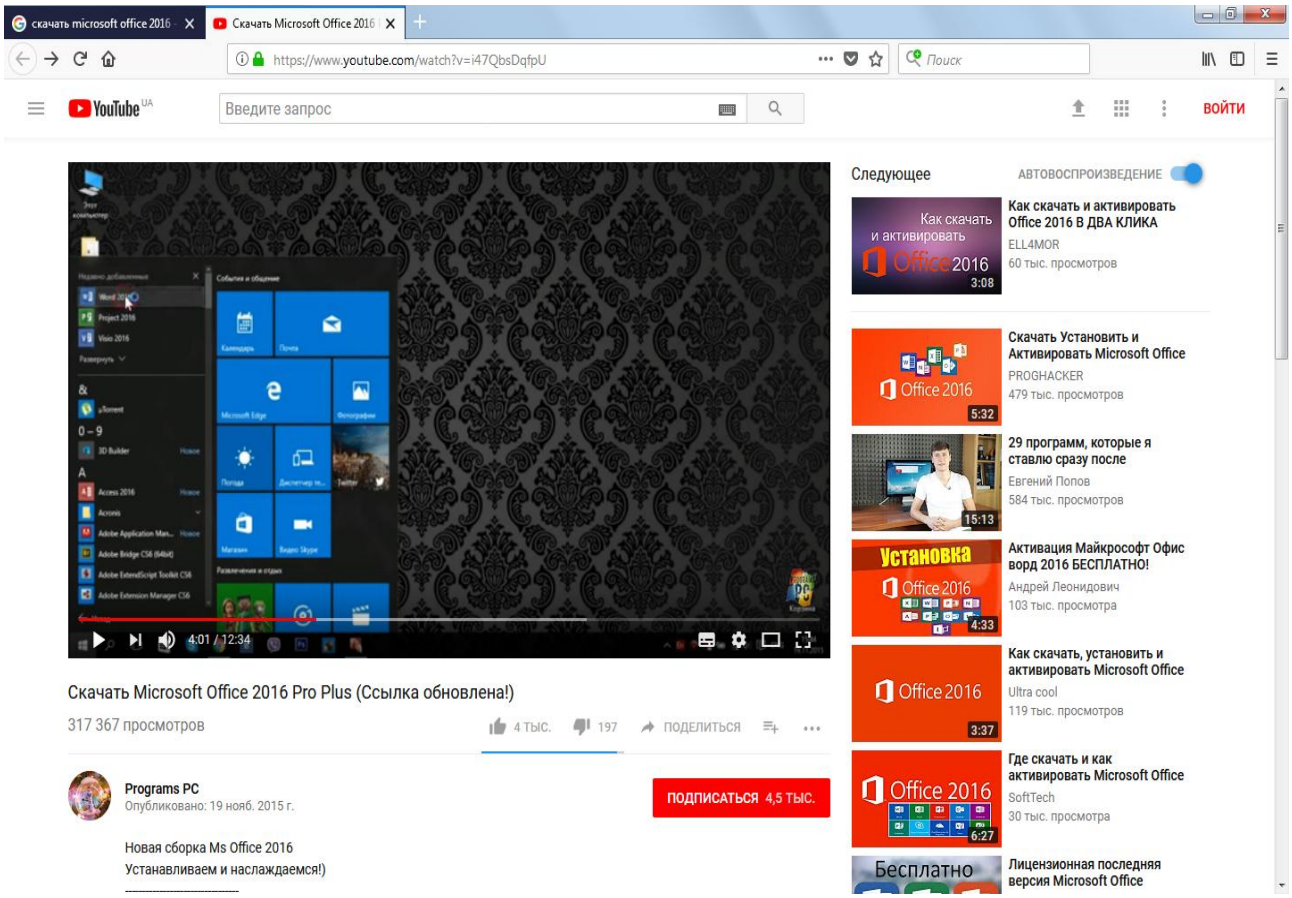


Рис. 12. Запускаємо Word

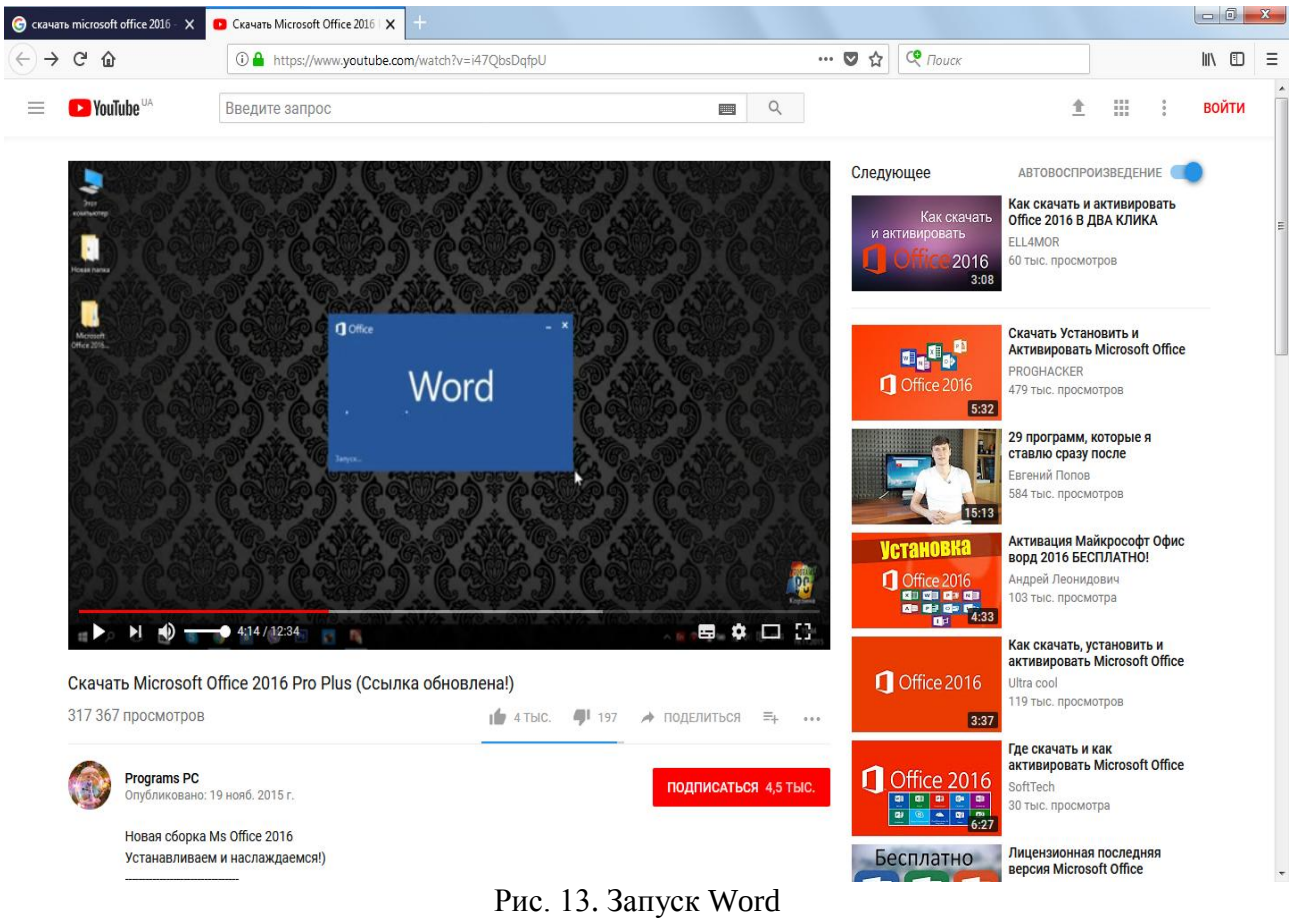


Рис. 13. Запуск Word

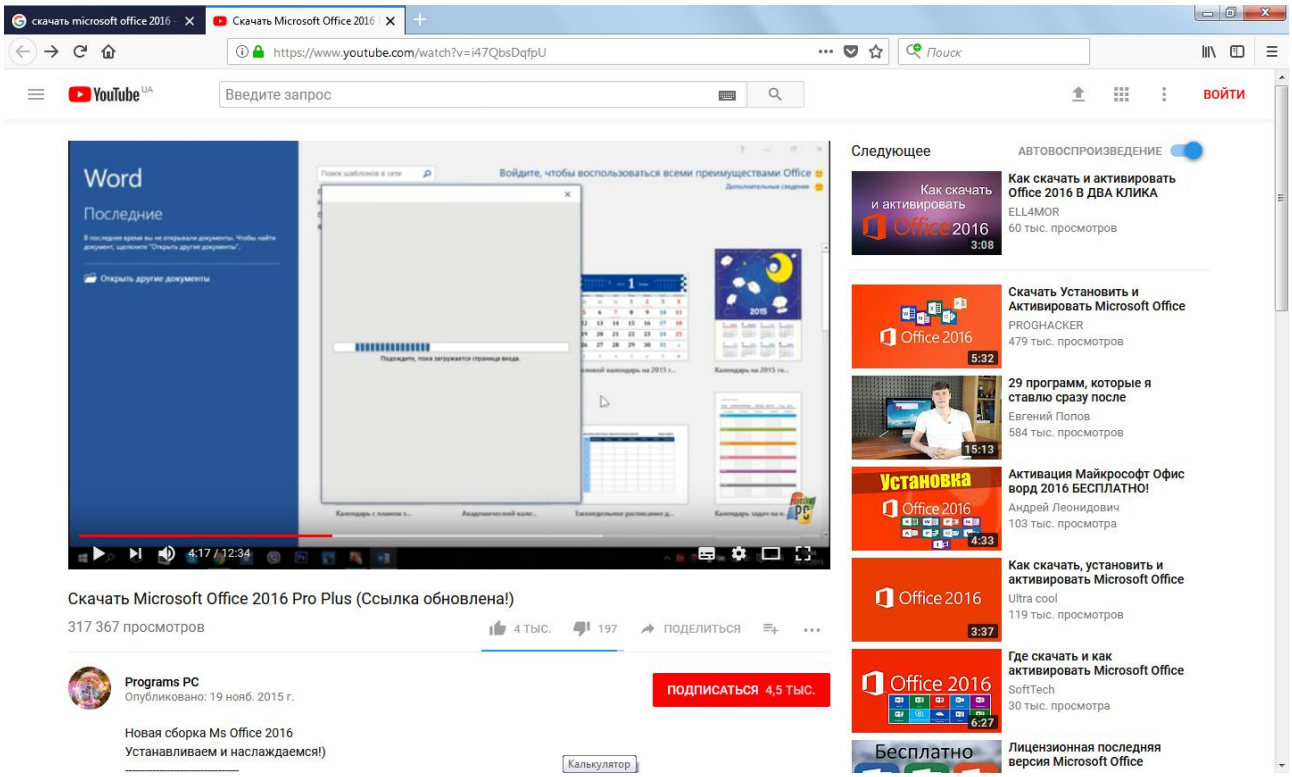


Рис. 14. Відкриття вікна Word

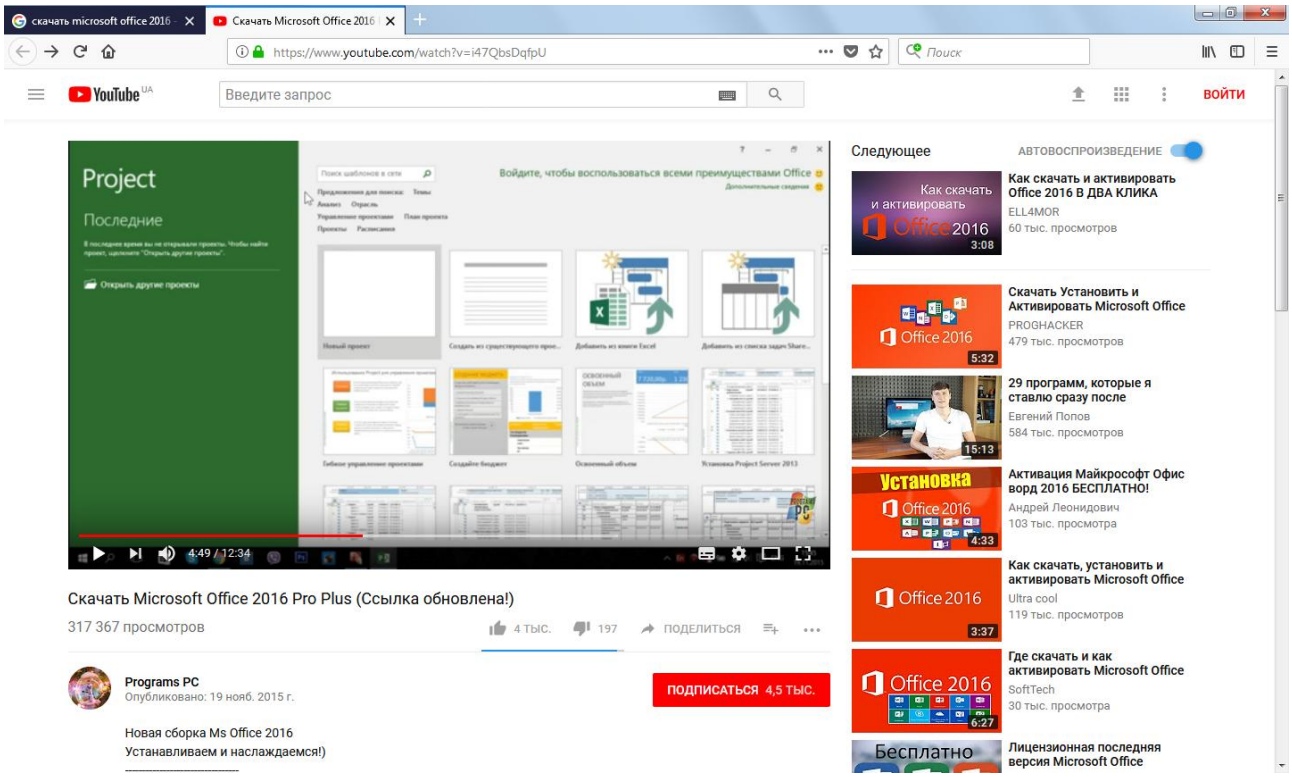


Рис. 15. Аналогічно вікно Project

1.4. Активування компонентів

Запускаємо файл активації програм (рис. 16-25).

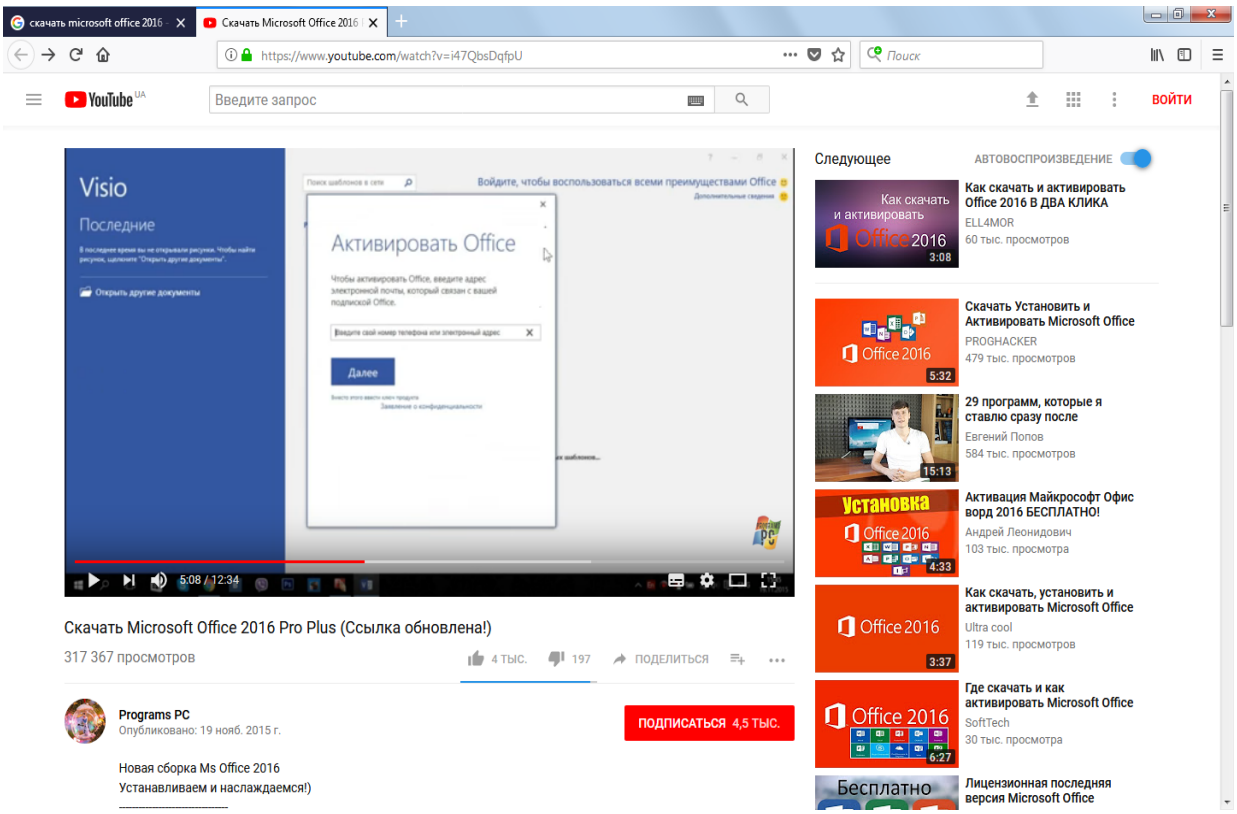


Рис. 16. Вікно активації для вказаних програм

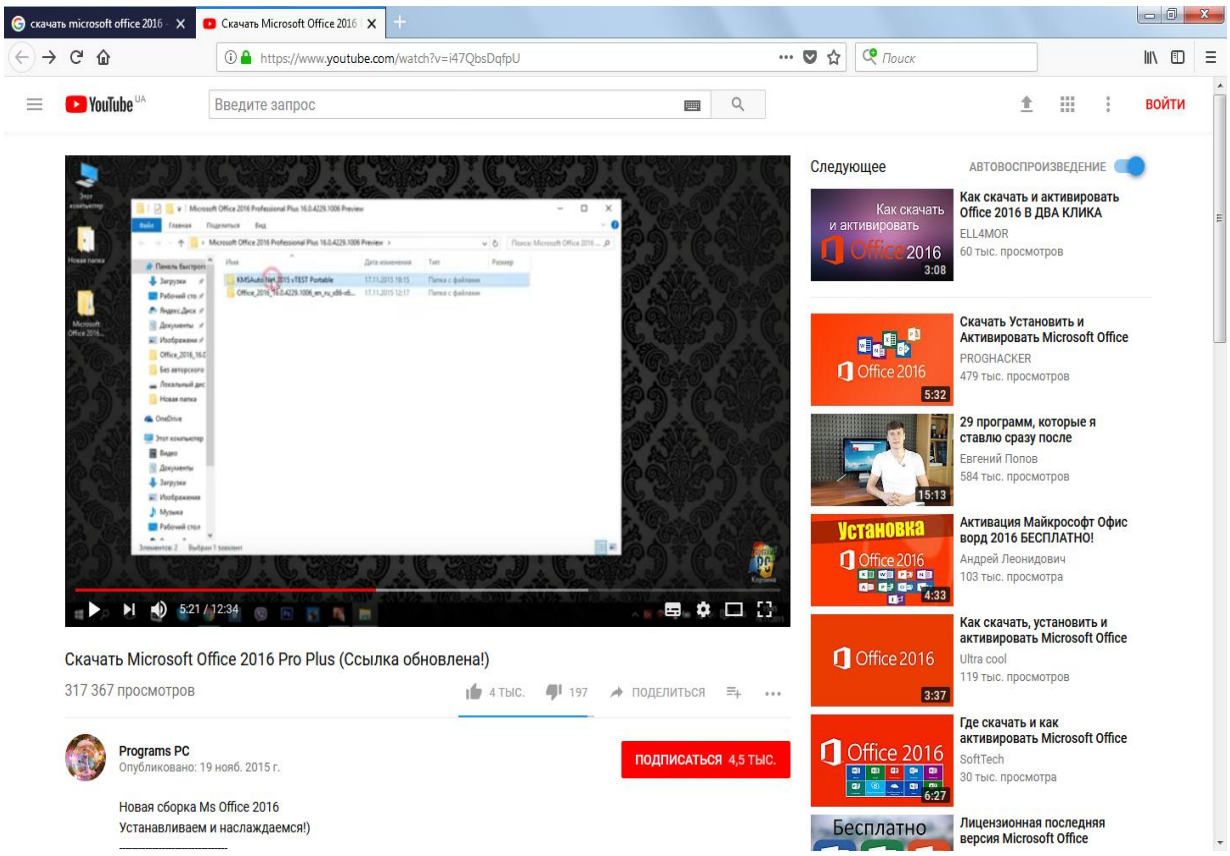


Рис. 17. Запуск другого каталогу для активації програм

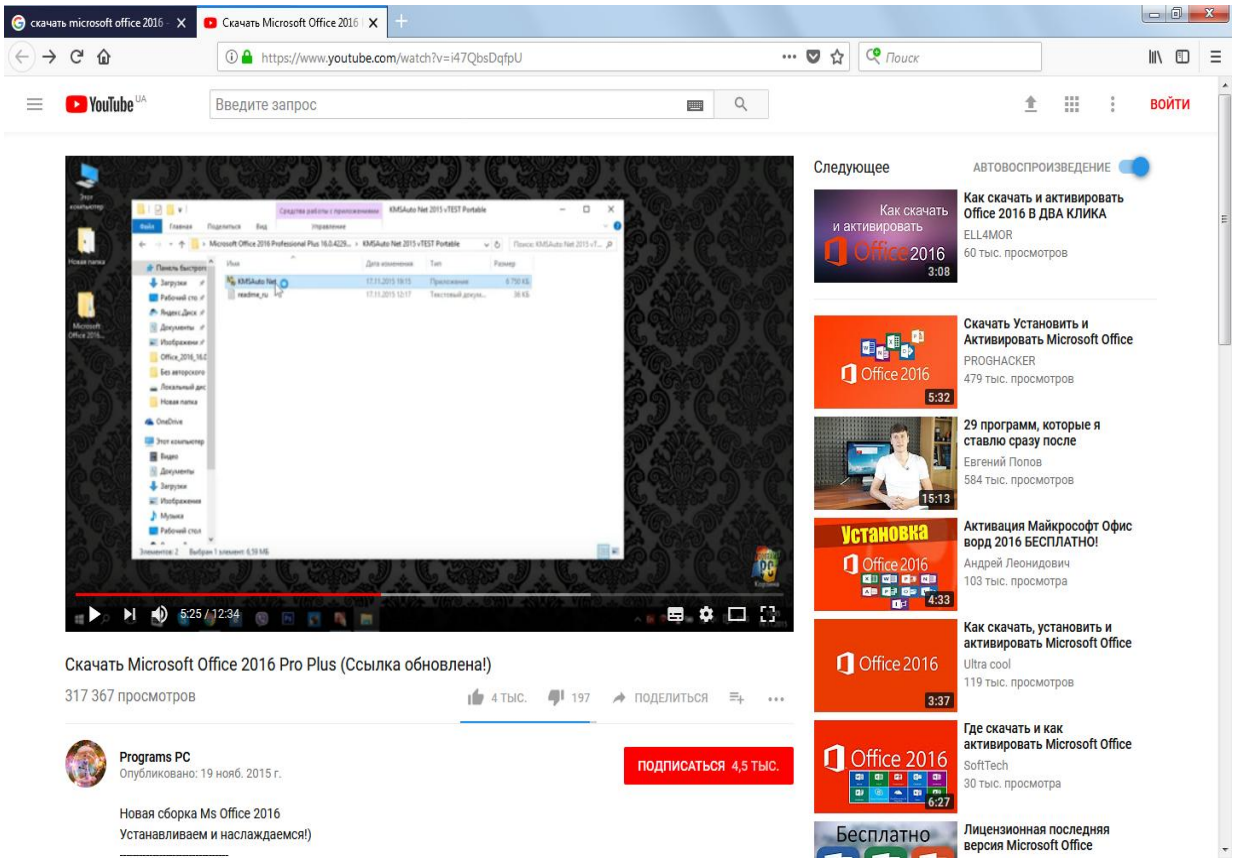


Рис. 18. Запуск на виконання файлу активації

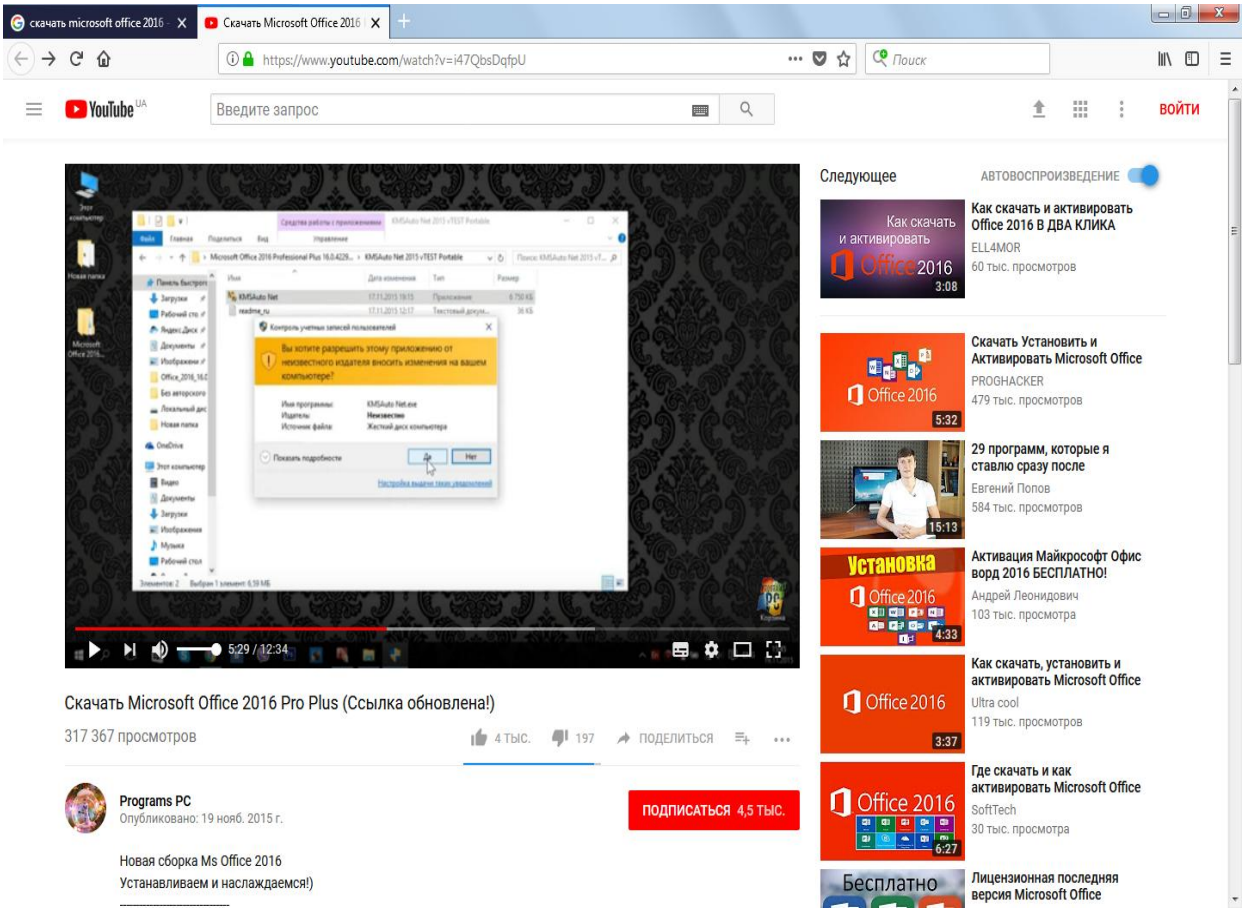


Рис. 19. Вікно запиту на активацію

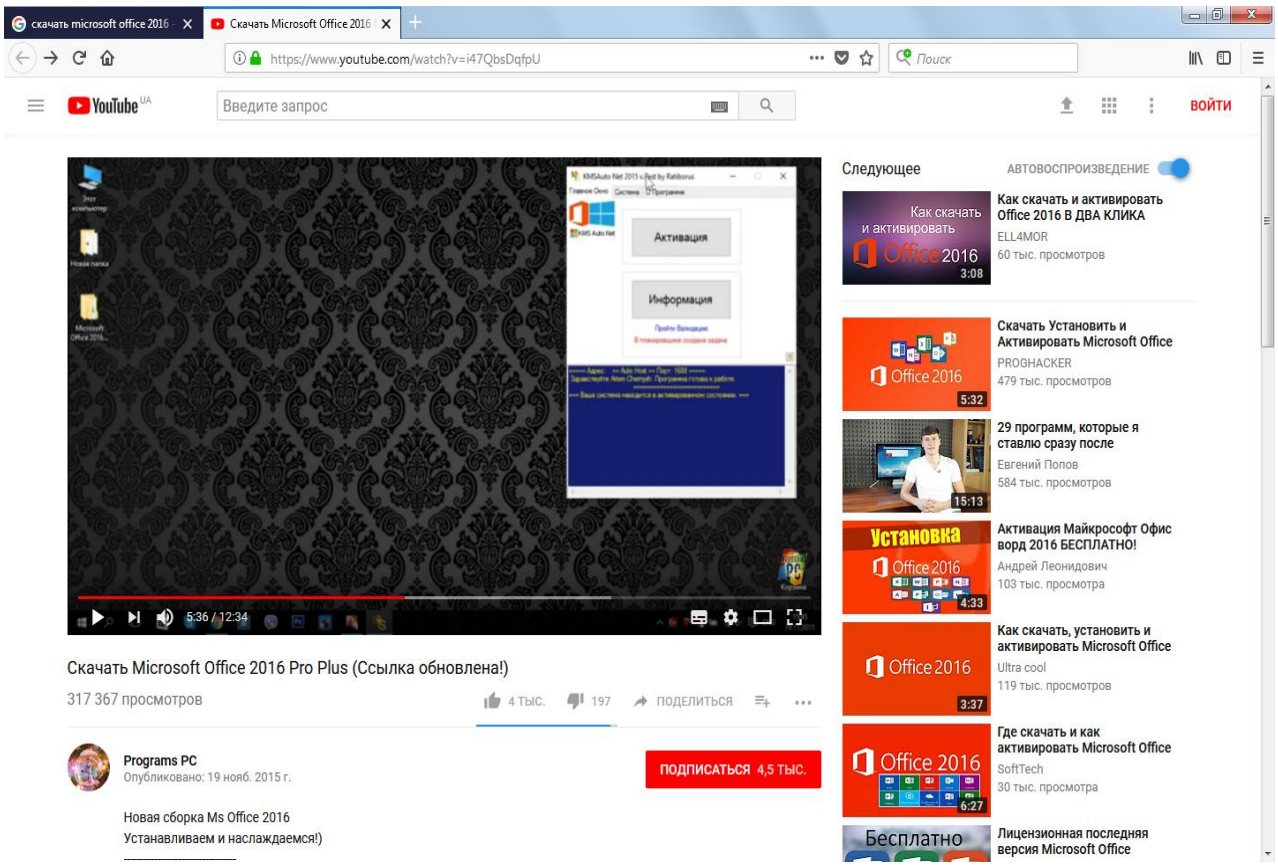


Рис. 20. Вікно активації

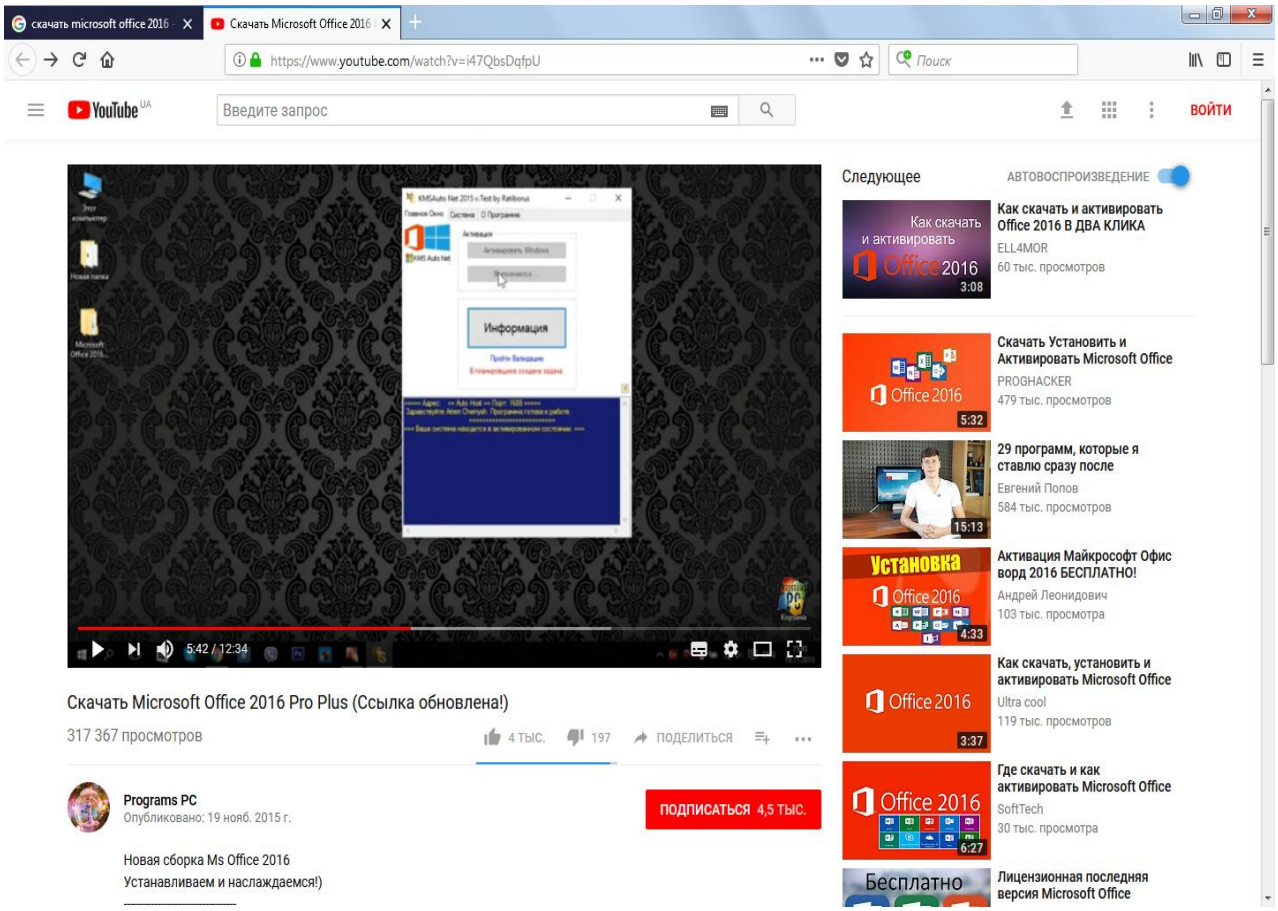


Рис. 21. Вікно виконання активації

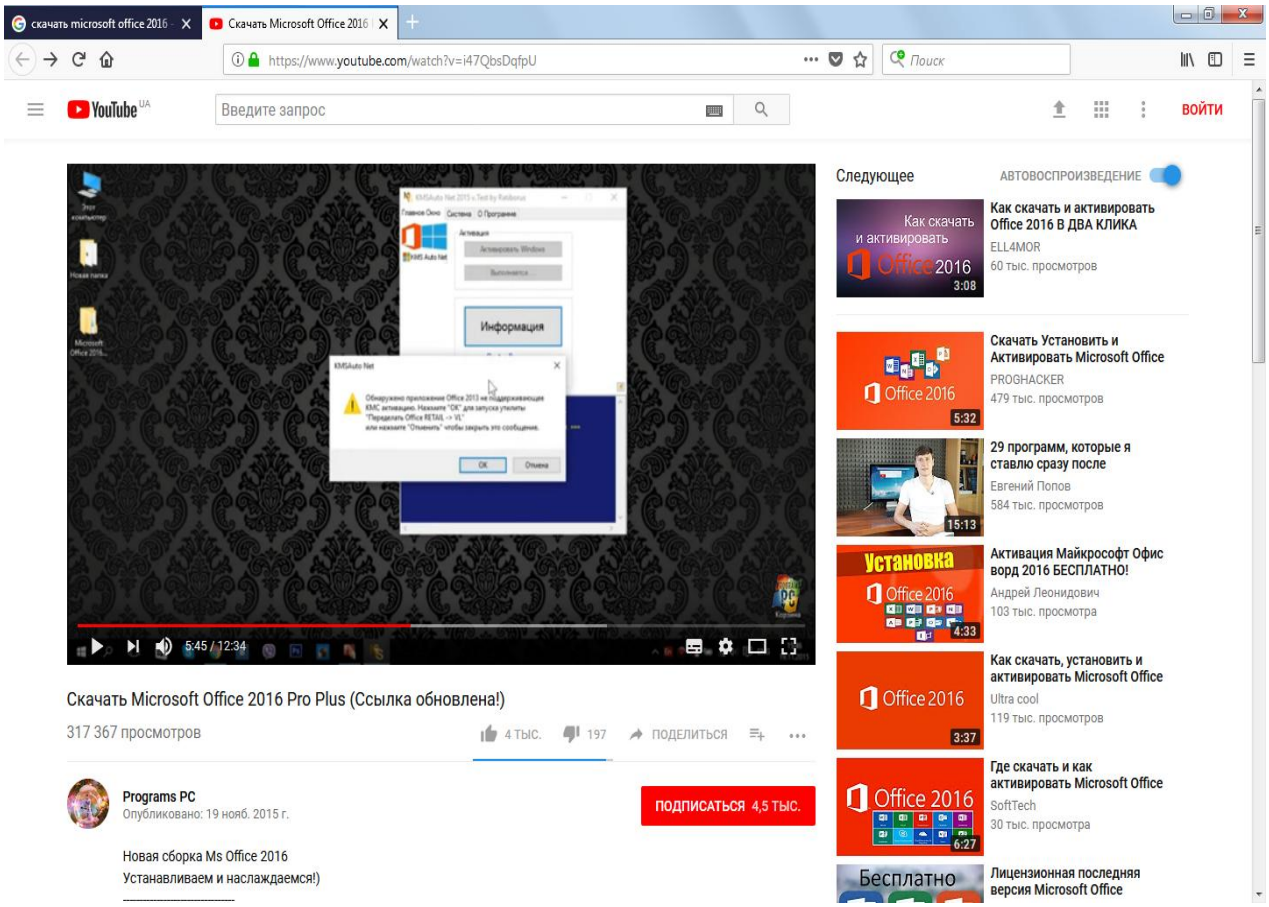


Рис. 22. Запуск утиліти активації

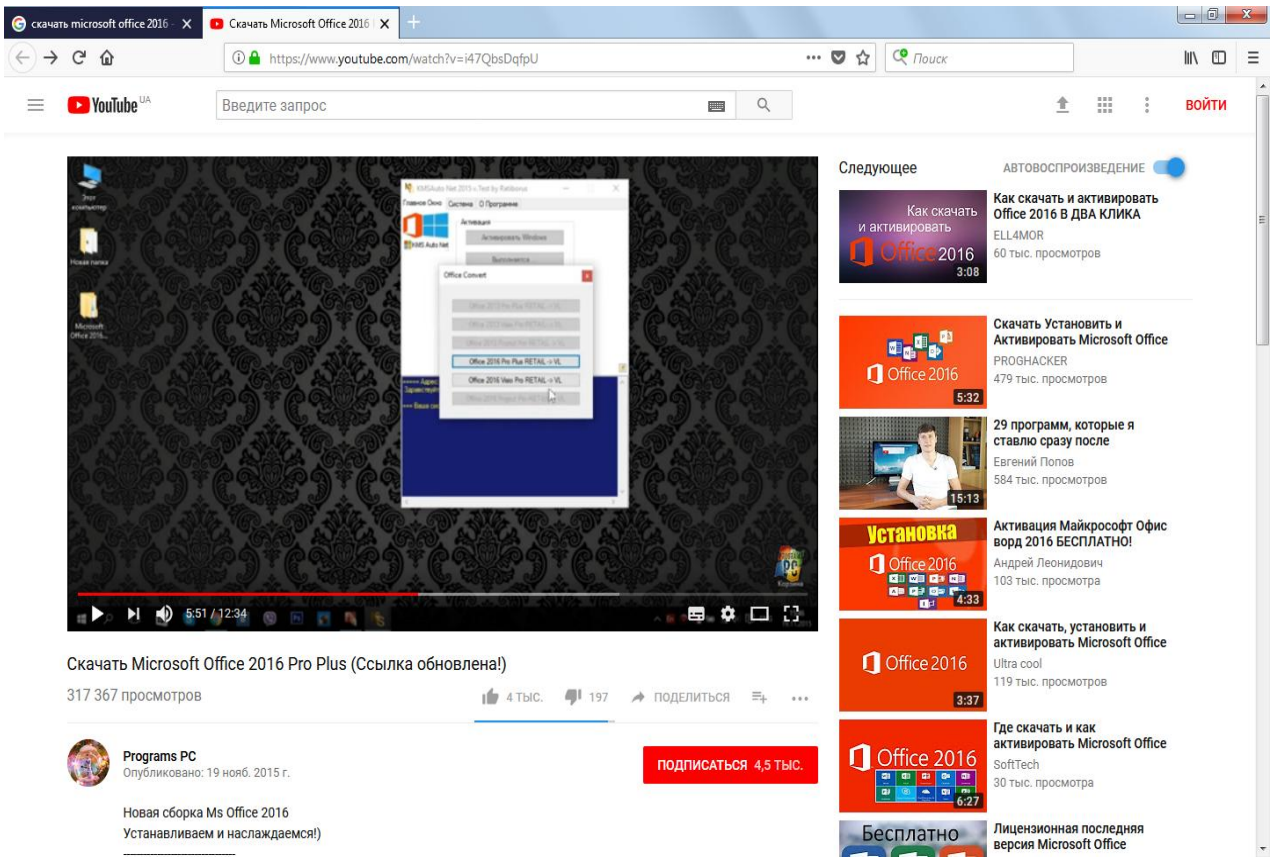


Рис. 23. Відбір типу офісу

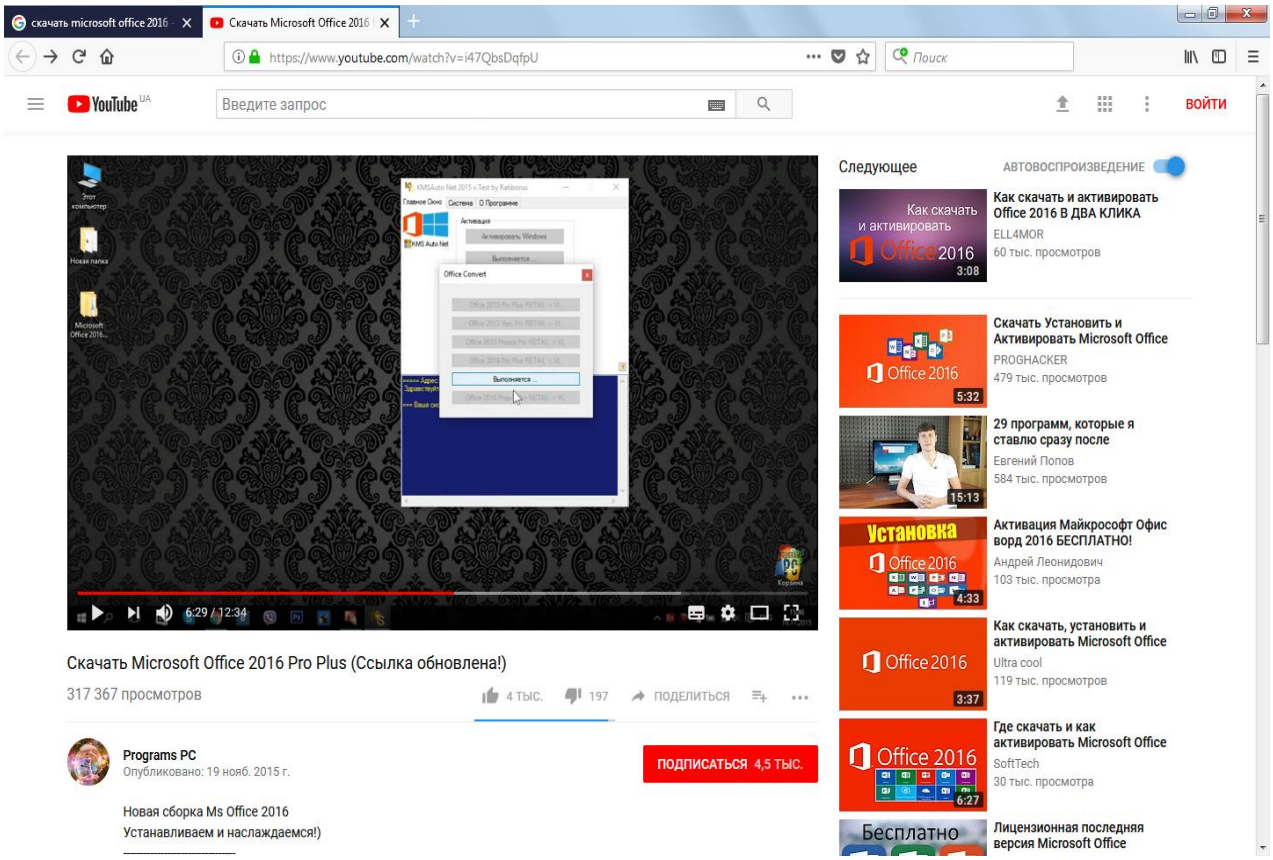


Рис. 24. Команда на активацію

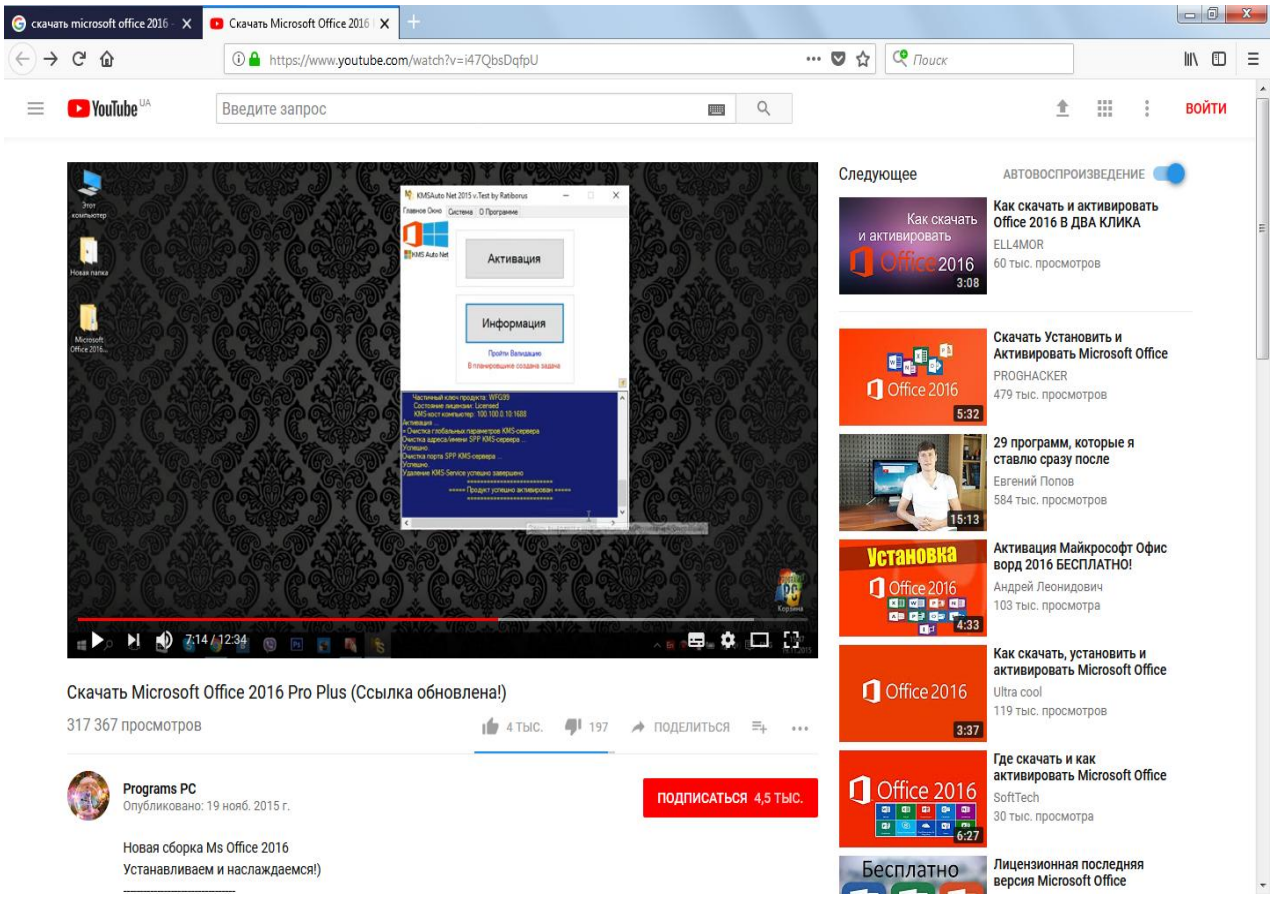


Рис. 25. Активація завершена

8. Створюємо ярлики компонентів – програм на робочому столі (рис. 26), шляхом перетягування мишкою з основного меню назв програм.

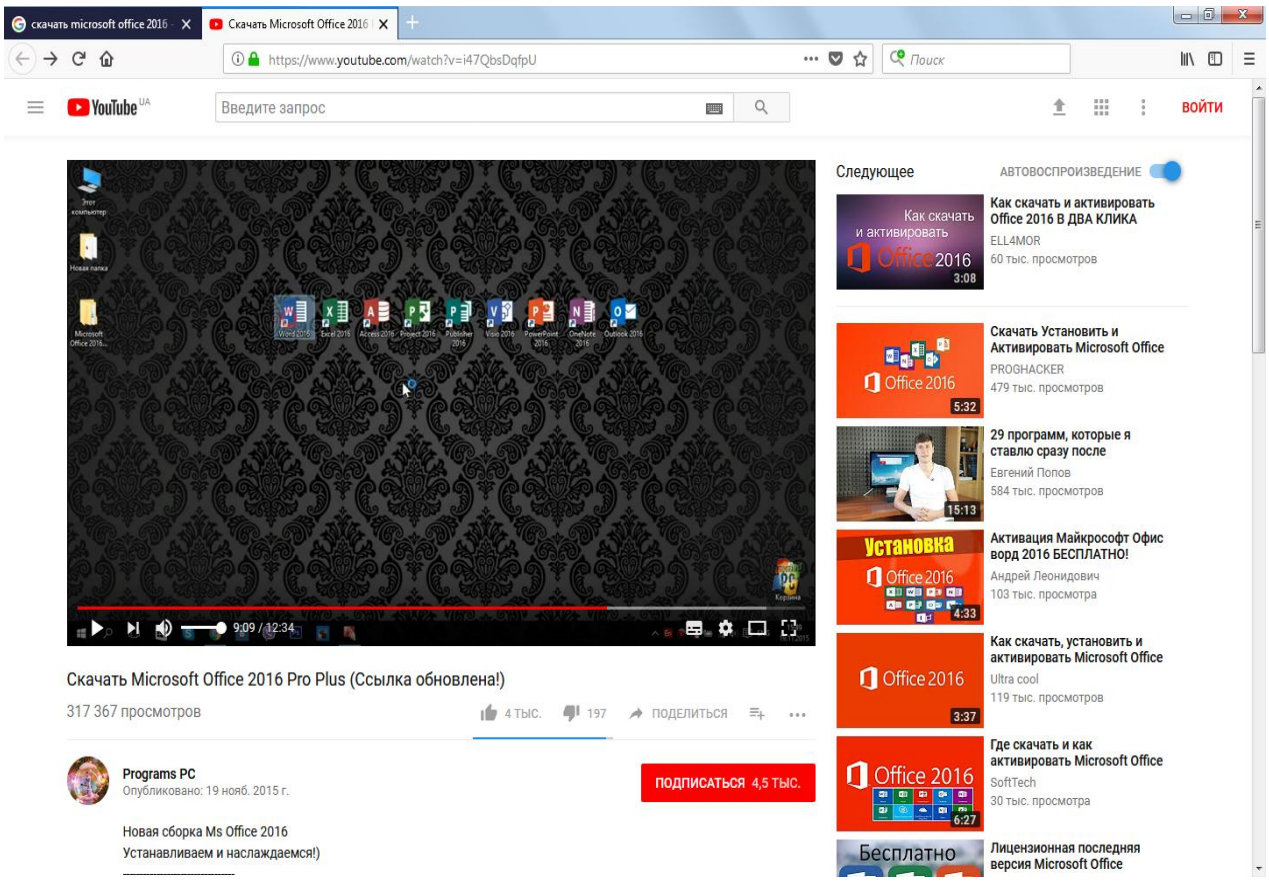


Рис. 26. Створення ярликів програм на робочому столі

9. Перевіряємо працездатність програм кожної окремо (рис. 27-29).

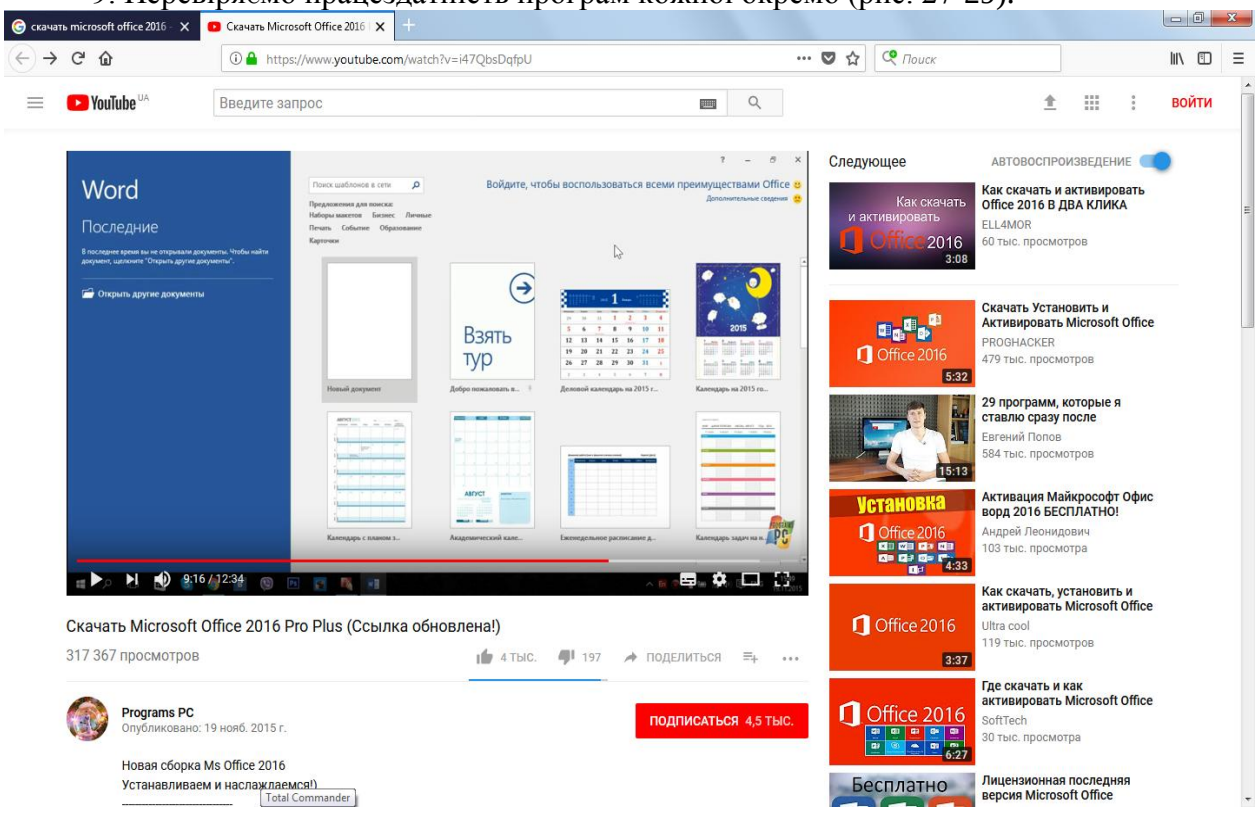


Рис. 27. Вікно Word

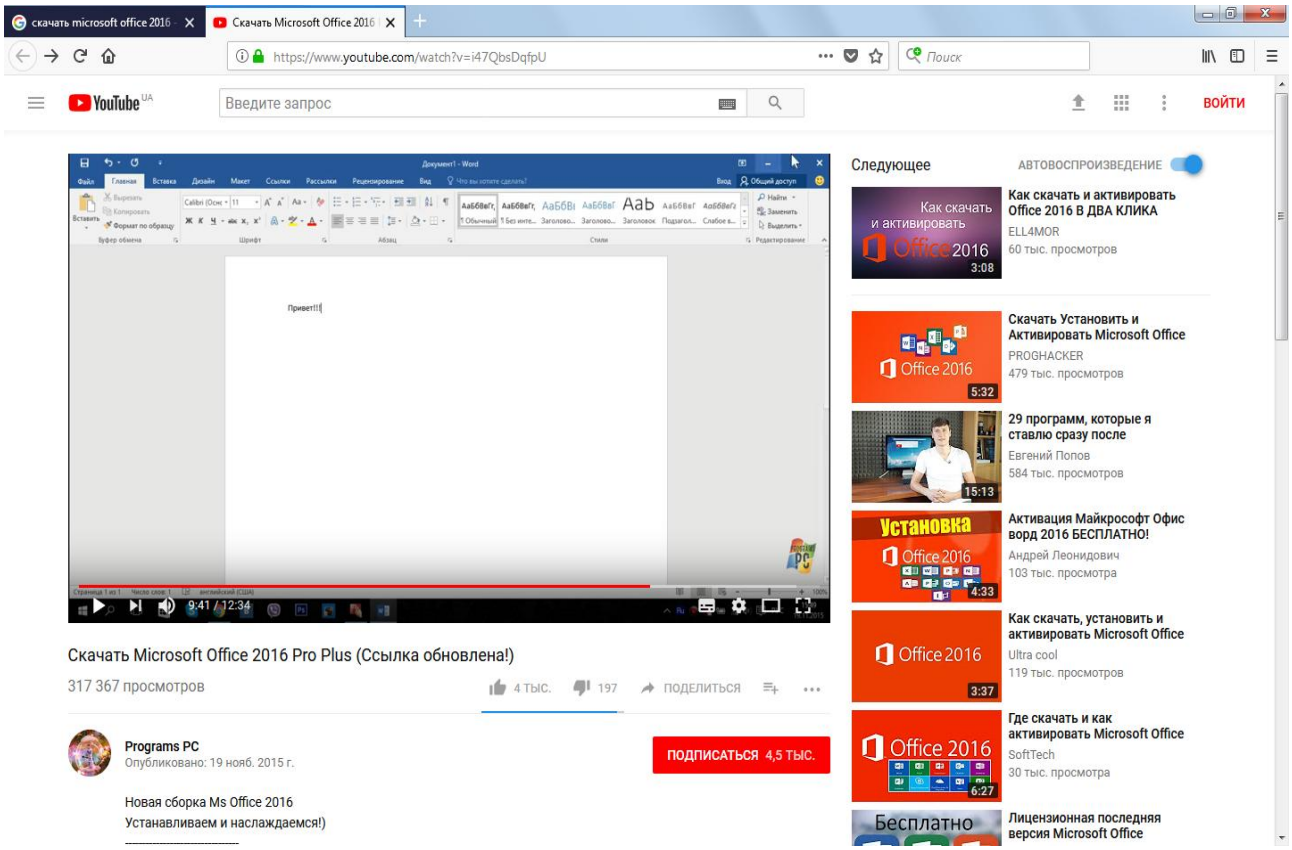


Рис. 28. Текстове вікно Word

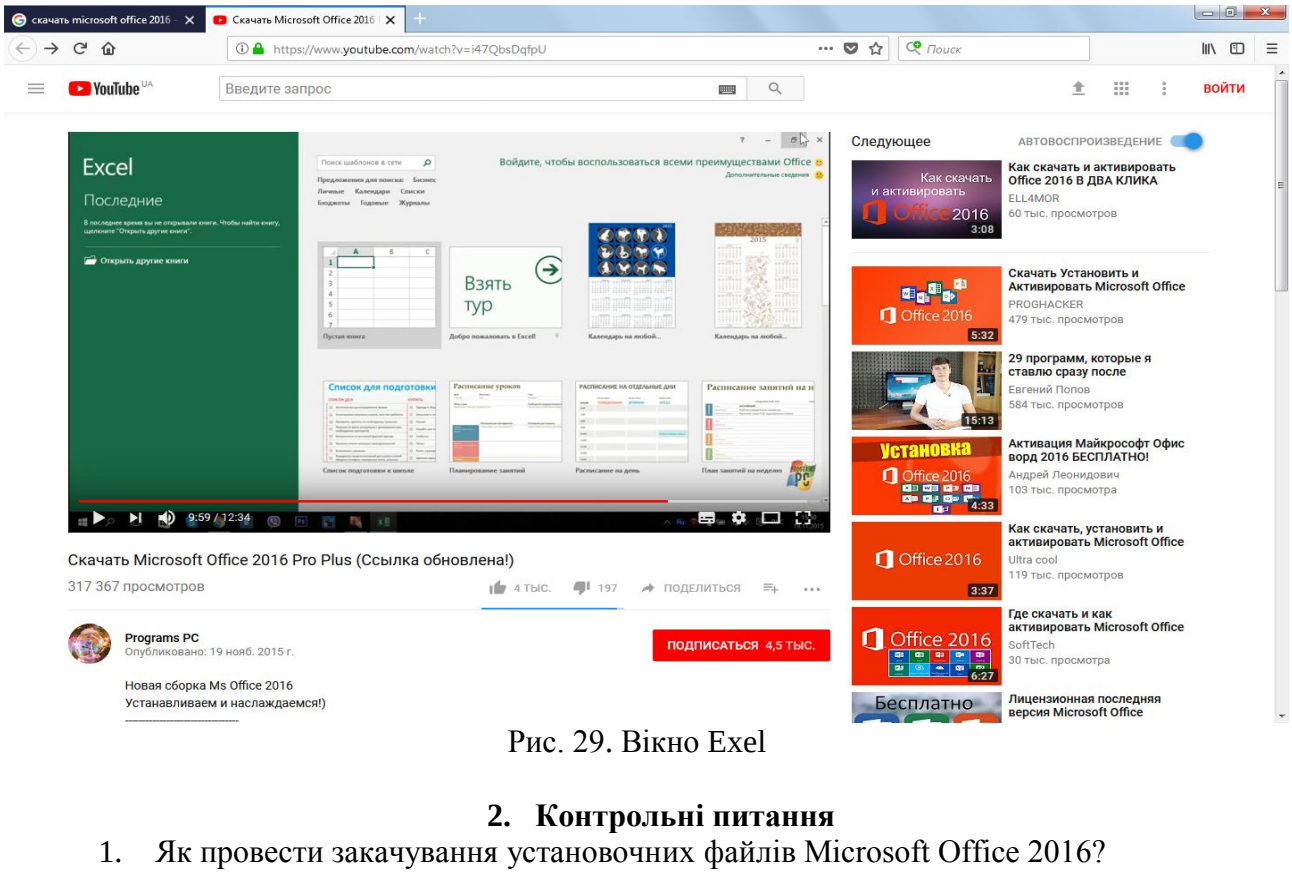


Рис. 29. Вікно Exel

2. Контрольні питання

1. Як провести закачування установочних файлів Microsoft Office 2016?
2. Як провести встановлення компонентів Microsoft Office 2016?
3. Як провести активацію компонентів Microsoft Office 2016?
4. Як провести перевірку працездатності компонентів Microsoft Office 2016?

ЛАБОРАТОРНА РОБОТА № 31.
ПРОГРАМА ЕЛЕКТРОННОЇ ПОШТИ OUTLOOK EXPRESS

Мета роботи: уміти підготувати програму Outlook Expres до роботи; налагоджувати її параметри; сформувати нові повідомлення; пересилати вкладені файли за E-mail; одержувати вхідну пошту; працювати з адресною книгою.

Зміст

1. Теорія
1.1. Налагоджування Outlook Express
1.2. Користувальницький інтерфейс пошти Outlook Express
1.3. Формування нового повідомлення
1.4. Пересилання вкладених файлів за E-mail
1.5. Одержання вхідної пошти
1.6. Адресна книга Outlook Express
1.7. Деякі додаткові можливості програми
1.8. Протокол відправлення електронної пошти SMTP
1.9. Протокол одержання електронної пошти POP3
2. Хід роботи
3. Контрольні питання:

1. Теорія
1.1. Налагоджування Outlook Express

У цей час у мережі Internet найбільше поширення отримали такі сервіси, як WWW (World Wide Web – всесвітня паутина), електронна пошта (e-mail) і служба передачі файлів за допомогою протоколу FTP.

Перераховані сервіси мають різні передумови й історію свого виникнення. Наприклад, відносно молодий, але динамічний сервіс, що розвивається, WWW з'явився в 1990 р., у той час як роком появи протоколу FTP можна вважати 1971, коли на зорі існування обчислювальних мереж був запропонований механізм передачі файлів, а перелік специфікацій, пов'язаних із цим протоколом, тримає більш 40 пунктів. Електронна пошта також є сервісом, без якого зараз важко представити мережу Internet; це добре видно з того, що велика кількість потужних компаній конкурують між собою, надаючи послуги безкоштовної електронної пошти на основі web-інтерфейсів і з можливістю доступу до неї за протоколом SMTP і POP3.

Щоб почати налагодження Outlook Express, досить клацнути по значку **Запустить Outlook Express (Launch Outlook Express)** на панелі задач Windows. Інакше програму Outlook Express можна викликати за допомогою послідовності меню **Пуск->Программы->Internet Explo->Outlook Express.**

Рис. 1. Запуск Outlook Express

Зауваження. Можливо, за якимись причинами додаток Outlook Express не встановлений на вашому комп'ютері, але це можна легко виправити, вибравши за допомогою послідовності меню **Пуск- >Настройка->Панель управления->Установка и удаление программ**, закладку **Установка Windows** і, установивши прапорець біля **Microsoft Outlook Express**. Оскільки це – стандартна операція установки нових програмних модулів із складу Windows, ми не будемо на ній зупинятися.

Власне початковий процес налагодження Outlook Express, необхідний для функціонування сервісу електронної пошти, гранично простий, – при першому виклику програми Outlook Express ще раз запускається Майстер підключення до Internet, що запросить у вас необхідні дані про поштові сервери й адресу електронної пошти, що ви повинні були одержати від провайдера.

1. У найпершому вікні треба буде увести ваше ім'я, як абонента електронної пошти, що буде з'являтися в заголовку ваших листів, коли вони прийдуть до адресатів. Звичайно, користувачі указують своє дійсне ім'я, але тут можна виявити гнучкість, і якщо ви поки не плануєте використовувати свою адресу для ділової кореспонденції, то можна обійтися і псевдонімом. Крім того, можна рекомендувати записувати своє ім'я латинським шрифтом, щоб уникнути проблем неправильного відображення заголовків із російським шрифтом у ряді програм електронної пошти (які можуть стояти у ваших колег за перепискою), так і не створювати зайвих проблем вашим можливим закордонним адресатам. Згодом, до речі, зазначене в цьому вікні ім'я можна буде легко змінити з псевдоніма на дійсне ім'я і навпаки, – якщо в цьому виникне необхідність.

2. У наступному вікні вам треба буде увести вашу адресу електронної пошти. Як правило, адреса E-mail складається з вашого імені і доменного імені провайдера, з'єднаних за допомогою знака @. Приміром, це може бути адреса виду user@peterlink.ru. Коли ви будете називати свою адресу кому-небудь уголос, то знак @ вимовляється як словосполучення "ат".

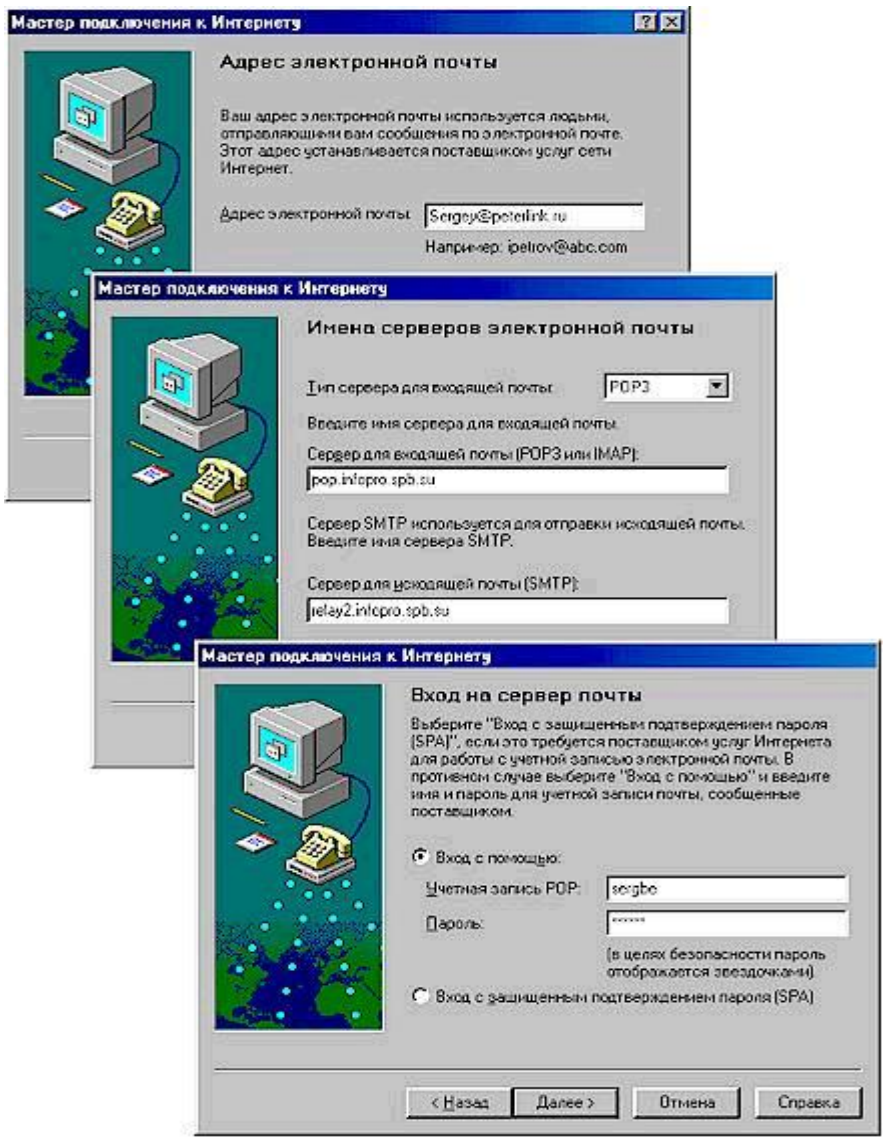


Рис. 2. Підключення до Internet

Далі Майстер запросить у вас тип сервера вхідної пошти і доменні імена поштових серверів провайдера, призначених, відповідно, для вхідної (POP3) і вихідної пошти (SMTP). Уведіть ці адреси. У випадку нашого приклада з Peterlink це будуть адреси pop.infopro.spb.su і relay2.infopro.spb.su, відповідно. Наявність різних поштових серверів зв'язане з тим, що повідомлення електронної пошти пересилаються між вузлами Internet (вузлами різних провайдерів) за протоколом SMTP (Simple Mail Transfer Protocol), а на останньому відрізку між вузлом вашого провайдера і вашим комп'ютером – за POP (Post Office Protocol). Введіть у відповідних полях діалогового вікна ті адреси поштових серверів, що отримані вами від провайдера. Що стосується типу сервера вхідної пошти, то якщо ваш провайдер спеціально не вказав даний параметр, то за замовчуванням залишіть POP3.

3. Тепер у новому вікні вкажіть зведення про обліковий запис вашого з'єднання – ім'я користувача й пароль. Це ті ж самі зведення, що ви звичайно, використовуєте для підключення до Internet. У даному випадку ці зведення потрібні для того, щоб програма Outlook Express могла автоматично додзвонюватися до провайдера і встановлювати з'єднання для відправлення й прийому електронних листів. У наступному вікні, вам буде запропоновано ввести "дружнє ім'я" для даного облікового запису пошти. Можете ввести що-небудь типу "Моя пошта на Peterlink" чи залишити той запис, що пропонується за замовчуванням.

4. У черговому вікні вкажіть тип вашого з'єднання, – для нашого випадку – це з'єднання за модемом, хоча якщо ви застосовуєте Outlook Express в офісі, то там можна використовувати і підключення через локальну мережу. Ці з'єднання будуть встановлюватися автоматично, але можна вибрати і третє значення перемикача, що

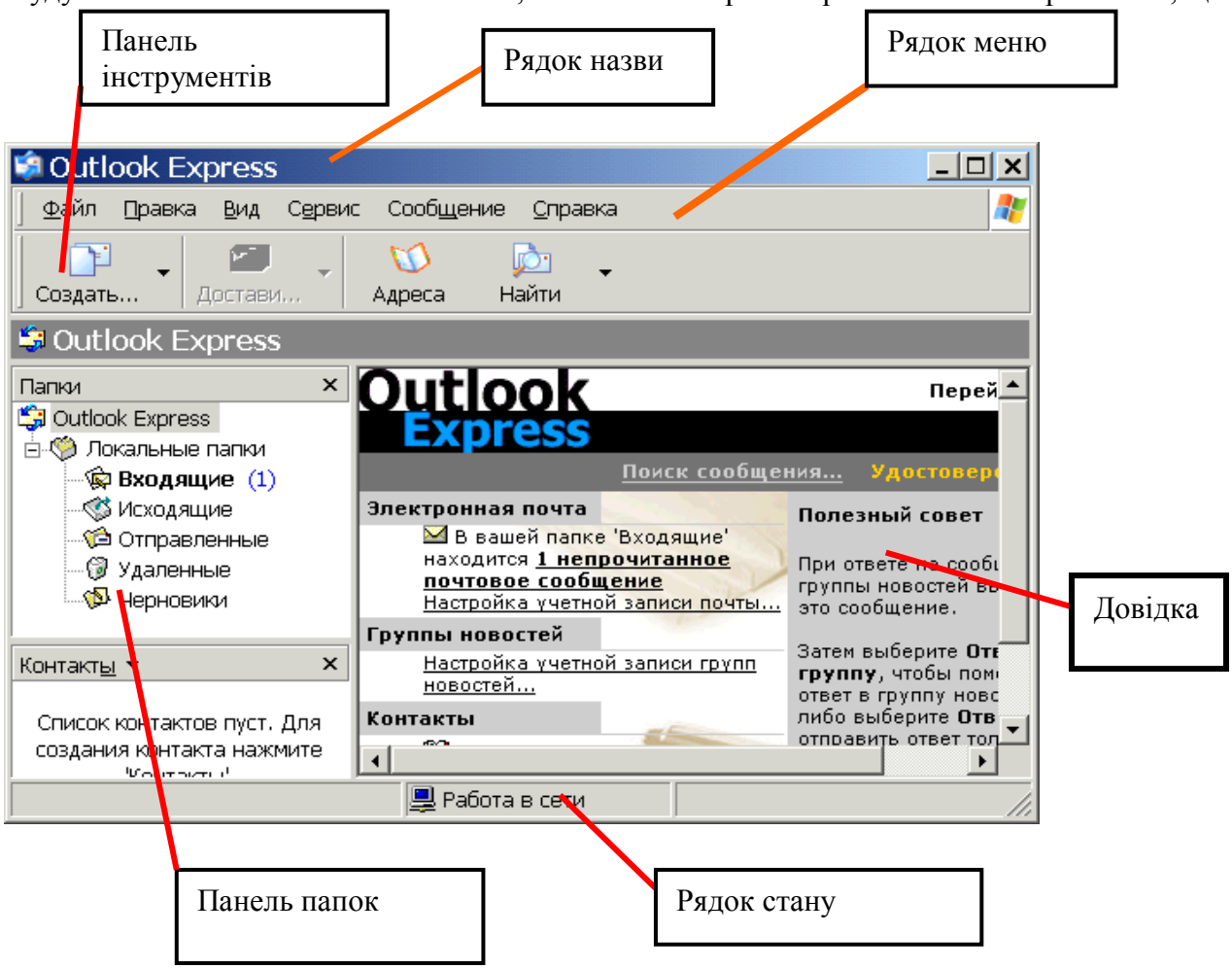


Рис. 3. Користувацький інтерфейс програми

пропонує вручну з'єднатися з провайдером перед кожним сеансом роботи з електронної пошти. Тепер залишилися два самих останніх вікна – в одному треба вибрати обліковий запис (якщо у вас усього один провайдер, то і вибір, рис. 3 відповідно, буде невеликий), але сьогодні нерідка ситуація, коли користувач має облікові записи в декількох провайдерів і плюс обліковий запис для модемного доступу до локальної мережі своєї компанії. І, нарешті, залишилося те вікно, де потрібно підтвердити дані, введені в попередніх вікнах, клацнувши по кнопці Готово (Finish). Після натискання кнопки Готово Майстер підключення до Internet завершить процес налагодження Outlook Express.

1.2. Користувальницький інтерфейс пошти Outlook Express

Давайте познайомимося з інтерфейсом Outlook Express, звернувшись до рис.3.

- Рядок заголовка (title bar) містить стандартні назви.
- елементи вікна Windows-додатка (кнопки Згорнути, Відновити і Закрити). У цьому рядку також зазначена назва додатка (Outlook Express).
- Рядок меню (menu bar) містить заголовки меню, що надають доступ до усіх функцій, необхідних для роботи з Outlook Express. За допомогою меню ви можете формувати нові повідомлення, відправляти й одержувати пошту, пересилати листа іншим користувачам, набудовувати інтерфейс Outlook Express і т.д. Крім того, ви зустрінете в меню безліч звичайних пунктів, характерних для всіх додатків Windows-друк, довідка і т.д. З рядка меню ви так само можете викликати Internet Explorer і завантажувати для перегляду сторінки Web.
- Панель інструментів (toolbar) призначена для швидкого доступу до деяких найбільше часто використовуваних команд Outlook Express. У залежності від того, у якому режимі працює Outlook Express (пошта чи новини), число кнопок і їхнє призначення автоматично змінюються. Крім того, у початковий момент після завантаження Outlook Express встановлюється в загальний режим (коли ще не обраний потрібний режим – пошта чи новини). У такому загальному режимі кнопки панелі інструментів виконують наступні функції:
- Створити повідомлення (Compose message) відкриває вікно для формування нового листа.
- Доставити пошту (Send and Receive) – за допомогою цієї кнопки ви можете швидко і легко підключитися до провайдера, щоб перевірити й доставити вхідну пошту, а так само відправити вашу власну.
- Адресна книга (Address Book) – відкриває доступ до адресної книги, куди ви записуєте для збереження адреси e-mail ваших друзів, колег по роботі і т.д.
- З'єднати (Connect) – натискання на цю кнопку викликає активізує процес з'єднання з провайдером.
- Розірвати з'єднання (Hang Up) – розриває з'єднання з провайдером Internet.
- Панель "Папки" (Folders) дозволяє вивести на екран списки листів і їхній уміст, що зберігаються в одній з 4-х стандартних папок Outlook Express: Вхідні (Inbox), Що Виходять (Outbox), Відправлені (Sent Items), Вилучені (Deleted Items) і Чернетки (Drafts). Outlook Express дозволяє завести нові додаткові папки користувача і вони так само будуть доступні з цієї панелі. Після того як ви настроїте доступ до серверів новин, то в цій панелі з'являться й імена відповідних серверів новин.
- Область перегляду Outlook Express при роботі з електронною поштою чи новинами розділена на дві частини: угорі ви бачите список повідомлень електронної пошти з поточної папки, а в нижній частині вікна показується уміст відзначеного листа. Уміст листа можна подивитися й в окремому вікні, якщо зробити подвійний щиглик по рядку з обраним листом. Область перегляду може бути розділена чи за горизонталлю, чи за вертикаллю, – якщо такий спосіб організації інтерфейсу покажеться вам більш зручним. Що стосується порядку показу листів, то за замовчуванням усі листи в папках розташовуються відповідно до алфавітного порядком імен відправників, але їх можна відсортувати й інакше – наприклад, за датою надходження листа.

Кілька слів про те, як інтерпретуються значки з різними зображеннями конверта в області перегляду:

- Відкритий конверт відзначає вже прочитаний вами лист
- Закритий конверт– плюс жирний шрифт відзначає лист, що ви ще не читали
- Скріпка в листах говорить про те, що в лист вкладений окремий файл (наприклад, документ у форматі Word, графічний файл і т.д.). Якщо виділити такий лист, і клацнути по зображенню скріпки в правому куті нижньої частини вікна, то буде показане ім'я файлу. Подвійний щиглик по імені вкладеного файлу дозволить переглянути його вміст за допомогою відповідної програми.

- Рядок стану (status bar) використовується для двох цілей. Звичайно, в ній Outlook Express указує загальне число повідомлень у даній папці й окремо – число непрочитаних повідомлень. У правій частині рядка стану при перевірці надходження нової пошти з'являється напис, що інформує про прихід чи навпаки, відсутності нових листів. Крім того, при роботі Outlook Express там з'являються значки, що характеризують режим роботи цього додатка в даний момент часу (наприклад, закреслений значок мережевого диска означає, що в цей момент немає з'єднання з Internet).

Рада. По-перше, щоб зберегти місце на екрані, можна порадити відразу ж відключити дві панелі – самий лівий стовпчик зі значками папок (тому що її вміст повторюється лівіше) і сірий рядок із написом Outlook Express над областю перегляду (як не несучого функціонального навантаження). Для цього виберіть у меню Вид (View) пункт Розкладка. Повторний вибір цього пункту меню відновлює ці панелі. Що ще можна порадити, так це установити в нижній частині області перегляду Outlook Express прапорець Переходити в папку "Вхідні" при запуску (When starting, go directly to my Inbox folder). Тоді відразу після запуску Outlook Express буде переходити до папки "Вхідні", що дозволить вам швидше приступити до читання нових листів.

1.3 Формування нового повідомлення

Для створення нового повідомлення натисніть на кнопку Створити повідомлення (Compose Message) на панелі інструментів Outlook Express, або подати *команду* **Почтовое сообщение** із підменю **Создать** підменю **Файл**, що викликає окреме вікно (рис. 4). Роботу з новим листом варто почати із заповнення заголовка листа, що має поля: Кому: (To:), Копія:(Cc:), Схована: (Bcc:), Тема: (Subject:). Помітимо, що за зрозумілими причинами, обов'язковим є заповнення тільки полю Кому: (To:), – інакше лист просто не знайде свого адресата. Розглянемо докладніше елементи заголовка:

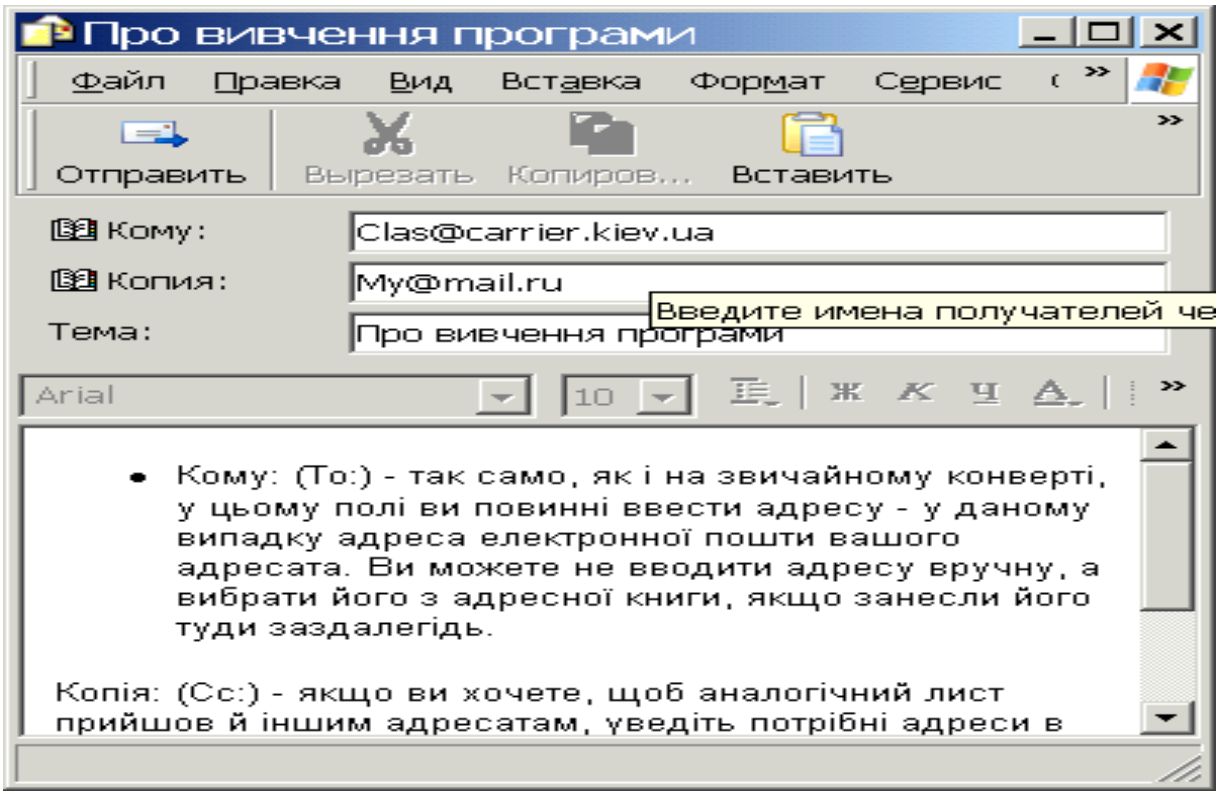


Рис. 4. Формування нового повідомлення

- Кому: (To:) – так само, як і на звичайному конверті, у цьому полі ви повинні ввести адресу – у даному випадку адреса електронної пошти вашого адресата. Ви можете не вводити адресу вручну, а вибрати його з адресної книги, якщо занесли його туди заздалегідь.

- Копія: (Cc:) – якщо ви хочете, щоб аналогічний лист прийшов й іншим адресатам, уведіть потрібні адреси в даному полі, розділяючи їх за допомогою знака ";" (крапка з комою). Словосполучення "Cc" – це скорочення від англійського "канцелярського" терміна Carbon Copy (по-російському – "копірка"). Усі люди, до яких прийшов даний лист, легко зможуть довідатися із заголовка, кому ви ще послали даний лист. Цей рядок також може бути заповнений з адресної книги.
- Схована: (Bcc:) – якщо ви хочете, щоб аналогічний лист прийшов й іншим адресатам, але вони не знали, кому ще ви відіслали даний лист, то введіть потрібні адреси в даному полі, розділяючи їх за допомогою знака ";" (крапка з комою). Словосполучення "Bcc" - це скорочення від англійського Blind Carbon Copy (по-російському можна було б перевести як "сліпа копірка"). Цей рядок також може бути заповнений з адресної книги.
- Тема: (Subject:) – тут варто вписати кілька слів, що характеризують тему повідомлення. Заголовок краще писати по-англійському, якщо ви не упевнені, що поштова програма вашого адресата підтримує 8-бітове кодування заголовків і на його машині інстальовані російські шрифти. Крім того, для російських заголовків часто ушкоджується їхній тип кодування при пересиланні між різними провайдерами.

Рада. Зверніть увагу на те, що Outlook Express підказує вам призначення кожного незаповненого полю за допомогою напису сірого кольору, чи пояснення. Після заповнення заголовка листа ви спочатку можете скористатися кнопкою на панелі інструментів вікна Перевірити імена (Check Names), щоб бути упевненим у правильній відповідності введених адрес того формату, що передбачений в Інтернеті для повідомлень E-mail, наприклад, user@host.domain, де user – ім'я адресата, host.domain – доменне ім'я поштового сервера адресата).

Далі вже можна приступати до самого листа, для чого клацніть курсором миші в поле листа і введіть потрібний текст. При необхідності ви можете "укласти" у лист файл будь-якого формату. За традицією, завершує лист вставка підпису, для чого варто натиснути кнопку із зображенням авторучки на панелі інструментів (оригінальний і дотепний підпис – одна з традицій Internet). Якщо у вас ще не створений підпис, то створити його можна, вибравши в меню Сервіс (Tools) пункт Бланк повідомлень (Stationary) і далі – натиснувши на кнопку Підпис (Signature). Створений в такий спосіб підпис можна потім багаторазово використовувати. Зверніть ще увагу на зображення логотипа Internet Explorer (стилізованої букви e) у правій верхній частині нового повідомлення. Лого є ідентифікатором "важливості" повідомлення, що відправляється. У меню Сервіс (Tools) мається пункт вибору важливості повідомлень, при натисканні на який буде виведений список можливих опцій важливості повідомлень (Висока, Звичайна і Низька). Тепер залишилося лише натиснути на кнопку відправлення листа (сама ліва кнопка на панелі інструментів цього вікна із зображенням конверта, що летить, і написом Відправити) і ваш лист - на шляху до адресата. Якщо встановлений прапорець Відправляти повідомлення негайно (Send messages immediately...) на вкладці Відправлення у вікні Параметри (див. меню Сервіс), то Outlook Express відразу ж зробить з'єднання з провайдером і відправить лист. Якщо ж прапорець знятий, ваші листи будуть тимчасово міститися в папку Вихідні (Outbox), де вони будуть накопичуватися перед відправленням. В останньому випадку на екран буде виведене повідомлення про приміщення листа в папку Вихідні. Коли ви завершите складання всіх листів, натисніть на кнопку Доставити пошту (Send and Receive) на панелі інструментів основного вікна Outlook Express, і далі процес з'єднання з провайдером піде зовсім аналогічно тому, як ми розглянули в попередньому розділі.

1.4. Пересилання вкладених файлів за E-Mail

Можливість відправити за електронною поштою файл будь-якого формату – одне із самих корисних якостей E-mail. Тим самим ви можете направити своїм адресатам і документ Word, і файл із потрібним зображенням, звукове чи відео-вітання і будь-які інші

файли. Єдина умова – не посилайте дуже великі файли, якщо ви не упевнені в тім, що ваш адресат має виділений канал в Internet, а можливо працює за звичайною телефонною лінією. Для таких випадків файл розміром 200-300 Кб вважається звичайно, межею "пристойностей". Також майте на увазі, що багато поштових серверів провайдерів просто повертають назад пошту, якщо її розмір більш визначеної межі (найчастіше – при розмірі пошти більш 1 Мб).

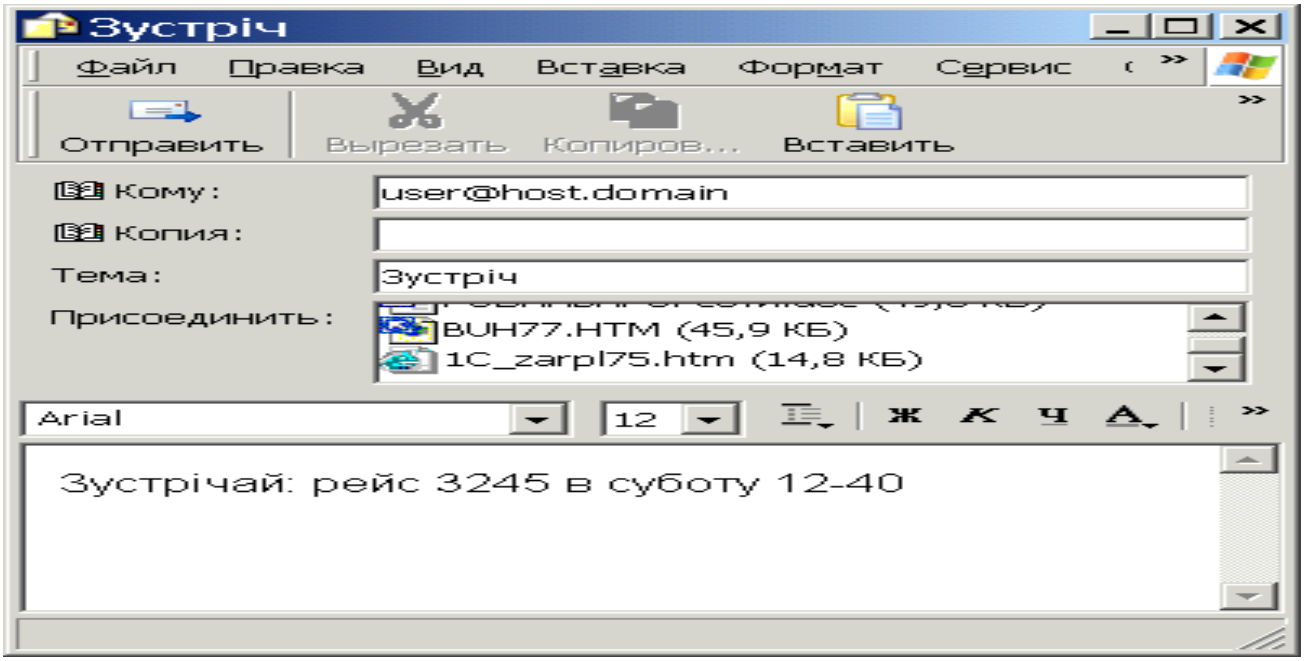


Рис. 5. Пересилання вкладених файлів

Отже, для вкладення файлу в лист, розмістивши курсор у вікні для введення листа, натисніть кнопку із зображенням скріпки на панелі інструментів, або подати команду **Вложение файлу** із підменю **Вставка**. У відповідь на екран буде виведене стандартне діалогове вікно із зображенням файлової структури вашого комп'ютера. Коли ви знайдете на диску потрібний файл, виділіть його і натисніть кнопку Вкласти (Attach). Outlook Express уставить файл у ваш електронний лист, і нижче тіла листа з'явиться додаткове вікно зі значком уставленого файлу (рис. 5).

Варто нагадати, що аналогічним чином виглядають і листи, що прийшли до вас, які мають вкладені файли. Досить двічі клацнути на значку з вкладеним файлом, як завдяки механізму OLE (Object Linking and Embedding) операційної системи Windows буде запущений відповідний додаток для перегляду цього файлу.

Поштові папки Outlook Express

Хоча назви поштових папок Outlook Express багато в чому говорять самі за себе, але якщо ви не маєте досвіду роботи з поштовими програмами, усе-таки варто познайомитися з їхнім призначенням:

- Вхідні (Inbox). Сюди за замовчуванням надходить уся нова пошта і тут зберігаються всі повідомлення, що прийшли. Згодом ви можете створити додаткові папки (наприклад, присвячені різним проектам чи листам від постійних адресатів) і настроїти Outlook Express таким чином, щоб при надходженні нових листів уся пошта автоматично розбиралася й складалася в окремі папки.
- Вихідні (Outbox). Це папка призначена для тимчасового збереження листів, що відправляються. Навіщо це потрібно? Представте, що ви підготовляєте кілька листів один за одним. Щоб не з'єднуватися щораз з Internet для відправлення чергового листа, листи тимчасово накопичуються в цій папці. Потім при натисканні на кнопку Доставити пошту (Send and Reseive) вони разом ідуть на поштовий сервер провайдера і далі – до своїх

адресатів. Саме такий режим відправлення листів установлюється в Outlook Express за замовчуванням.

- Відправлені (Sent Items). Тут за замовчуванням зберігаються копії відправлених повідомлень, і ви завжди зможете згадати, що, кому і коли ви відсилали.
- Вилучені (Deleted Items). Якщо ви вирішите видалити непотрібні повідомлення, то вони тимчасово поміщаються на збереження в цю папку (на випадок, якщо ви передумаєте їх видаляти). Якщо ви вирішите назовсім видалити повідомлення з цієї папки, зробіть правого щиглика по значку папки і з меню виберіть пункт Очистити папку (Empty folder).
- Чернетки (Drafts). Якщо ви готуєте новий лист, але в процесі роботи над ним вирішите дописати лист пізніше, те виберіть у меню Файл (File) пункт Зберегти (Save). Такий "недописаний" лист тимчасово зберігається в папці Чернетки (Drafts). Щоб продовжити згодом роботу над листом із цієї папки, просто відкрийте цю папку і двічі клацніть по чернетці листа. Потім, якщо лист готовий, то його можна відправити і він буде поміщено в папку Вихідні (Outbox). Якщо ж лист як і раніше не готовий до відправлення, то його знову можна зберегти в папці чернеток.

1.5. Одержання вхідної пошти

Одержання вхідної пошти – це, напевно, найпростіша дія з усього спектра робіт із Outlook Express, уся функціональність якого полягає в тому, що треба установити з'єднання з поштовим сервером провайдера. Тому досить запустити програму Outlook Express, що за замовчуванням відразу запропонує вам з'єднатися із сервером провайдера. Якщо з'єднання з провайдером уже встановлено, то досить, вибравши назву з'єднання, натиснути кнопку **ОК.** Інакше з'явиться додаткове вікно, де треба буде увести ваше ім'я користувача й пароль. У будь-якому випадку підсумок буде один – комп'ютер почне встановлювати з'єднання з поштовим сервером провайдера.

Після того як ваш модем здійснить з'єднання, з'явиться вікно, у якому Outlook Express буде перевіряти наявність листів, що прийшли, і здійснювати їхнє завантаження на ваш комп'ютер. Після завершення цієї дії поштова програма перевірить, чи немає у вас у папці Вихідні (Outbox) готових листів для відправлення, і якщо є, то у свою чергу, перешле їх на поштовий сервер провайдера, відкіля вони вже підуть адресатам.

Рада. Outlook Express дозволяє встановлювати сеанс зв'язку з провайдером тільки на час доставки листів (одержання листів, що прийшли, і відправлення своїх), відразу, ж відключаючи від Internet за завершенням передачі. Щоб уключити цю опцію, потрібно установити прапорець Розірвати з'єднання за завершенням доставки (Disconnect...) на вкладці Вилучений зв'язок (Connection) вікна чи властивостей прямо у вікні. Тим самим ви уникнете нераціональних витрат часу.

1.6. Адресна книга Outlook Express

Адресна книга – це збірник адрес e-mail ваших колег за електронним переписуванням, організований за допомогою зручної програмної оболонки. Адресна книга в програмі Outlook Express являє собою "запозичену" копію адресної книги з могутньої корпоративної поштової програми MS Exchange. Крім експорту адрес з MS Exchange, у Outlook Express можна також експортувати адреси з цілого ряду інших поштових програм: MS Internet Mail, Eudora Pro, Eudora Light, а також із цілого ряду поштових клієнтів Netscape різних версій. Заповнювати адресну книгу Outlook Express можна в двох режимах: по-перше, витратити спочатку якийсь час і заздалегідь увести дані про ваших колег, і по-друге, поповнювати адресну книгу "на льоту", у міру роботи з поштою, просто копіюючи туди адреси листів, що прийшли. Нижче ми розглянемо ці два випадки.

1. Якщо ви хочете заповнити адресну книгу заздалегідь, натисніть кнопку Адресна книга, або введіть команду **Адресная книга** із під меню **Сервис**, що викликає появу головного вікна цього збірника адрес і ін. контактної інформації (рис. 6).

Крім імен і адрес E-mail в адресній книзі можна зберігати безліч різної інформації – номера телефонів, пейджерів, особистих і службових сторінок Web, звичайний поштової адреси абонента й ін. Для того щоб внести в адресну книгу нове ім'я, натисніть кнопку Створити адресу (New Contact) або введіть команду **Создать контакт** із під меню **Файл.** Уведіть у відповідних полях ім'я абонента й адреса його електронної пошти, при бажанні можете заповнити додаткові дані на абонента на інших закладках. Якщо ви захочете відредагувати адресу електронної пошти чи інший параметр, то виберіть ім'я в адресній книзі і натиснувши кнопку Властивості (Properties), змініть дані на закладках аналогічним чином.

2. Друга можливість: після того, як ви завели адресну книгу і наповнили її деякими адресами, надалі книгу можна поповнювати за рахунок адрес із листів які знову прийшли. Для цього відкрийте потрібний лист, відзначте ім'я адресата в полі заголовка, натисніть праву клавішу миші і зі спливаючого контекстного меню виберіть пункт Додати в адресну книгу (Add To Address Book).

3. Тепер, коли адресна книга містить дані за адресами E-mail ваших колег за перепискою, ми коротенько розглянемо порядок роботи з нею при формуванні нових листів і заповненні полю Кому: (To:):

- Натисніть кнопку Створити повідомлення (New Message) в основному вікні Outlook Express, помістіть курсор у поле Кому: (To:) у вікні створення нового повідомлення.
- Клацніть по значку з зображенням відірваного листка папера поруч із словом Кому. Ця дія викликає появу діалогового вікна, де можна легко вибрати одержувачів даного листа.
- Виберіть із списку абонентів потрібну людину і натисніть кнопку Кому -> (Te->) у середній частині вікна.
- Аналогічним чином додайте абонентів у полях Копія: (Cc:) чи Схована: (Bcc:), якщо необхідно розіслати цей лист ще декільком адресатам.

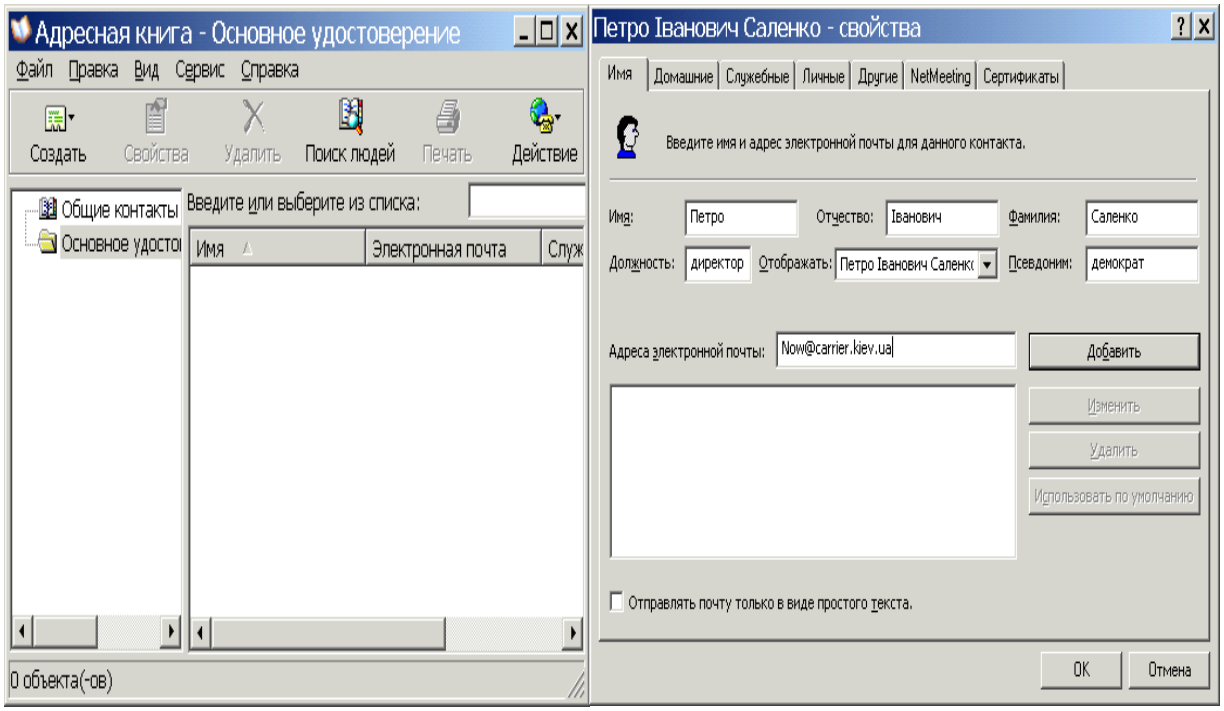


Рис. 6. Адресна книга

- Натисніть кнопку **ОК**, і обрані адреси з'являться у відповідних полях заголовка нового листа.
- Тепер можна приступати до заповнення тіла листа і його відправленню, про що ми вже розповіли раніше.

Зауваження. Імена абонентів, введених у поле Кому: (To:), Копія: (Cc:), Схована: (Bcc:) за допомогою адресної книги, можуть бути представлені у вікні іменами абонентів, а не їх електронними адресами. Не турбуйтеся – програма Outlook Express сама підставить адреси E-mail при відправленні повідомлення.

Ще одна опція, що ви можете використовувати в адресній книзі Outlook Express – це групові імена. Групові імена являють собою ваші особисті списки розсилання і зручні в тому випадку, якщо вам треба часто розсилати листа постійним групам людей (наприклад, учасникам якого-небудь спільних із вами проекту). Групові імена в Outlook Express створюються натисканням на кнопку Створити групу (New Group) на панелі значків адресної книги. Потім ви можете вказати ім'я групи і скласти список людей у цій групі. Після того як ви створили групу, ви можете використовувати ім'я групи в поле Кому: чи Копія: повідомлення, що відсилається – це повідомлення буде спрямоване усім, хто входить у цю групу. Щоб у наслідку відредагувати список членів групи і їхніх адрес e-mail, треба вибрати (відзначити) уже існуючу групу і клацнути по кнопці **Властивості.**

1.7. Деякі додаткові можливості програми

1. Відправлення сторінок на основі бланка повідомлень. Оскільки Outlook Express уміє відправляти повідомлення у форматі HTML, то для таких повідомлень можна використовувати заздалегідь підготовлений бланк (шаблон HTML-сторінки) із фоновим малюнком. Разом із Outlook Express поставляються більш десятка стандартних бланків, що відповідають різним випадкам життя. Природно, що такий лист варто відправляти тільки тому одержувачу, хто також працює з Outlook Express чи іншою програмою, що вміє показувати повідомлення у форматі HTML. Для вибору бланка в меню Повідомлення вибрати пункт Створити з використанням.
2. Пошук потрібного повідомлення в папках Outlook Express. Якщо не вдається знайти потрібне повідомлення електронної пошти, то можна задіяти функцію пошуку за папками на основі шаблона. Щоб викликати вікно пошуку, натисніть на клавіатурі одночасно клавіші CTRL+SHIFT+F.
3. Сортування повідомлень у папках Outlook Express. Повідомлення в папках Outlook Express можна легко відсортувати в тім порядку, що вам більше подобається (за алфавітом, за датою одержання і т.д.). Для цього виберіть у меню Вид пункт Сортування, і далі – той вид сортування, що вважаєте потрібним.

1.8. Протокол відправлення електронної пошти SMTP

Метою протоколу SMTP є забезпечення надійної й ефективної доставки електронної пошти. Протокол SMTP не залежить від конкретних підсистем передачі й вимагає для роботи лише канал з гарантованою й упорядкованою доставкою потоку даних.

Поштове повідомлення складається тільки із трьох частин: конверта, заголовку й тіла повідомлення. Конверт використовується тільки програмами доставки й не видний користувачеві. Заголовок завжди перебуває перед тілом повідомлення й відділений від нього порожнім рядком. Заголовок повідомлення складається з полів, які, у свою чергу, складаються з розділених двокрапкою імені й значення поля. У заголовку завжди є наступні поля, які представлені в табл. 2.

Таблиця 2

Поля заголовка

Ім'я поля	**Зміст поля**
FROM	Адреса відправника повідомлення
TE	Адреса одержувача повідомлення
CC	Адреси одержувачів копій повідомлення
DATE	Час і дата відправлення повідомлення
MESSAGE ID	Ідентифікатор, використовуваний програмами електронної пошти
SUBJECT	Тема (короткий опис) повідомлення

У заголовку можуть бути присутні і інші, необов'язкові поля.

Важливою властивістю протоколу SMTP є можливість транспортування пошти через безліч мереж, які звичайно називають «поштовими трансляторами SMTP». Мережі складаються з обопільно доступних за протоколом TCP хостів публічної мережі Internet, обопільно доступних за TCP хостів приватних мереж TCP/IP, що перебувають за міжмережевими екранами, або хостів деяких інших локальних і розподілених середовищ, що використовують на транспортному рівні протоколи, відмінні від TCP.

Використовуючи протокол SMTP, процес може передавати пошту іншому процесу в тій же мережі або в деяких інших мережах через транслятори або шлюзи, доступні з обох мереж. Таким шляхом поштові повідомлення можна передавати через безліч проміжних трансляторів (називаних «relay») або шлюзів на шляху між відправником і кінцевим адресатом. Для визначення наступного проміжного одержувача на шляху до адресата використовується механізм Mail exchanger (MX) системи доменних імен.

1.9. Протокол одержання електронної пошти POP3

Протокол POP3 пропонує наступний порядок обміну інформацією між клієнтом і поштовим сервером:

На початку роботи користувача проводиться його авторизація шляхом перевірки відповідності імені й пароля користувача. Запити клієнта й відповіді сервера з результатами обробки запитів передаються в текстовому вигляді. Після успішної авторизації клієнт починає роботу зі змістом поштової скриньки. Протокол POP3 дозволяє одержати зведену інформацію про повідомлення – кількість повідомлень, їх розмір і список, а також вибрати певне повідомлення. Після прочитання повідомлень користувач може позначити повідомлення до видалення.

При одержанні команди завершення сеансу сервер видаляє позначені повідомлення й завершує сеанс роботи із клієнтом. Команди протоколу POP3 складаються із ключових слів, за якими може випливати один або більше аргументів. Усі команди закінчуються парою <CRLF>. Відповіді в POP3 складаються з індикатору стану й ключового слова, за яким може випливати додаткова інформація. Відповідь закінчується парою <CRLF>. Протоколом POP3 передбачено два індикатори стану: «+OK» – позитивний і «-ERR» – від'ємний.

Якщо відповідь на команду складається з декількох рядків, то рядка відповіді розділяються послідовністю <CRLF>, а закінчення відповіді позначається крапкою (Ascii-Символ з кодом 46) і послідовністю <CRLF>. У мінімальній реалізації POP 3-сервер повинен підтримувати команди клієнта, наведені з їхніми розшифруваннями в табл. 1.

Таблиця 1

Команди протоколу POP3

USER	Завдання імені користувача
PASS	Завдання пароля користувача
QUIT	Завершення Tcp-З'єднання
STAT	Запит кількості повідомлень у поштовій скриньці і його розділах
LIST [ідентифікатор]	Запит ідентифікаторів поштових повідомлень і їх розмірів
RETR	Запит повідомлення із зазначеним номером
DELE	Відзначити повідомлення для видалення
NOOP	Фіктивна дія
LAST	Максимальний номер повідомлення з тих, до яких звертався клієнт
RSET	Скасування видалення повідомлення, відзначеного DELE

Приклад початку сесії протоколу POP3:
Client: USER ssau
Server: +OK User accepted
Client: PASS ssaupassword
Server: +OK Pass accepted

З метою підвищення безпеки поштових скриньок протокол POP3 підтримує передачу серверу пароля в зашифрованому вигляді. У цьому випадку для авторизації використовується команда APOP, що має два аргументи: ім'я поштового користувача й дайджест – обчислений з використанням алгоритму MD5 хеш-сума паролю й отриманої при установлені з'єднання від сервера тимчасової мітки.

2. Хід роботи

1. Ознайомтеся з інтерфейсом пошти Outlook Express.
2. Заповніть адресну книгу декількома адресами (вказані адреси отримати у викладача) для подальшого відправлення за ними поштових повідомлень.
3. Створіть декілька нових повідомлень на вільну тему та відправити їх до папки Вихідні.
4. Відправте створені повідомлення одночасно за декількома адресами.
5. Створіть нове повідомлення, вложіть в повідомлення два довільні файли, які є на вашому комп'ютері та відправити його за адресою, яку вкаже викладач.
6. Відправте створені два-три повідомлення на особисту адресу.
7. Отримайте повідомлення, які ви відправили на особисту адресу, та всі інші повідомлення, які маються у вашому поштовому “ящику”.
8. Додайте до адресної книги адреси на основі отриманих повідомлень.

3. Контрольні питання

1. Порядок запуску програми Outlook Express.
2. Порядок налагоджування програми Outlook Express.
3. Користувальницький інтерфейс пошти Outlook Express
4. Склад вікна програми.
5. Призначення складових вікна програми.
6. Інтерпретація значків із різними зображеннями конверта в області перегляду:
7. Порядок формування нового повідомлення.
8. Типи “важливості" повідомлення.
9. Як налагодити програму на термінову відправку листів?
10. Як налагодити програму на зберігання листів перед відправкою в папці Вихідні?
11. Пересилання вкладених файлів за E-mail.
12. Типи поштових папок Outlook Express.
13. Одержання вхідної пошти.
14. Адресна книга Outlook Express
15. Два шляхи поповнення адресної книги Outlook Express.
16. Додаткові можливості програми Outlook Express.

ЛАБОРАТОРНА РОБОТА 32. РОБОТА З FTP АРХІВАМИ

Мета роботи: уміти користуватися FTP архівами за допомогою утиліти FTP, браузера; їх параметрами; формувати відповідні команди; аналізувати отримані дані.

Зміст

1. Теорія
1.1. Файлові архіви і їх роль
1.2. Утиліта ftp і основні ftp-команди
1.3. Приклад використання утиліти ftp
1.4. Доступ до FTP-серверів за допомогою браузера
1.5. Пошук файлів у FTP-архівах
2. Варіанти виконання завдань.
3. Контрольні питання

1. Теорія

1.1. Файлові архіви і їх роль

Протокол передачі файлів FTP (File Transfer Protocol), який забезпечує обмін файлами між віддаленими користувачами, є одним з найстарших протоколів, що працюють у мережі Інтернет. Уперше він був описаний у специфікації в 1971 р., а остаточна на даний момент часу редакція датована 1985 роком. Усього було випущено більш 40 специфікацій, що відносяться до цього протоколу.

FTP не тільки дозволяє робити передачу файлів, але й забезпечує розмежування прав доступу користувачів до ресурсів. Файлові архіви Internet називають ще FTP-архівами за іменем протоколу обміну інформацією – File Transfer Protocol. Цей протокол дозволяє передавати двоїчні файли, тобто файли довільних типів, а не тільки текстові. FTP-архіви спочатку створювалися для обміну і збереження стандартів мережі (так називаних документів RFC– Request for Comments) і програмного забезпечення. Але згодом вони перетворилися у величезні багатопрофільні сховища даних.

До винайдення World Wide Web, FTP-сервери були єдиним засобом передачі найрізноманітнішої інформації – безкоштовного і умовно безкоштовного програмного забезпечення, драйверів, утиліт, графічних файлів та інших. На сьогодні їх роль є допоміжною і найчастіше використовуються компаніями для розповсюдження свого програмного забезпечення.

Для доступу до FTP-архівів потрібно мати вхідне ім'я і знати відповідний пароль. Користувачу дається можливість переглядати каталоги архіву, виконувати пошук файлів, пересилати як файли, так і їх групи, а також каталоги разом з усіма вкладеними на будь-яку глибину підкаталогами. Існує особливий підвид FTP-архівів, називаних анонімними. Анонімність полягає в тому, що для роботи з такими файловими архівами можна зареєструватися під ім'ям **anonymous** і вказати замість пароля свою поштову адресу.Як правило, файли, що доступні при анонімній реєстрації, розміщуються в підкаталогах спеціального каталогу /PUB, тому більшість URL закінчуються цим каталогом. Для пошуку і надання інформації про розташування загальнодоступних файлів на анонімних FTP-архівах існує спеціальна система Archie. Ця система регулярно збирає з анонімних FTP-архівів інформацію про файли, що містяться в них, (списки каталогів, списки файлів за каталогами, а також файли їхніх описів) і дозволяє робити пошук за назвами файлів або каталогів і за описовими файлами, а саме – за словами, що містяться в них. При зверненні до Archie можна, наприклад, зазначити ім'я файлу або шаблон для пошуку й одержати у відповідь список анонімних архівів, в яких такі файли знаходяться, з вказівкою шляху доступу до самих файлів; або ж шукати файли за значеними словами, що містяться в їх стислому описі.

1.2. Утиліта FTP і основні FTP-команди

До складу операційної системи для доступу до FTP-серверів включена комунікаційна утиліта ftp.exe. Запускається утиліта з командного рядка. Зразу після її

запуску утворюється тимчасове середовище, в якому підтримуються ftp-команди. Ознакою середовища ftp є те, що запрошення командного рядка приймає вигляд ftp>. Повернутися в командний рядок можна за допомогою команди quit.

В середовищі ftp доступне використання ftp-команд. Щоб отримати список всіх ftp-команд, достатньо ввести у відповідь на запрошення команду help або ?. Для отримання довідки про призначення конкретної команди використовується такий синтаксис: help <ім'я_команди> або ?<ім'я_ команди>.

Найчастіше використовуються такі ftp-команди (табл. 1,2):

Таблиця 1

Деякі команди утиліти ftp

Команда	**Параметри**	**Опис**
ascii		Перемкнутися в режим передавання текстових файлів
binary		Перемкнутися в режим передавання двійкових файлів
cd	ім'я каталогу	Змінити робочий каталог на віддаленій ЕОМ
close		Закрити з'єднання з віддаленою ЕОМ
del	ім'я файлу	Видалити файл на віддаленій ЕОМ
dir	маска файлів	Відобразити вміст поточного каталогу серверу
get	ім'я файлу	Одержати файл з віддаленої ЕОМ
hash	on/off	Увімкнути або вимкнути режим знаку "#" для кожного переданого блоку даних при передаванні файлів
help		Одержати підказку
lcd	ім'я каталогу	Змінити робочий каталог на локальній ЕОМ
mget	маска файлів	Одержати декілька файлів з віддаленої ЕОМ
mput	маска файлів	Відправити декілька файлів на віддалену ЕОМ
open	адреса ЕОМ	Встановити з'єднання з вказаною ЕОМ
put	ім'я файлу	Передати файл на віддалену ЕОМ
pwd		Вивести ім'я поточного каталогу
quote	команда	Передати команду безпосередньо FTP (для введення команд адміністратора)
quit		Завершити роботу з утилітою

Таблиця 2

Команди необхідні для забезпечення процесу копіювання файлів

open ім'я_сервера – відкрити з'єднання	відкриває з'єднання з сервером. Це ім'я можна вказати відразу при введенні команди, що завантажує клієнта
cd ім'я_директорії – змінити каталог	здійснює перехід в інший робочий каталог на FTP-сервері
dir [ім'я_файлу] – видати список файлів	видає список файлів в поточній директорії. Не забувайте, що можна використовувати шаблони групових операцій
get ім'я_файлу [ім'я_локального_файлу] – переписати файл	переписує файл з віддаленого комп'ютера на локальний. Якщо вказано ім'я локального файлу, то записує його під цим ім'ям, інакше – в каталог
mget [ім'я_файлу] – переписати групу файлів	те ж саме, що і get, але дозволяється використовувати шаблони. Перед копіюванням кожного файлу запрошуватиметься підтвердження. Для відміни підтверджень введіть prompt
prompt	відміняє підтвердження в командах mget і mput
put ім'я_файлу [ім'я_віддаленого_файлу] – записати файл на сервер	переписує файл з локального комп'ютера на віддалений під ім'ям *ім'я_віддаленого_файлу*. Якщо воно не вказане, то файл записується в поточний каталог з ім'ям локального файлу. Команда заборонена для анонімних користувачів

mput [ім'я_файлу] – записати групу файлів	те ж саме, що і put, але дозволяється використовувати шаблони. Перед записом кожного файлу запрошуватиметься підтвердження
ascii	встановлює ascii-спосіб передавання файлів. Використовується для пересилання файлів-текстів англійською мовою. Проте для надійності краще використовувати binary
binary	встановлює двійковий спосіб пересилання файлів. При цьому файл при передавання не перекодовується і записується в незміненому вигляді. Це найнадійніший спосіб передавання файлів
close	закриває з'єднання з даним сервером і проводить повернення в командний режим. Ця команда автоматично виконується при виході з FTP-клієнта.
quit	вихід з FTP-клієнта
user	реєструє на поточному сервері користувача з новим ім'ям. Використовуйте цю команду, якщо перший раз помилково неправильно ввели ім'я анонімного користувача і не хочете знову перенабирати команду open
lcd [ім'я_каталогу]	здійснює перехід на локальному комп'ютері у вказаний каталог
pwd	виводить на екран поточний каталог на віддаленому комп'ютері
system	виводить на екран тип операційної системи на віддаленому комп'ютері
help [FTP-команда] – допомога	видає коротку інформацію про команди FTP-клієнта або про конкретну команду

Щоб за допомогою ftp-команд виконати копіювання файлу з FTP-сервера, необхідно:

- Відкрити з'єднання з сервером (open <ім'я_сервера>).
- Зареєструватися на сервері (для анонімної роботи – під ім'ям **anonymous** і замість пароля вказати свою поштову адресу).
- Встановити спосіб передачі файлів (як правило – **binary**).
- Перейти у потрібний каталог (**cd <ім'я_каталогу**>).
- Вказати файл для передачі на локальний комп'ютер (**get <ім'я_файлу>**).
- Закрити з'єднання з сервером (**close або quit**).

1.3. Приклад використання утиліти FTP

В якості приклада розглянемо, як за допомогою утиліти завантажити zip-архів для установки одного з популярних FTP-клієнтів – WS_FTP, який можна знайти за адресою: **ftp://ftp.ipswitch.com/ipswitch/product_downloads /ws_ftple.zip.**

1. Відкрийте вікно командного рядка (**Пуск- Программы- Стандартные- Командная строка**).
2. У відповідь на запрошення командного рядка введіть ім'я утиліти – **ftp.**
3. Після появи запрошення ftp> відкрийте з'єднання з сервером ftp.ipswitch.com , ввівши команду: **open ftp.ipswitch.com** .
4. Після появи запрошення **User** (ftp.ipswitch.com: (none)): введіть для анонімного доступу ім'я **anonymous**.
5. На запит **Password**: введіть свій **E-mail** (він не буде виводитись на екран).
6. Перейдіть у каталог, в якому зберігається потрібний файл: **cd\ipswitch\product_downloads.**
7. Встановіть двоїчний спосіб передачі файлів за допомогою команди **binary.**

8. Введіть команду для копіювання файлу з сервера: **getws_ftple.zip.**

9. Зачекайте, поки процес копіювання завершиться і з'явиться відповідне повідомлення (“**Transfer complete…**”).

10. Завершіть сеанс з'єднання за допомогою команди **quit**.

11. Перевірте (наприклад, за допомогою команди **dir**), що файл **ws_ftple.zip** скопійований в поточний каталог.

Нижче наведений приклад установлення з'єднання (анонімним користувачем), запиту підтримуваних сервером команд і закриття з'єднання.

```
220 Proftpd 1.3.0a Server [89.186.244.16]
USER anonymous
331 Anonymous login ok, send your complete email address as your password.
PASS anonymous@my.mail
230-welcome to Samara State Aerospace Univercity FTP Server
230 Anonymous access granted, restrictions apply.
HELP
214-the following commands are recognized (* =>'s unimple-mented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
XRMD MKD XMKD PWD XPWD SIZE SYST HELP
NOOP FEAT OPTS AUTH CCC* CONF* ENC* MIC*
PBSZ PROT TYPE STRU MODE RETR STOR STOU
APPE REST ABOR USER PASS ACCT* REIN* LIST
214 Direct comments to root@web.ssau.ru
QUIT
221
```

Goodbye.

1.4. Доступ до FTP-серверів за допомогою браузера

Браузер також можна використовувати в якості FTP-клієнта для роботи з файловими архівами. URL-адреса для FTP-серверу в загальному випадку виглядає так:
ftp://<user>:<password>@<host>/<url-path>,
де <user> – ім'я користувача, <password> – його пароль, <host> – доменне ім'я або IP-адреса серверу, <url-path> – шлях до файлу.

На практиці найбільш часто використовуваним варіантом FTP є анонімний. Для доступу до анонімних FTP-серверів може використовуватися спрощений формат URL-адреси:
ftp://<host>/<url-path>.

Так, наприклад, до деяких найбільш великих анонімних архівів можна звернутися за адресами:

204.209.81.178	00002. awe3.iserver.net	00003. ftp.veracomp.com.pl
00004. download.canon.jp	00005. 204.209.81.97	00006. ftp.figlet.org
00007. tenzor.kmail.ru	00008. 85.128.139.67	00009. 66.39.177.3
00010. ftp.algo-hk.cz	00011. ftp.rahul.net	00012. uhp.com
00013. ice.spb.ru	00014. 192.53.187.171	00015. ftp.univie.ac.at
00016. index.storsys.ibm.co...	00017. ftp.vline.pl	00018. ftp.rsu.ru
00019. ftp.futurenet.co.uk	00020. ftp.eng.buffalo.edu	00021. www.multicom.bg
00022. ftp.f-secure.com	00023. ftp.vdraw.com	00024. relay.fidonet.org.ua
00025. es-designs.com	00026. ftp.tridia.com	00027. news.fido7.ru
00028. ftp.deepspace6.net	00029. portret.tomsk.ru	00030. www.infinisys.co.jp
00031. ftp.sk.debian.org	00032. ftp.dlink.eu	00033. 216.71.51.54
00034. ftp.virgilio.it	00035. ftp.alsa-project.org	00036. ftp.wave.net
00037. ftp.rec.org	00038. ftp.igh.cnrs.fr	00039. www.thetargetgroup.c...
00040. ftp.eecs.harvard.edu	00041. 93.190.206.160	00042. ftp.icsi.berkeley.ed...
00043. uvp.com	00044. 220.130.112.225	00045. ftp.skynet.lt
00046. ftp.vtc.ru	00047. 195.184.195.199	00048. 212.85.100.216

00049. ftp.euroweb.hu	00050. sunsite.univie.ac.at	00051. ftp2.jacobs.com
00052. ftp.wavesurgeon.com	00053. ns.isan.troitsk.ru	00054. ftp.umontreal.ca
00055. ftp.volmed.org.ru	00056. ftp.exler.ru	00057. ftp.north.ad.jp
00058. freepascal.stack.nl	00059. patches.ubi.com	00060. gloria.pskovenergo.r...
00061. rabbit.corbina.net	00062. cmp.felk.cvut.cz	00063. ftp.rz.uni-frankfurt...
00064. ftp.muc.de	00065. ftp.sys.toronto.edu	00066. 90.188.30.72
00067. ftp.iem.ac.ru	00068. 62.76.7.10	00069. nlmpubs.nlm.nih.gov
00070. ftp.suncity.net.tw	00071. 15.216.110.139	00072. linst.bu.edu
00073. mail.rax.ru	00074. ftp.esd.ornl.gov	00075. ftp.cs.wisc.edu
00076. ftp.franken.de	00077. ns.depfin.vologda.ru	00078. ftp.princeton.edu
00079. ftp.fftw.org	00080. www.lanet.lv	00081. ftp.perftech.com

Якщо доменне ім'я сервера починається з ftp, то в адресний рядок необов'язково вводити частину URL-адреса з назвою протоколу – ftp:// . Наприклад, замість повної URL-адреси ftp://ftp.elvis.ru достатньо ввести ftp.elvis.ru. Після встановлення зв'язку файли і каталоги серверу відображаються в вікні браузера у вигляді гіперпосилань. Піктограми у вигляді папок представляють собою каталоги, у вигляді листів – файли. Поруч із кожним із них виводяться ім'я, розмір (для файлу), дата і час створення.

Відкриття каталогу здійснюється при виборі посилання на нього. При цьому відкривається Web-сторінка, яка відображає вміст каталогу. Часто на ній розміщується спеціальне посилання “Up to Higher Level” (на один рівень вверх) – для переміщення в сторону кореня файлової структури сервера. При виборі посилання на файл спочатку здійснюється спроба його відкриття за допомогою відповідної програми перегляду, а якщо така програма відсутня – видається запрошення зберегти файл на жорсткому диску. Використання браузера для роботи з FTP-архівами можна рекомендувати в тому випадку, коли необхідно скопіювати невелику кількість незначних за розміром файлів. Справа в тому, що при використанні браузера кожного разу при зверненні до сервера виконується авторизація користувача, а це може значно збільшити час, необхідний для завантаження файлів. До того ж швидкість завантаження буде меншою, чим при використанні ftp-клієнта, оскільки використовується не FTP–, а HTTP–протокол, який гірше пристосований для передачі файлів.

1.5. Пошук файлів у FTP-Архівах

Спеціалізованою системою для пошуку файлів у FTP-архівах є Archie. Archie-сервер періодично звертається до усіх відомих йому FTP-архівів і створює список наявних на них файлів. Кожний такий сервер будує базу даних цих файлів. При зверненні до Archie-серверу виконується пошук інформації щодо файлу у базі даних і користувачу повертається список серверів, що мають файл з таким ім'ям.

Браузер безпосередньо не підтримує роботу з Archie-серверами (див. додаток 4). Проте існують десятки Web-серверів, що надають користувачу інтерфейс для виконання Archie-пошуку за допомогою браузера. До деяких з них можна звернутись, наприклад, за адресами:

- http://archie.icm.edu.pl/archie-adv_eng.html;
- http://elfikom.physik.uni-oldenburg.de/Docs/net-serv/archie-gate.html;
- http://www.lanet.lv/services/archieplex/doc/form.html;

Для виконання пошуку користувачу пропонуються форми, що містять поля, кнопки, перемикачі опцій і т.п. У найпростішому випадку для виконання пошуку достатньо в поле для пошуку ввести ім'я файлу або його частину. При необхідності у формі можна зазначити додаткові опції, щоб визначати вигляд пошуку, сортування результату, домен для пошуку й т.ін.

Archie-сервери є дуже завантаженими і тому не завжди можна отримати від них в відповідь інтерактивному режимі.

Поступово Archie-сервери втрачають своє значення, а їхні функції все частіше переходять до спеціалізованих пошукових систем для пошуку в файлових архівах:

- FtpSearch (http://www.ftpsearch.net);
- Files.ru (http://www.files.ru);
- FileSearh.ru (http://www.filesearch.ru).

Відмінність їх від звичайних пошукових систем WWW полягає в тому, що пошук здійснюється не за змістом Web-сторінок, а за іменами самих файлів і каталогів. До того ж такі системи створюються таким чином, щоб оптимізувати пошук певних типів файлів, зокрема, зображень, звукових файлів, відеороликів.

При зверненні до таких систем теж відкривається форма (схожа на Archie), в якій визначаються критерії пошуку. В найпростішому випадку для виконання пошуку достатньо вказати тільки ім'я файлу, але при необхідності можна задати і більш складні критерії.

2. Варіанти виконання завдань.

Номер варіанту завдання вибирається за першою літерою прізвища студента:

Перша літера прізвища	Номер варіанту
А, Б, В, Г, Д,Е, Є ,Ж	**1**
З, І, Й,К, Л, М,Н,О	**2**
П, Р, С, Т, У,Ф, Х,	**3**
Ц, Ч, Ш, Щ, Ї, Ю, Я	**4**

Варіант 1

1) Відкрийте вікно командного рядка (**Пуск-Программы-Стандартные-Командная строка**) і за допомогою команд операційної системи перейдіть у свій персональний каталог.
2) В умовах локальної мережі, використовуючи утиліту **ftp.exe**, підключіться до сервера ftp://ftp.ncren.net.
3) Скопіюйте до свого персонального каталогу файл стандартів Internet.
4) Виконайте індивідуальне завдання, використовуючи ftp-команди.
5) За допомогою браузера Internet Explorer зверніться до FTP-сервера ftp://ftp.ncren.net.
6) Перейдіть в каталог RFC – в ньому містяться RFC-документи щодо стандартів Internet.
7) В каталозі RFC відшукайте текстовий файл rfc-index-latest.txt з переліком найостанніших стандартів і збережіть його у своїй персональній папці.
8) Перегляньте збережений файл і визначте номер XXXX останнього RFC-документа в цьому переліку.
9) Введіть в адресний рядок URL-адресу ftp://ftp.ncren.net/rfc/rfcXXXX.txt, де XXXX номер RFC-документу, щоб отримати останній з RFC-документів у вигляді текстового файлу. Збережіть файл у своїй персональній папці.
10) З каталогу RFC перейдіть перейдіть у підкаталог PDF-RFC, в якому зберігаються RFC-документів у форматі PDF – зручному компактному форматі для обміну електронними документами.
11) Завантажте до своєї персональної папки архівний файл rfc901.pdf.Z з RFC-документом у форматі PDF щодо офіційних ARPA- та INTERNET-протоколів.
12) Розархівуйте збережений архівний файл (наприклад, за допомогою WinZip), щоб отримати документ в PDF-форматі. Для перегляду файлів у такому форматі найчастіше використовується така популярна програма-переглядач, як Adobe Acrobat Reader.
13) Відшукайте для завантаження дистрибутив програми. Для цього виходячи з припущення, що він розміщується у каталозі Acrobat, за допомогою пошукової системи FileSearh.ru (http://www.filesearch.ru) виконайте пошук серверів, що містять каталог Acrobat.
14) Перейдіть у один з них, наприклад, ftp://ftp.ipswitch.com/ipswitch/Acrobat/ і завантажте дистрибутив програми Adobe Acrobat Reader.

15) З дозволу викладача виконайте установку програми Adobe Acrobat Reader для перегляду файлів у PDF-форматі, якщо вона ще не встановлювалась.
16) Ознайомтесь з документом rfc901.pdf, використавши для його перегляду Adobe Acrobat Reader.

Варіант 2

1) Відкрийте вікно командного рядка (**Пуск-Программы-Стандартные-Командная строка**).
2) В умовах локальної мережі, використовуючи утиліту **ftp.exe**, підключіться до www.filesearch.ru
3) За допомогою команд операційної системи завантажте один зі знайдених файлів
4) Виконайте індивідуальне завдання, використовуючи ftp-команди.
5) За допомогою браузера Internet Explorer зверніться до пошукової системи FileSearh.ru (http://www.filesearch.ru).
6) Виконайте пошук (простий) музичних композицій групи Beatles. Для цього в якості типу файлів виберіть MP3 і вкажіть ключове слово для пошуку –beatles.
7) Завантажте один зі знайдених файлів (наприклад, Beatles__She_Loves_You.mp3) до своєї персональної папки.
8) Перейдіть на сторінку розширеного пошуку і виконайте пошук графічних зображень групи (за ключовим словом beatles), розмір яких не перевищує 50К.
9) Перегляньте знайдені графічні зображення і кілька з них (3-5) збережіть у своїй персональній папці.
10) Використовуючи сторінку розширеного пошуку, за тим же ключовим словом beatles виконайте пошук відео-файлів, упорядкувавши їх за розміром файлів.
11) Оцініть час, необхідний для завантаження одного з знайдених відео-файлів на локальну машину (але не завантажуйте сам файл, бо цей процес може виявитись досить тривалим!).
12) За допомогою браузера зверніться до файлового архіву умовно-безкоштовного програмного забезпечення ftp://ftp.sigma-soft.ru.
13) Перейдіть в каталог pub/shareware/WinZip з дистрибутивами популярного архіватора WinZip.
14) Завантажте з останню версію архіватора у свою персональну папку WinZip.
15) З дозволу та під наглядом викладача виконайте установку програми WinZip, якщо вона ще не встановлювалась.
16) За допомогою WinZip стисніть завантажені раніше (п.7,9) файли у форматі MP3 і JPG, GIF. Порівняйте розміри архівних файлів з розмірами вихідних файлів і зробіть висновок, чому файли у форматі MP3 і JPG, GIF поширюються нестисненими.

Варіант 3

1) Відкрийте вікно командного рядка (**Пуск-Программы-Стандартные-Командная строка**) і за допомогою команд операційної системи перейдіть у свій персональний каталог.
2) В умовах локальної мережі, використовуючи утиліту ftp.exe, підключіться до http://archie.icm.edu.pl/archie-adv_eng.html.
3) Скопіюйте до свого персонального каталогу файл.
4) Виконайте індивідуальне завдання, використовуючи ftp-команди.
5) За допомогою браузера Internet Explorer зверніться до сторінки з Archie-формою за адресою http://archie.icm.edu.pl/archie-adv_eng.html.
6) Відкрийте сторінку допомоги з використання Archie, скориставшись посиланням Help внизу форми.
7) Ознайомтесь з правилами користування системою і збережіть файл допомоги у своїй персональній папці.
8) За допомогою Archie-форми виконайте пошук дистрибутива одного з найбільш популярних ftp-клієнтів – WS_FTP. Для цього задайте такі умови пошуку, за якими будуть шукатись файли, в назвах яких зустрічається рядок ws_ftp.

9) Збережіть результати пошуку у вигляді текстового файлу у своєму персональному каталозі.
10) Використовуючи пошукову панель браузера, зверніться до однієї з пошукових систем загального призначення (наприклад, Яndex) і виконайте з її допомогою пошук дистрибутиву програми WS_FTP.
11) Зафіксуйте кроки, які довелося виконати, щоб дістатися дистрибутива WS_FTP і завантажити його. Зробіть висновки щодо доцільності використання для пошуку файлів пошукових систем загального призначення.
12) Завантажте знайдений дистрибутив програми WS_FTP у свою персональну папку. Зверніть увагу, що завантаження відбувається знову ж таки з FTP-сервера; зафіксуйте його ім'я.
13) З дозволу викладача встановіть програму WS_FTP на локальну машину.
14) Ознайомтесь з вбудованою довідкою щодо користування програмою WS_FTP, (команда Help-Help Topics) або скористайтесь інтерактивним підручником (команда Help-Tutorials…).
15) Зробіть висновки щодо зручності і доцільності використання FTP-клієнта, яким є WS_FTP.

Варіант 4

1) Відкрийте вікно командного рядка (**Пуск-Программы-Стандартные-Командная строка**) і за допомогою команд операційної системи перейдіть у свій персональний каталог.
2) В умовах локальної мережі, використовуючи утиліту ftp.exe, підключіться до сервера ftp://ftp.nic.it.
3) Скопіюйте до свого персонального каталогу файл.
4) Виконайте індивідуальне завдання, використовуючи ftp-команди.
5) За допомогою браузер Internet Explorer зверніться до FTP-сервера організації Network Information Center (NIC) – ftp://ftp.nic.it.
6) Перейдіть в каталог RFC, в якому містяться RFC-документи щодо стандартів Internet.
7) В каталозі RFC відшукайте текстовий файл rfc-retrieval.txt з інформацією про те, які існують можливості для отримання RFC-документів, і збережіть його у своїй персональній папці.
8) Уважно ознайомтесь з файлом rfc-retrieval.txt і зверніть увагу на те, що RFC-документи можна отримувати не тільки з FTP-серверів, але й за електронною поштою (Via e-mail). Скористайтесь цією можливістю, щоб отримати RFC- документ 1738 (файл rfc1738.txt) з вимогами стандарту до URL-адрес
9) В каталозі RFC відшукайте текстовий файл rfc-index.txt з коротким описом всіх RFC-документів, і збережіть його у своїй персональній папці. Даний файл має значні розміри (більше 0,5 М) і тому завантажується досить довго.
10) В каталозі RFC відшукайте текстовий файл rfc-index-latest.txt і збережіть його у своїй персональній папці. Цей файл має таку ж структуру, що й rfc-index.txt, але містить список тільки останніх RFC-документів. Тому його розміри значно менші (близько 4 К) і завантажується він значно швидше.
11) Перегляньте файл rfc-index-latest.txt і зверніть увагу на RFC-документ 3572 з інформацією щодо новітньої версії IP- протоколу V6.
12) Введіть в адресний рядок URL-адресу ftp://ftp.ncren.net/rfc/rfc3572.txt, щоб завантажити цей документ. Ознайомтесь з ним.
13) Зверніться до пошукової системи FtpSearch (http://www.ftpsearch.net) і виконайте пошук документа 3572 у форматі PDF – зручному компактному форматі для обміну електронними документами. Для цього в рядку пошуку вкажіть шаблон rfc3572*.pdf.
14) Завантажте знайдений RFC-документ 3572 у PDF-форматі і скористайтесь програмою Adobe Acrobat Reader для його перегляду.

15) Якщо програма Adobe Acrobat Reader на вашій машині не встановлена , її дистрибутив можна завантажити, наприклад, з ftp://ftp.ipswitch.com/ipswitch/Acrobat/. Установка програми виконується з дозволу і під наглядом викладача.

3. Контрольні питання

1. Файлові архіви і їх роль
2. Утиліта ftp її призначення, особливості
3. Основні ftp-команди
4. Доступ до FTP-серверів за допомогою браузера
5. Призначення Archie-серверів

ЛАБОРАТОРНА РОБОТА 33.
ЗАКАЧУВАННЯ ФАЙЛІВ ЗА ДОПОМОГОЮ ПРОГРАМ TELEPORT PRO ТА FLASHGET

Мета роботи: уміти користуватися програмами Teleport Pro та FlashGet їх параметрами; формувати відповідні команди; аналізувати отримані дані.

Зміст

1. Теорія
1.1. Закачування файлів за допомогою програми Teleport Pro
1.2. Створення нового проекту
1.3. Збереження проекту
1.4. Запуск проекту
1.5. Перегляд результатів
1.6. Налагоджування параметрів проекту
1.7. Закачування файлів за допомогою програми FlashGet
1.8. Головне меню програми FlashGet
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Закачування файлів за допомогою програми Teleport Pro

Teleport Pro – це переглядач offline, має можливість віддзеркалювання вузла, автоматизований інструмент в Інтернеті, багатопотоковий web-павук. Він дозволяє повністю завантажити на комп'ютер весь web-вузол (з усіма каталогами, файлами та їх зв'язками), указані файли разом з їх зв'язками, або окремі файли при високих швидкостях виконання.

Програма дозволяє проводити пошук файлів та web-вузлів (можна задати глибину пошуку) за визначеними параметрами (назва, розширення, зміст, розмір, дата створення, тип зв'язків і т.п.).

Для використання teleport Pro, необхідно створити проектний файл, який містить один або більше звернення до файлів в Інтернеті, надати програмі деякі правила, які визначають які зв'язки треба відслідковувати і які файли відновлювати. Далі необхідно посилати павука з його місією за допомогою вибору **Стартової команди** в меню **Файл**, або **Стартової кнопки** на панелі інструментів. Одного разу активізований, teleport-павук прочитає ваш проект запуску адреси і відновить будь-які файли, які знайде там, потім прочитає всі зв'язки на сторінці, прослідує за тими зв'язками, одержить файли на тих сторінках, і т. д.

Teleport Pro використовує спеціальний пошуковий алгоритм, щоб швидко шукати мережеві сторінки, ідентифікувати й класифікувати їх зв'язки, а потім відновлювати всі відповідні типи файлів, які конкретизовані у вікні **Проектних Властивостей**.

Teleport Pro починає роботу із запуску адреси, він пам'ятає, що і де було, тому ніколи не відвідує того ж місця двічі, у межах того ж проектного сеансу. Можливе блокування користувачем відвідування якогось сайту.

Є чотири істотних кроки до запуску teleport Pro на виконання завдання:

1. Створення нового проекту.
2. Збереження проекту.
3. Запуск проекту.
4. Перегляд результатів.

1.2. Створення нового проекту

Щоб створити новий проект, треба ввести команду **Новый Проект** із меню **Файл**, або натиснути кнопку на панелі інструментів **Новый Проект** (досвідчений користувач

може почати створювати новий проект із нуля, однак при цьому доведеться встановити й проектні властивості вручну).

Майстер нового проекту, який викликається командою **Мастер Нового Проекта** з меню **Файл** (рис. 1) за декілька кроків дозволить відібрати вказані властивості та автоматизує процес створення проекту.

Якщо вибрана можливість **Копировать вебсайт на диск проекта**, то на другому кроці роботи майстра (рис. 2) треба ввести адресу та ввести глибину пошуку. На третьому кроці (рис. 3) вибираються типи файлів та, за необхідності, вводиться пароль (необов'язково). Четвертий крок – заключний, тут підтверджується проект уведенням команди Finish. Після цього у вікні програми (рис. 4) з'явиться адреса проекту, якщо проектів декілька – список адрес.

Примітка: під час указаної роботи програма може дослідити тільки типи файлів за адресами HTTP і FTP.

Якщо вибрати команду **Копировать Web-сайт со структурой каталогов** (рис. 1), то на комп'ютері зберігається копія сайту з деревом каталогів, зв'язками і т.п. Уся подальша робота аналогічна вищеописаній.

Команда **Поиск файлов определенного типа** (рис. 5) дозволяє створити проект для проведення пошуку файлів визначеного типу в мережі Internet. Відбір файлів проводиться в третьому вікні майстра. Для вказівки типів файлів, які буде шукати програма, можна використовувати наступні групові імена: наприклад, *.cgi – відповідає будь-якому файлу, що має розширення cgi; bob* – boba.jpg, або навіть bobble; ???.jpg – star005.jpg або starting.jpg, але не star.jpg або starry.jpg.

Команда **Исследовать ссылку из сайта** використовується в тому випадку, якщо необхідно створити проект для дослідження видів файлів, які містяться на сайтах, куди є посилання із сайту, який досліджується. При цьому проводиться зберігання не змісту файлів, а посилання на них, тобто ярликів. Це дозволяє економити час обстеження сайтів.

Команда **Получить несколько файлов из адресов** дозволяє створити проект для дослідження наявності потрібних файлів за списком адрес.

Команда **Поиск за ключевыми словамы** дозволяє створити проект для пошуку та збереження інформації за ключовими словами, які вносяться в третьому вікні майстра проекту (рис. 2-5).

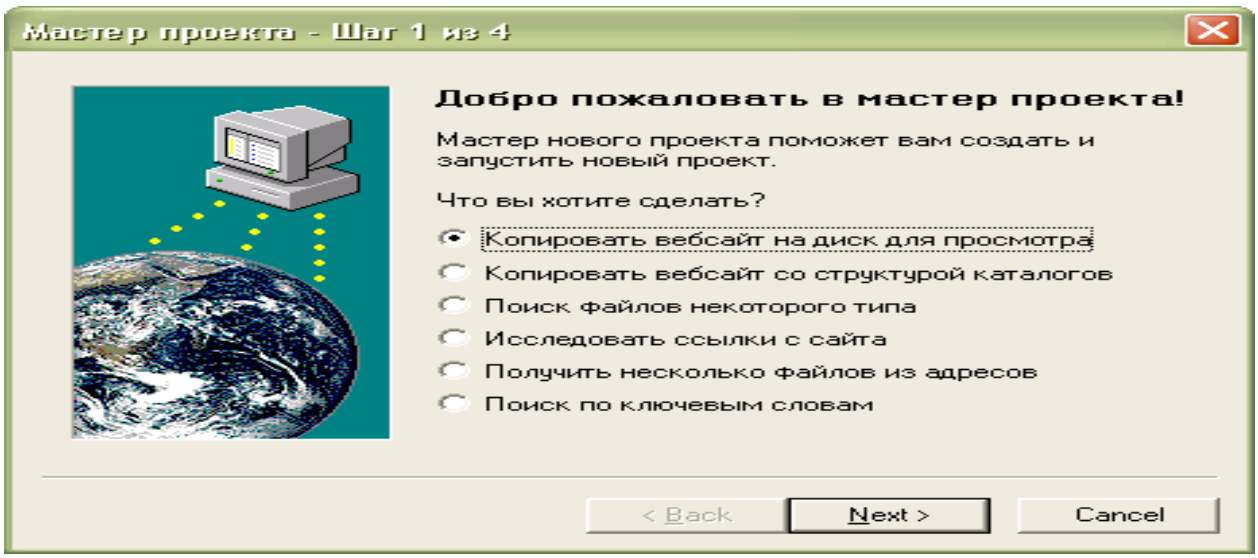


Рис. 1. Вікно майстра створення проекту

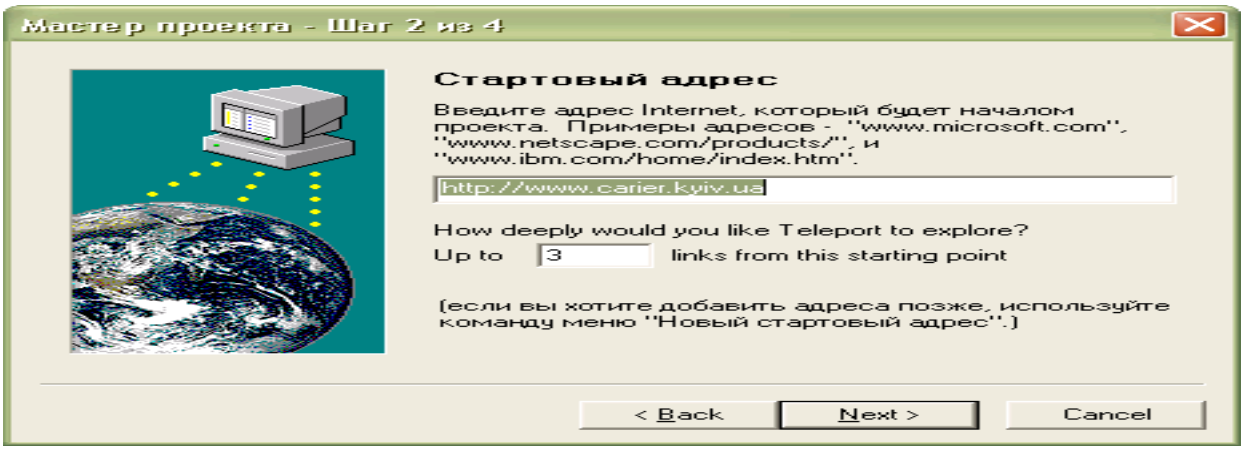


Рис. 2. Вікно введення адреси

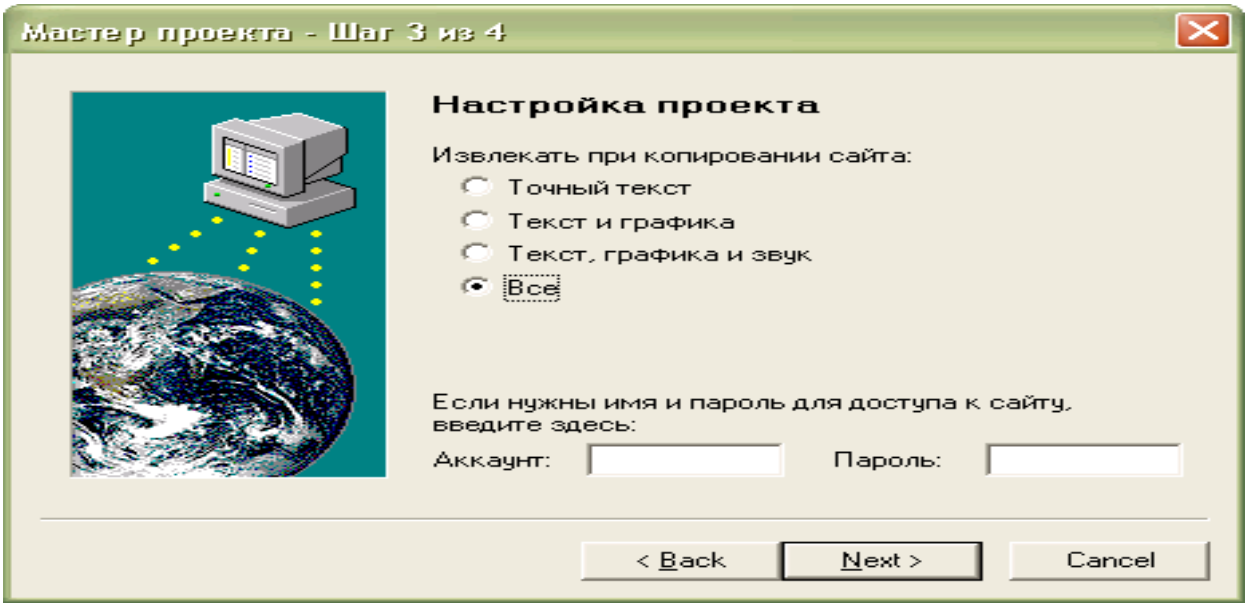


Рис. 3 Вікно третього кроку роботи майстра

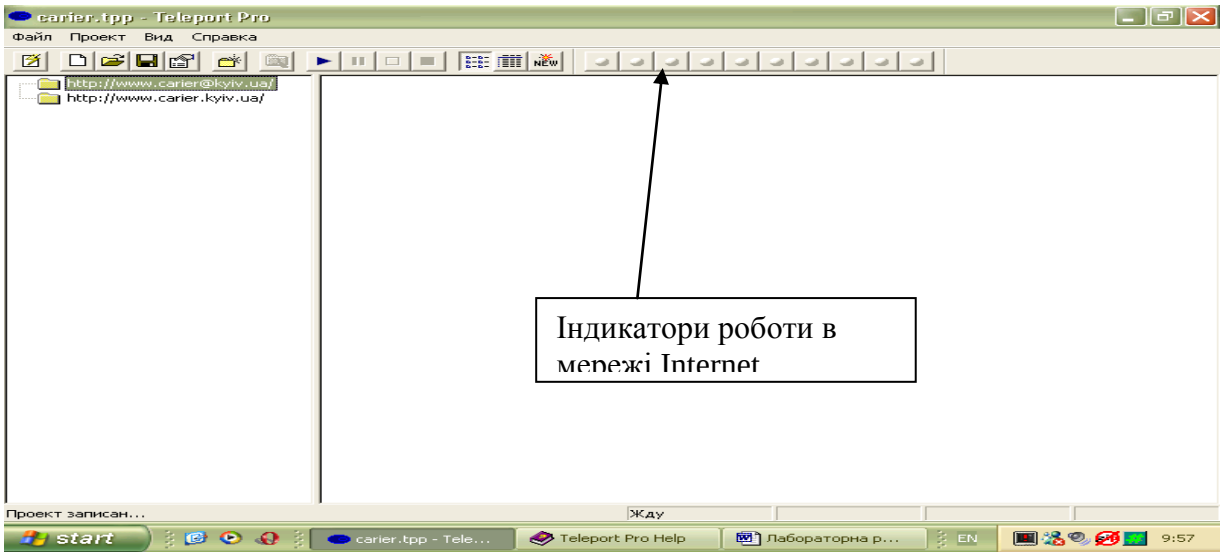


Рис. 4 Вікно програми зі списком адрес

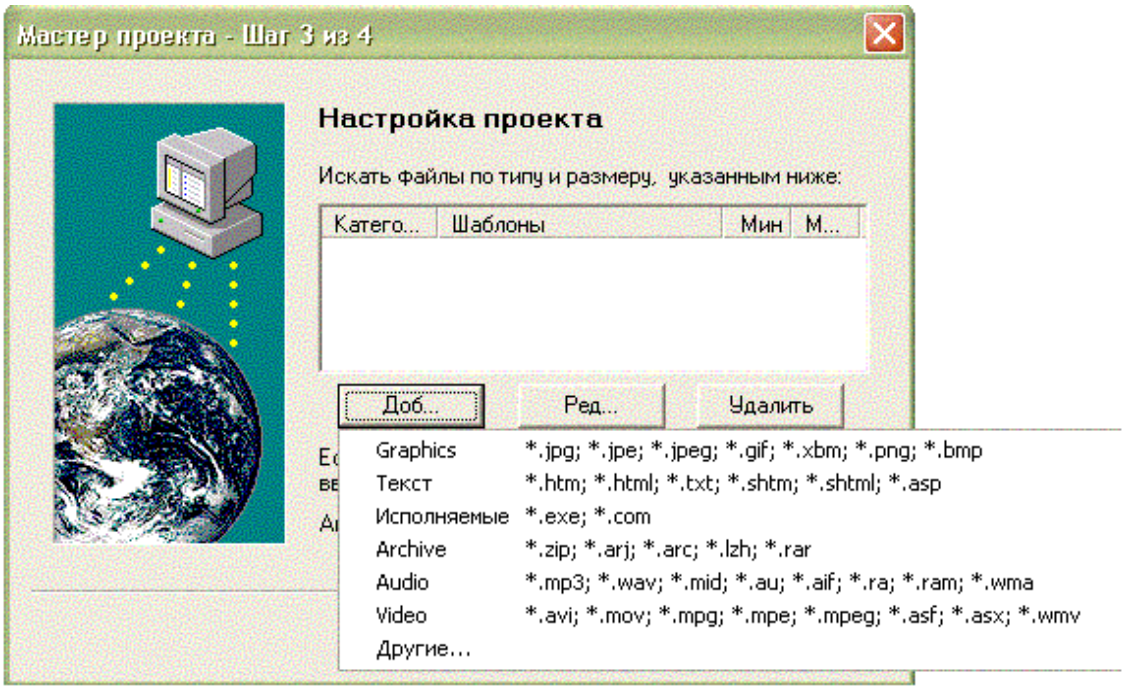


Рис. 5. Вікно відбору типів файлів

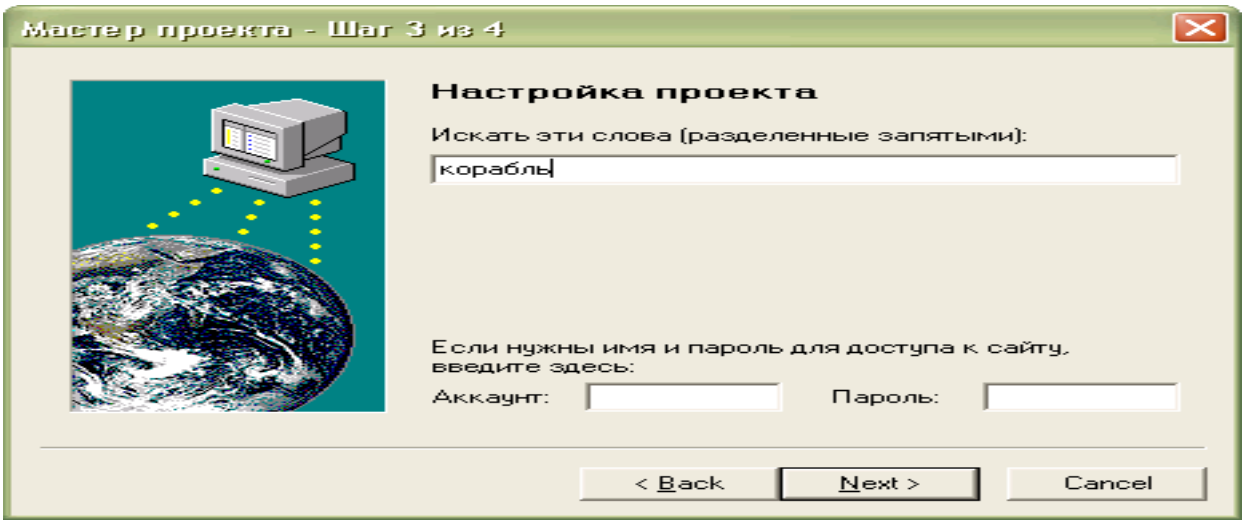


Рис. 6. Вікно введення ключових слів

1.3. Збереження проекту

При завершенні роботи з **майстром створення проекту** автоматично після введення команди Finish з'являється діалогове вікно збереження проекту (рис. 6). Треба звернути увагу на те, що розширення файлу, у якому буде зберігатися вміст проекту – .tpp.

Якщо майстер не використовувався при побудові проекту, то для його збереження необхідно вибрати команду **Сохранить проект**, або **Сохранить проект как** із меню **Файл**. Потім указати диск та теку, де будете зберігати проект. Програма може при збереженні файлів в одній теці їх перейменовувати, щоб не допустити колізії при однакових іменах. Найшвидше збереження файлів буде при зберіганні «плоскої» копії Web-вузла, тобто без урахування зв'язків та глибини.

1.4. Запуск проекту

Запуск проекту проводиться командою **Старт** із меню **Проект**, або натискуванням стартової кнопки на панелі інструментів. Після введення команди програма автоматично з'єднується за вказаною адресою через мережу Internet (з'єднання з Internet запускається програмою автоматично, якщо введені всі параметри, які дозволяють працювати в мережі).

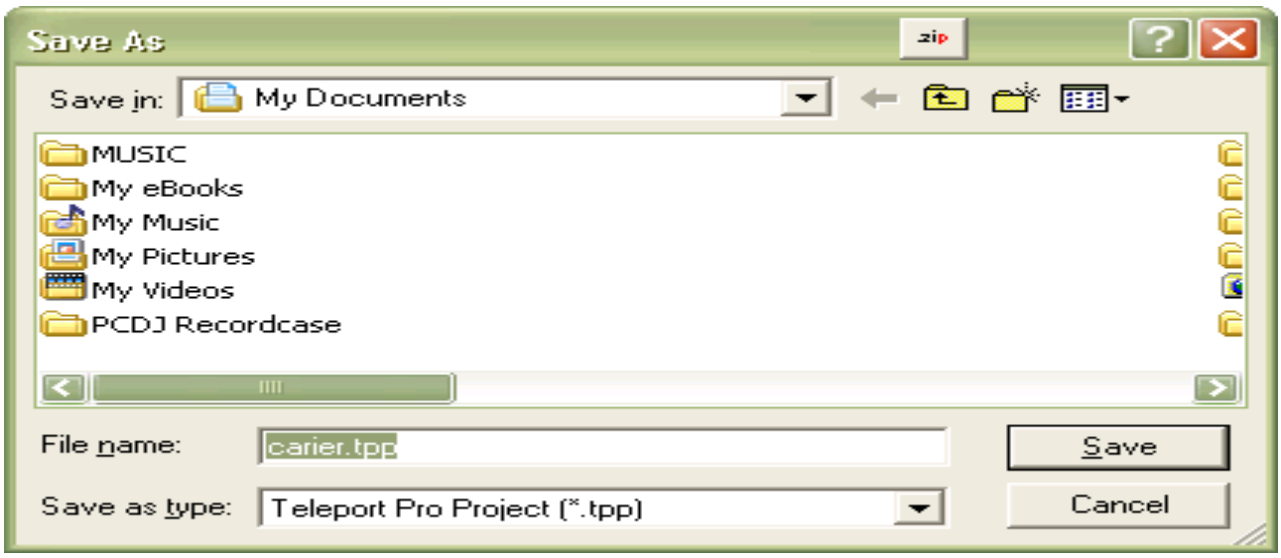


Рис. 6. Вікно збереження проекту

Індикатори програми (рис. 7) сигналізують про роботу в мережі. Після цього можна перевести роботу програми у фоновий режим (мінімізувавши вікно).

Примітка: типовий проект Klingon, звичайно, проведе закачування близько 150 файлів, що становить близько одного мегабайта, при швидкості з'єднання 28.8 Кб/с протягом 5 хвилин.

1.5. Перегляд результатів

Після того як проект почав працювати або закінчив роботу можна переглянути результати в проектному вікні. У лівій панелі програми показана карта проекту (список сторінок, який дослідила програма), а у правій панелі – список файлів, які закачані.

Можна переглянути повний список файлів або всю їх деталізацію.

Закачані файли зберігаються в теці, яка створюється teleport pro і одержує те ж ім'я,що і проект. перегляд теки можна провести із провідника windows. з файлами в теці можна виконувати всі дії, притаманні windows (копіювати, переміщати, перейменовувати, видаляти й т.п.). параметрів проекту

Налагодити додаткові параметри проекту можна при використанні кнопки  **свойства проекта** на панелі інструментів. Після введення команди з'явиться діалогове вікно (рис. 7).

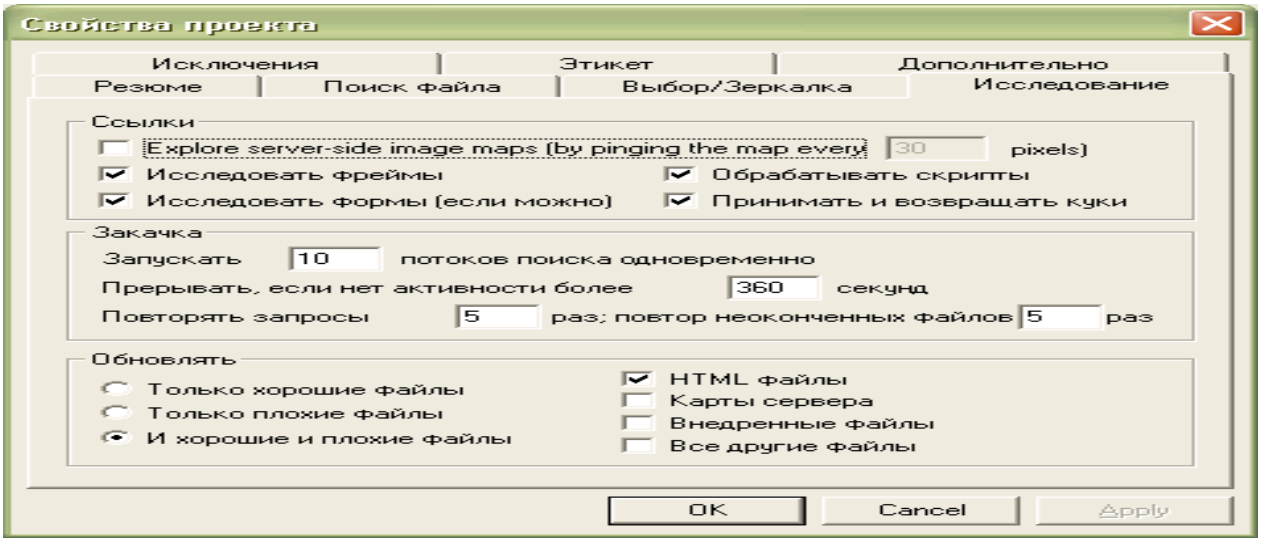


Рис. 7. Вікно налагоджування параметрів проекту

Примітка: встановлення мінімального або максимального розміру файлу для закачування до нуля, указує на те, що розмір не обмежений для закачування. Teleport Pro фільтрує файли за розміром, якщо сервер передає їх розміри, якщо сервер цього не робить, то програма закачує файл до розміру обмеження, а потім припиняє його закачування.

Teleport Pro знайде ключові слова, навіть якщо вони приховані всередині кодів HTML або коментарів.

Увага!! Якщо ввести у вкладці **Исключения** типи файлів, які не потрібно переглядати програмі (ключові слова у файлах, розширення, адреси сайтів), то ніякі інші налагодження не вкажуть програмі на можливість пошуку вказаних файлів.

Увага!! Teleport тільки намагається відновити (або модифікувати) ті файли, які відповідають поточним установкам **Проектных свойств** і правилам дослідження. Іншими словами, якщо в попередньому проектному сеансі направити teleport, щоб відновити графіки і текстові файли; а потім змінити пошукові установки, щоб відновити тільки текстові файли, виконуючи проект, програма буде шукати тільки текстові файли, тому що графічні файли більше не відповідають пошуковим установкам проекту.

Команди **Пауза** й **Прервать** меню **Проект** дозволяють провести до кінця закачування тих файлів, закачування яких уже почалося. Відновлення закачування файлів почнеться в будь-якому випадку (після зупинки процесу) із місця зупинки.

Можливе встановлення виконання проектів один за одним через певні проміжки часу.

Teleport Pro може автоматично під'єднуватися і від'єднуватись від Internet, як вимагається для виконання й завершення створених teleport-проектів. Можливий запуск до 10 ліній запитів одночасно.

Teleport може прийняти й передати cookies, які є малим набором даних для ідентифікації та обробки клієнтів, такі як браузери або teleport. Вимкнення вказаного параметра забезпечить у якійсь мірі конфіденційність, але при цьому teleport не зможе обробляти деякі сервери, які вимагають ідентифікації користувача до передавання даних.

У програмі передбачено автозбереження за умовчанням через кожні 5 хвилин.

Можливо встановити автоматичне з'єднання, роз'єднання, і повторне підключення до послуг, використовуючи команду **Соединения** меню **Файл** (рис. 8).

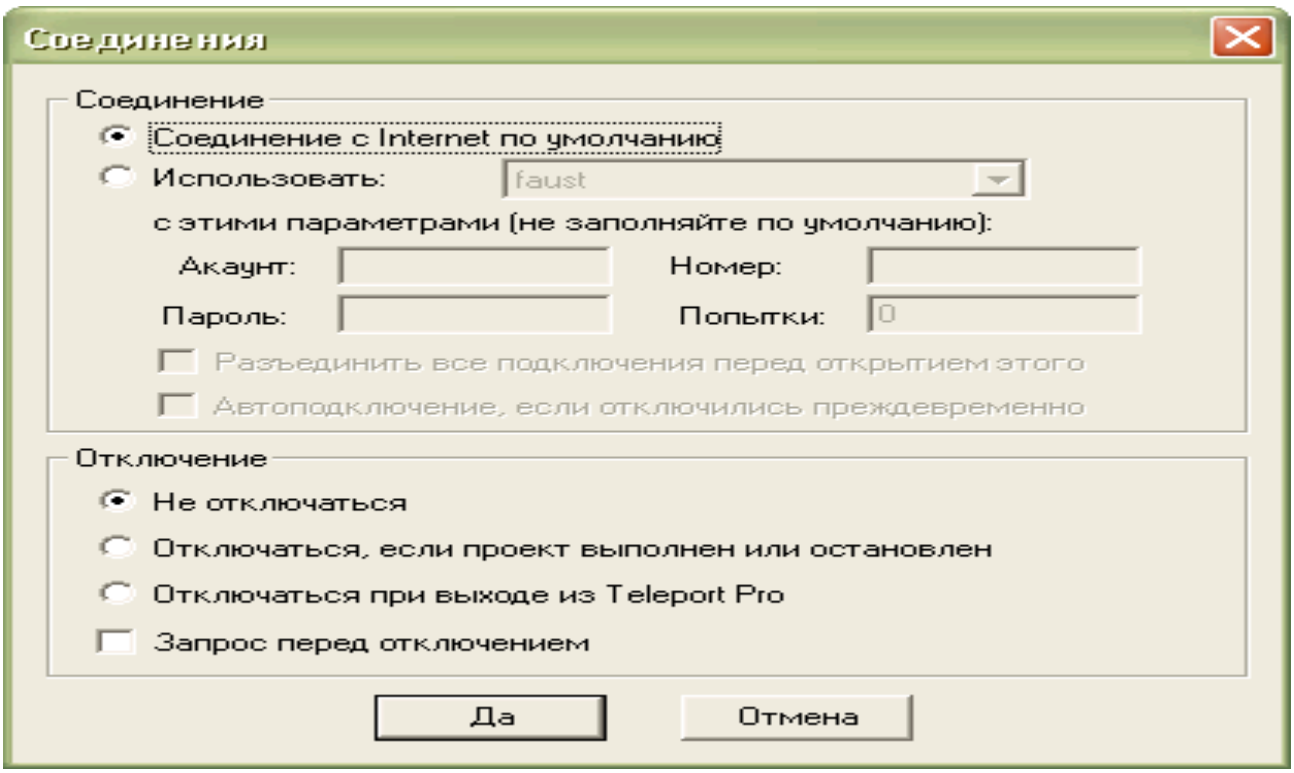


Рис. 8. Вікно встановлення автоматичного підключення до Internet

1.6. Закачування файлів за допомогою програми FlashGet

Програма FlashGet створена, щоб вирішити дві із найбільших проблем при завантаженні файлів у мережах: швидкість й можливість управління завантаженими файлами.

Це особливо актуально, коли встановлений зв'язок із віддаленим комп'ютером із малим трафіком, або якщо під час завантаження файлу перервано зв'язок. FlashGet може розділити завантажені файли на секції (до десяти частин), завантажуючи кожну секцію одночасно, для зростання швидкості завантаженні до 100-500 %.

Можливе створення списку файлів, які необхідно завантажити на комп'ютер без допомоги користувача. Програма дозволяє здійснити автоматичний пошук найшвидшого сервера, доступного для найшвидшого можливого завантаження. FlashGet автоматично набирає номер телефону, припиняє роботу комп'ютера при відсутності користувача.

Користувач програми може управляти лімітом швидкості завантаження файлів на комп'ютер, із тим аби завантаження файлів не заважало вашому перегляду Internet.

При установленні програми використовується архіватор, наприклад, WinZip, після розархівації дистрибутиву запускається на виконання файл SETUP.EXE. Після чого працює майстер установлення, який дозволить відібрати потрібні характеристики за декілька кроків установки, при цьому необхідно мати права адміністратора. За умовчанням усі установки завантаження файлів записуються у файл default.jcd. Видалення вказаного файлу може привести до некоректної роботи програми. Ключі, які відповідають за інтеграцію програми з операційною системою, знаходяться у файлі UNREG.INF. Після встановлення програми вона автоматично бере на себе функції закачування файлів. Якщо цього не сталося, то необхідно налагодити параметри програми командою **Опции** (рис. 9) із підменю **Опции/Дозвон**, вкладка **Спостереження**, крім параметрів програми.

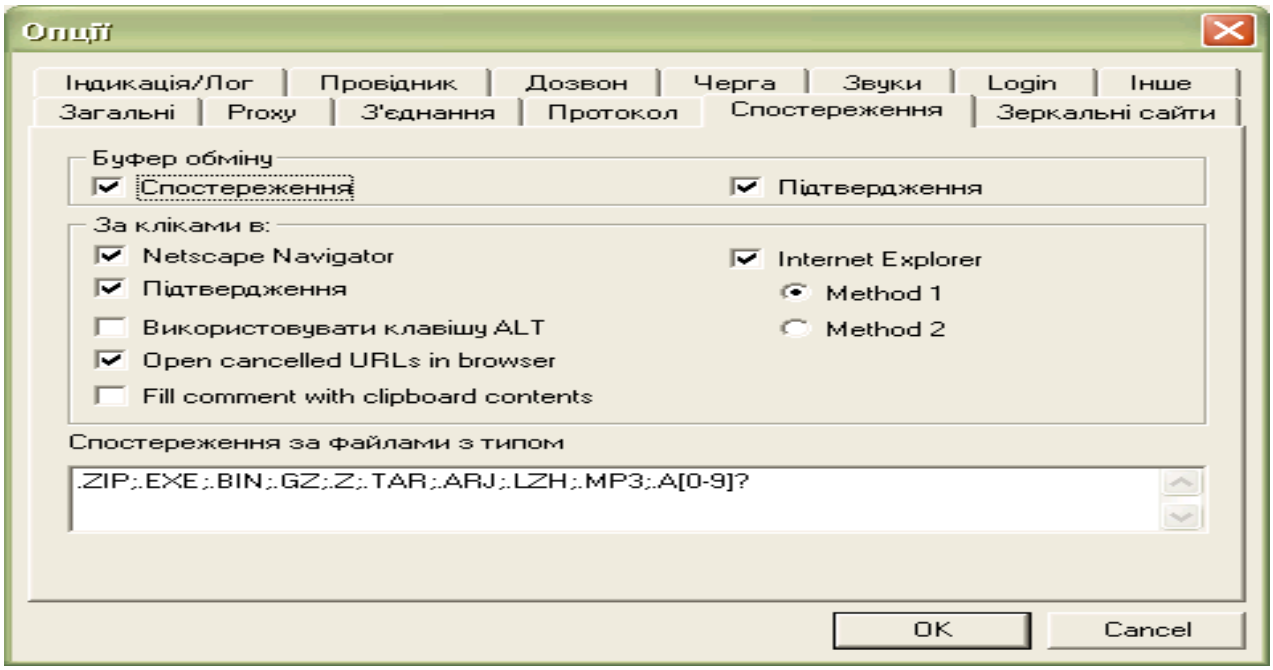


Рис. 9. Вікно налагодження параметрів програми

Крім того, можливо відібрати можливі варіанти завантаження файлів, використовуючи відповідні вкладки. Використавши вкладку **Інше**, можна встановити процес закачування файлів подвійним клацанням маніпулятором типу «миш» на терміналі монітору (рис. 10).

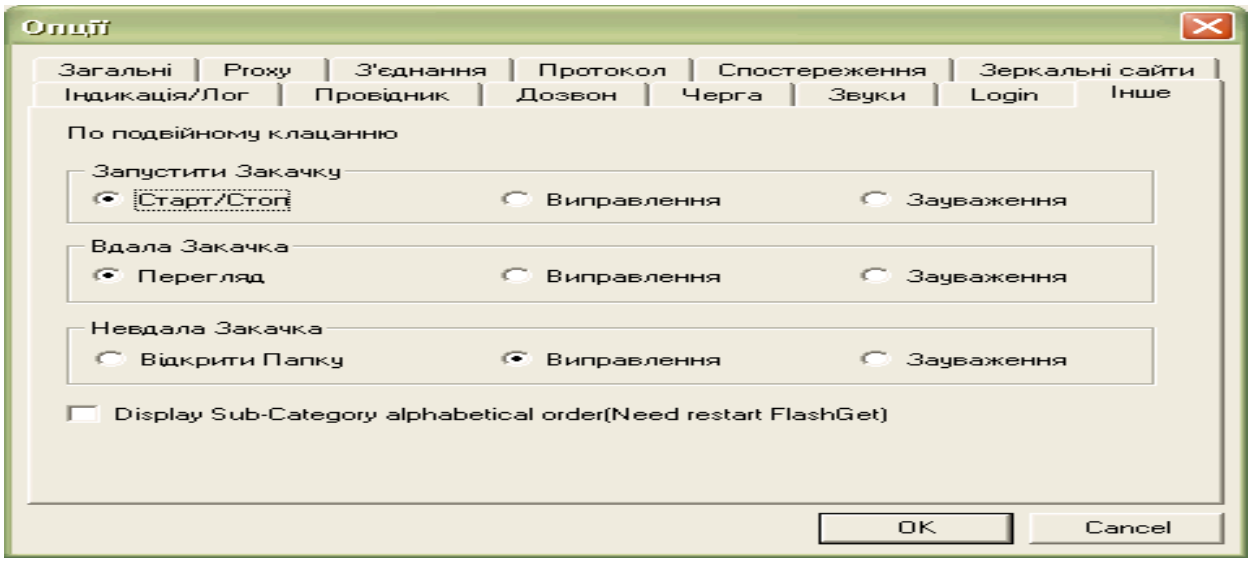


Рис. 10. Вікно встановлення закачування файлів

Використання контекстно-залежного меню (рис. 11) із відбором команди **Завантажте все** в програмі Internet Explorer надає можливість FlashGet завантажити файл з усіма зв'язками у межах сторінки. Команда **Завантажити** дозволить завантажити тільки виділений файл. Можна використати буксування файлів, які необхідно закачати, у каталог **Закачані**, (рис. 12) в потрібну категорію, або копіювати вказаний файл (файли), при цьому автоматично файли додаються у список файлів для подальшого автоматичного закачування. У даному випадку FlashGet підтримує багаторазові зв'язки від IE. У процесі відбору параметрів можна змінити параметри закачування, вибравши з контекстно-залежного меню команду **Властивості**.

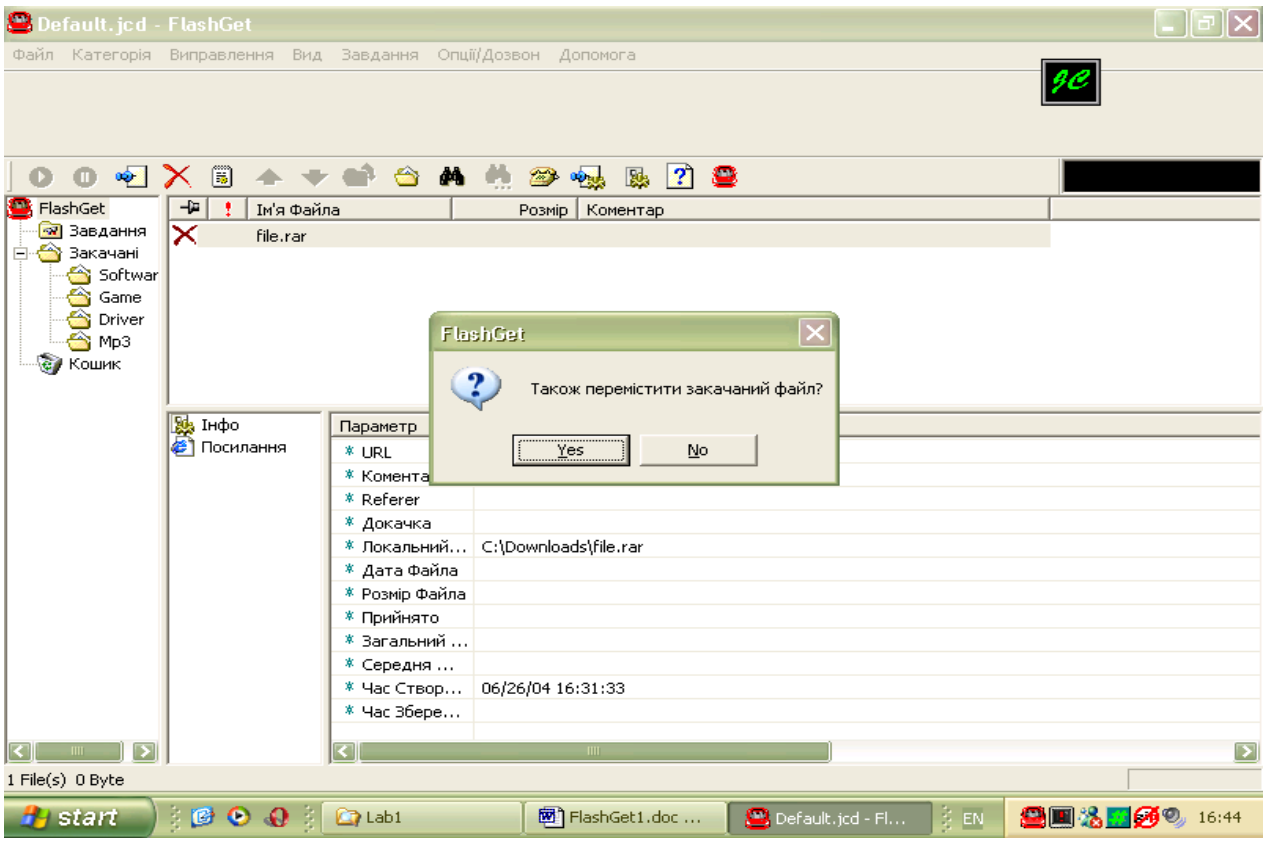


Рис. 11. Вікно відбору параметрів запуску процесу завантаження файлів

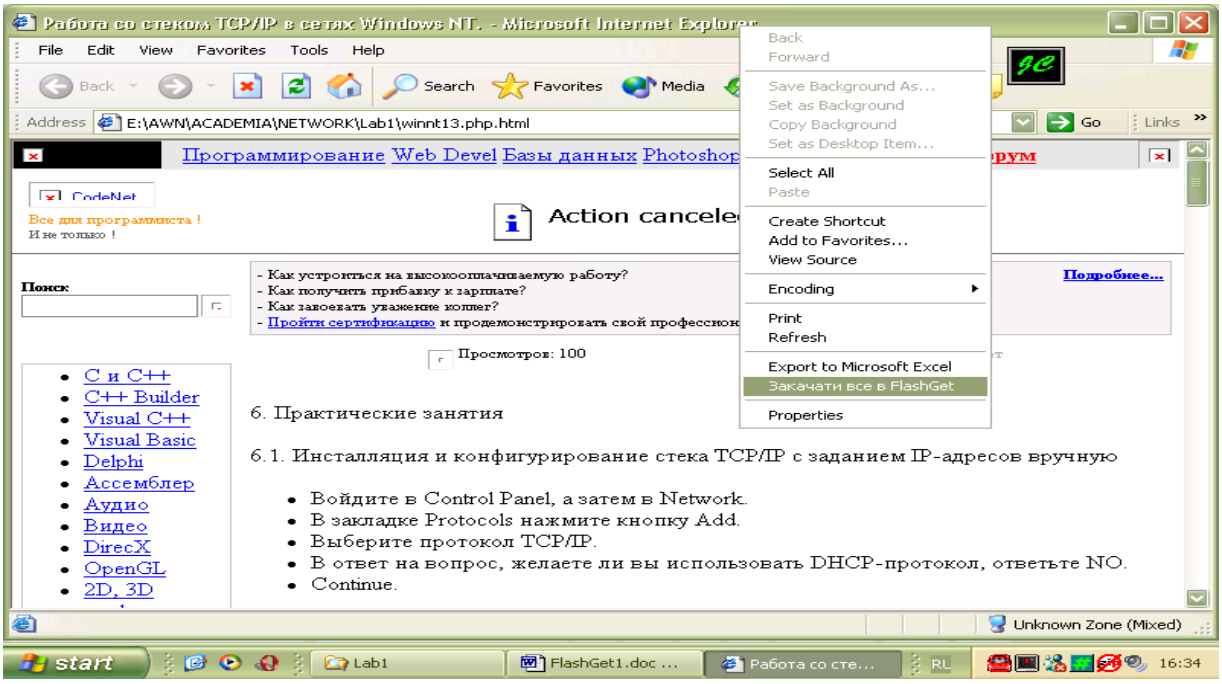


Рис. 12. Вікно відбору файлів для завантаження

Файл можна при закачуванні розбити на десять частин (рис. 13), але на практиці достатньо мати їх три-п’ять, при цьому на більш повільних серверах треба вибирати більше частин, що може дати економію часу при закачуванні файлу.

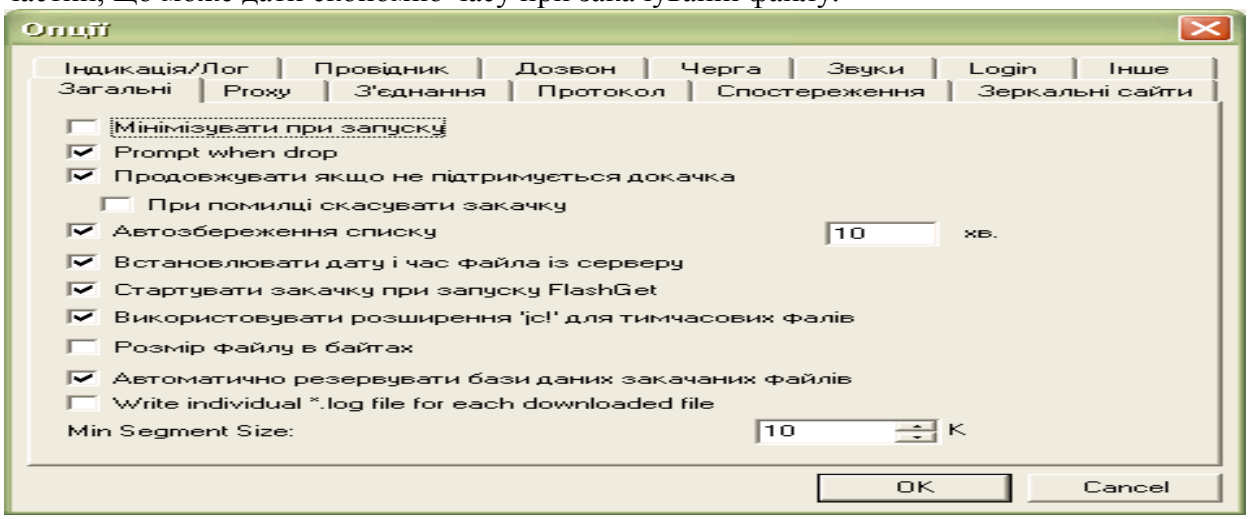


Рис. 13. Вікно встановлення поділу файлу для закачування на декілька частин

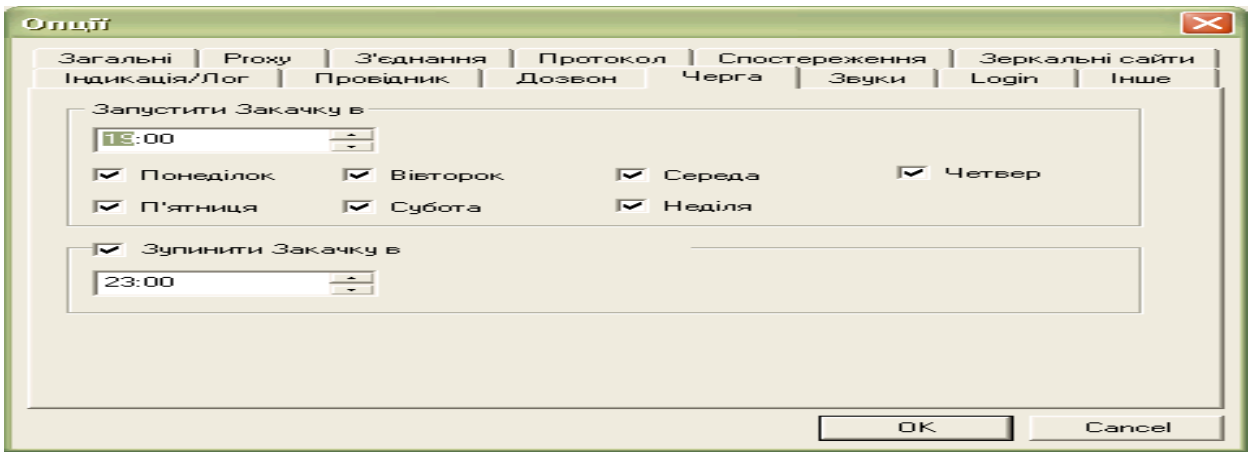


Рис. 14. Вікно встановлення часу закачування

З метою економії часу та грошей треба планувати завантаження файлів у не пікові часи роботи мережі, а у часи коли завантаження дешевше, для цього використовується вікно (рис. 14) вкладка – **Черга**. З указаною метою використовується вкладка **Дзеркальні сайти,** яка дозволяє перемкнути закачування файлів на більш доступний сервер.

Деякі сервери вимагають перевірки логіну та паролю перед закачуванням файлів. Вони установлюються через вкладку **Login**, команда **Додати.** При використанні проксі-сервера можна налагодити параметри через вкладку **Proxy** команду **Додати.**

Важливо перевірити закачані файли на наявність вірусів, закладок і т. п. Для цього через вкладку **Провідник** установлюються відповідні параметри (рис. 15).

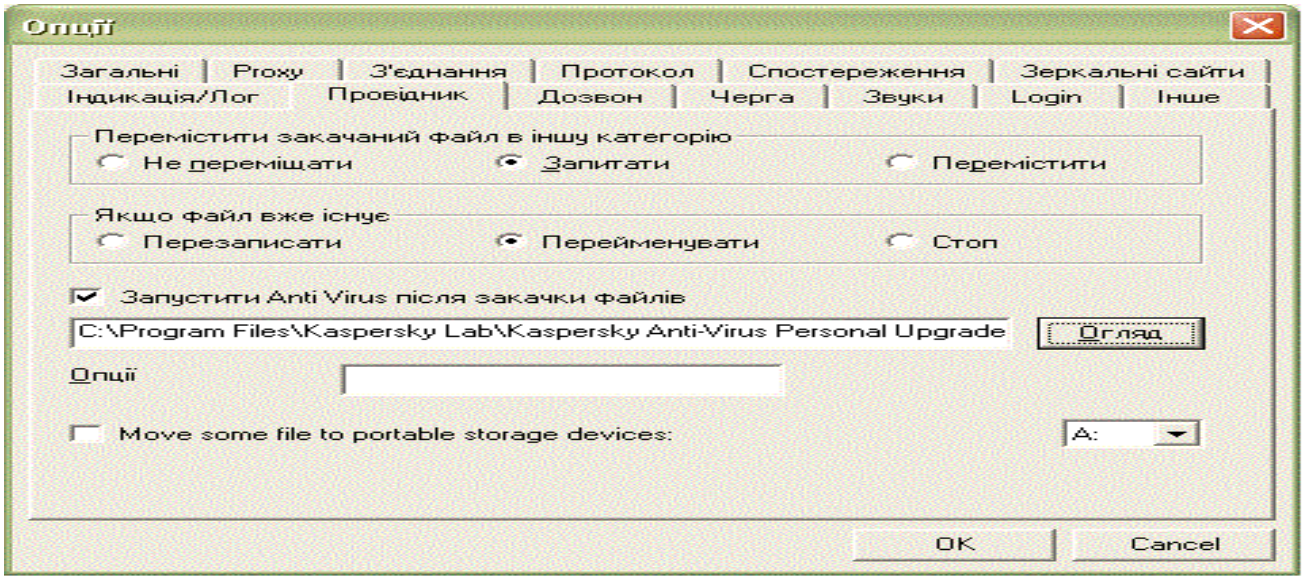


Рис. 15. Вікно встановлення автоматичного запуску антивірусної програми

1.7. Головне меню програми FlashGet

Підменю Файл

Новий файл – створюється новий файл даних завантаження.

Відкрити – відкрити існуючий файл даних завантаження.

Збереження – зберегти файл поточних даних. Кожний файл, збережений у категорії MP3, буде переміщений на c:\download\mp3.

Зберегти як – зберегти файл поточних даних із новим ім'ям.

Додати попередній файл – додати завантажені файли (finished/unfinished) до списку роботи.

Імпортувати інформацію – додають пакетні завдання, які не були завантажені або розподілені за категоріями FlashGet.

Експортна інформація – це список вашої поточної бази даних, який указує на те, які файли були завантажені.

Експортуйте – експортує завантажений файл(и) і інформацію завантаження.

Вихід з FlashGet.

Підменю Категорія

Нова категорія – створюється нова категорію завантаження. FlashGet дозволяє створювати необмежену кількість категорій. Якщо завантажується велика кількість файлів, то створення нових категорій необхідне.

Перемістити в – перемістити вибрану категорію/категорії в іншу категорію.

Видалити – видаляє вибрану категорію/категорії. При видаленні категорії, усі файли будуть також видалені.

Властивості – зміна властивостей вибраної категорії.

Підменю Виправлення

Вставте URL – створення нових даних для закачування файлу.

Виділіть усі – виділяється кожна робота в поточній категорії**.**
Інвертувати виділення – зміна вибраних елементів на невибрані, а невибраних елементів на вибрані**.**
Знайти – здійснюється пошук елементів завантаження за іменем, URL або коментарем.
Підменю Вид
Детально – показати вікно завантаження детально (нижнє вікно, що графічно показує завантаження файлу в FlashGet і ділення його на частини).
Кошик – приховує або показує зону кошику FlashGet.
Панель інструментів – налагоджує вигляд панелі інструментів**.**
Колонки – дозволяє налагодити потрібні колонки програми.
Мова – дозволяє вибрати мову спілкування.
Підменю Завдання
Нова закачка – створюється нове завантаження файлу (файлів).
Додати завдання – використовується завантаження пакету. Додають завантаження пакету, якщо там було багато файлів для завантаження й вони мають зразок у їх іменах. Наприклад: file01.zip до file10.zip.
Старт – запуск.
Призупинити – зупинка**,** пауза.
Перемістити в – перемістити вибраний файл(и) в іншу категорію.
Видалити – видалити вибраний файл(и).
Властивості – властивості файлу.
Перемістити вгору (униз) – вибраний файл(и) пересувається вище, або нижче.
Перевірити на відновлення – здійснюється перевірка: був оновлений завантажений файл чи ні.
Повторити закачку – завантажують файл знову.
Підменю Опції/Дозвон
Дозвон – дозволяє відібрати параметри дозвону до віддаленого комп'ютера.
Виключити живлення за завершенням – дозволяє виключити живлення комп'ютера після завершення роботи програми.
Розірвати з'єднання за завершенням – дозволяє розірвати з'єднання з віддаленим комп'ютером після завершення роботи програми.
Повторити з'єднання, якщо припинилося – дозволяє повторити з'єднання з віддаленим комп'ютером після його розриву.
Обмеження трафіку – дозволяє обмежити трафік закачування файлу.
Зберегти за умовчанням – дозволяє зберегти за умовчанням параметри програми.
Опції – дозволяє налагодити параметри програми.

2. Хід роботи

1. Створити в Teleport Pro послідовно проекти закачування файлів з сервера www.google.com.ua, www.ukr.net, www.rambler.ru з груповими іменами *.bmp, *.txt, *.html.
2. Зберегти проект.
3. Запустити на виконання.
4. Переглянути результати та показати їх викладачеві
5. Створити в програмі FlashGet завантаження файлів за пунктом 1 без розбивки на частини під час закачування та з розбивками на 3,7, 11 частин. Порівняти час закачування файлів в програмі Teleport Pro та FlashGet.
6. Завантажити програму NetMeeting –з сайту http://microsoft.com/windows/netmeeting/download/default.asp та програму ICQ -- *http://web.icq.com*

3. Контрольні питання

1. Закачування файлів за допомогою програми Teleport Pro
2. Створення нового проекту
3. Збереження проекту
4. Запуск проекту
5. Перегляд результатів
6. Налагоджування параметрів проекту
7. Закачування файлів за допомогою програми FlashGet
8. Особливості програми FlashGet
9. Головне меню програми FlashGet

ЛАБОРАТОРНА РОБОТА 34.
РОБОТА З БРАУЗЕРОМ MICROSOFT INTERNET EXPLORER

Мета роботи: уміти підготувати програму Internet Explorer до роботи, налагоджувати її параметри, проводити пошук потрібної інформації в мережі Internet з використанням методики пошуку, яка включає правила формування запиту на пошук, методи звуження області пошуку, управління процесом пошуку, вибір форми представлення результатів.

Зміст

1. Теорія
1.1. Способи запуску програми Internet Explorer.
1.2. Пошук інформації у мережі Internet
1.3. Засоби пошуку інформації у мережі Internet
1.4. Методика пошуку
1.5. Управління процесом пошуку
1.6. Результати пошуку
1.7. Обмеження доступу
2. Хід роботи.
3. Контрольні питання
Додаток 1
Додаток 2
Додаток 3
Додаток 4

1. Теорія

1.1. Способи запуску програми Internet Explorer.

Для перегляду web-ресурсів розроблена безліч програм-клієнтів, називаних браузерами (browser, оглядачі). Першим з них був текстовий браузер lynx, реалізований в операційній системі UNIX. З розвитком і розширенням можливостей системи WWW були розроблені різні браузери із графічним інтерфейсом, першим з яких став браузер Mosaic, узятий за основу при створенні широко розповсюдженого в цей час браузера Microsoft Internet Explorer.

Програма Internet Explorer (завантажувальний файл explorer.exe знаходиться в каталозі Program Files\Internet Explorer) призначена для навігації за мережею Internet і виконання дій над її об'єктами. Для запуску цієї програми можна скористатися одним з наведених нижче способів:

а) в меню **Пуск** вибираємо команду **Программы,** потім команду **Internet Explorer**;

б) двічі клацнути основною клавішею маніпулятору "миша" на піктограмі **Internet Explorer**;

в) в меню **Пуск** вибрати команду **Выполнить**, використовуючи кнопку **Обзор** знайти файл **E**xplorer.exe та клацнути основним клавішем маніпулятору "миша" на кнопці **Ok**.

Після запуску програми відкриється вікно (рис 1).

1.2. Пошук інформації у мережі Internet

Основна мета користувача при роботі з мережею Internet – це отримання інформації, так як Internet є гігантським інформаційним ресурсом. Цілеспрямований пошук інформації вимагає формулювання мети пошуку, розуміння того, що є об'єктом пошуку, обґрунтування вибору засобів пошуку та ефективної методики.

Мета пошуку визначає характеристики об'єктів пошуку, об'ємів та термінів виконання роботи, перелік засобів пошуку та способів їх застосування.

В якості об'єкта пошуку може розглядатися будь-яка інформація, якщо є можливість представлення її в Internet. Це можуть бути телефони, адреси, інформація про товари, послуги, телевізійні трансляції і т.п.

Рис. 1. Загальний вигляд вікна Internet Explorer

Огляд пошукових систем

В даний час існує багато пошукових систем, які цікаві, якісні, але в силу ряду причин не дуже популярні. Більш того, багато хто з них надають інформацію в такому цікавому і незвичайному вигляді, що робота з ними перетворюється з рутинного дії в захоплюючу гру. Аналіз тенденцій на цьому ринку дозволяє зробити висновок, що основний напрям розвитку – візуалізація отриманих результатів пошуку і більш вузька спеціалізація пошуку (пошуковики зображень, пошуковики ігор, пошуковики для жінок і т.д.). Більшість пошукових систем дають прекрасну можливість отримання необхідної інформації. Всі пошукові системи можна поділити на кілька основних груп. В даному огляді зроблена спроба такої систематизації, наведені деякі приклади членів кожної групи. Для кожного пошукача дано його короткий опис і підкреслені основні відмінні риси. Приклади наведені таким чином, щоб дати максимально вичерпну інформацію про кожну групу пошуковиків, їх можливості, сфери застосування, відмінні особливості. Маючи уявлення про основні характеристики, користувач може провести самостійне додаткове дослідження з даної теми і знайти для себе ще багато цікавих, красивих і незвичайних пошукових систем.

В даний час існує 3 основних міжнародних пошукових системи – Google, Yahoo і MSN, що мають власні бази даних і пошукові технології. Більшість інших пошукових систем використовує в тому чи іншому вигляді технології трьох перерахованих. Наприклад, пошук AOL (search.aol.com) використовує базу Google, а AltaVista, AllTheWeb і Lycos-базу Yahoo. Портал Mail.ru довгий час використовував пошукову технологію Google, а з 2006 року – Yandex. У Росії основний пошуковою системою є Yandex, за ним йдуть Mail.ru, що використовує технологію Yandex, замикає трійку лідерів – Rambler. Однак найбільша кількість пошукових запитів обробляє Google, російська версія якого (Google.ru) розпочала свою роботу в 2004 році. Кожен користувач Інтернету орієнтується на ту пошукову систему, до якої він звик або яку йому порадили його колеги. В додатку 5 наведені короткі характеристики основних пошукових систем.

1.3. Засоби пошуку

Засобами пошуку можуть бути: Web-індекси, Web-каталоги, гібридні системи пошуку, метапошукові системи, засоби локального пошуку, утиліти автономного пошуку.

Створення Web-індексів виконується спеціальними програмними продуктами на основі алгоритмів штучного інтелекту, в результаті чого здійснюється постійне поповнення виключно комп'ютерами в автоматичному режимі величезних баз даних за індексуємими документами. Основний недолік цих систем – це те, що знайдені "ключові слова" далеко не завжди відповідають за суттю темі пошуку.

Найбільш відомі Web-індекси: Google (http:www.google.com), AltaVista (http://www.altavista.com), HotBot (http://www.hotbot.com), Open Text (http://www.opentext.com/) і т.п.

Принципово інший підхід реалізовано при створенні Web-каталогів. Такі пошукові системи створюються людьми, котрі самі переглядають вузли Web, читають електронну пошту і телеконференції, аналізують і класифікують отримані дані. Тому за якістю сортування документів Web-каталоги суттєво переважають Web-індекси, суттєво програючи останнім за кількістю переглянутих документів.

Найбільш відомі Web-каталоги: Yahoo! (http://www.yahoo.com), Magellan (http://www.magellan.com), Ukr.net (http://www.ukr.net) і т.п.

Існує багато веб-каталогів, у тому числі українські **Мета** (http://meta.ua), **UAport**(http://uaport.net), **Пошук** (http://www.poshuk. com), **Холмс**(http://holms.ukrnet.net), **UkraiNet** (http://www.ukrainet.com.ua/ukr) та інші.

Крім класичних індексів і каталогів, в Internet існують і "гібридні пошукові системи", в яких можна скористатися і індексованою базою даних, і структурованими тематичними каталогами.

Приклад гібридних пошукових систем: Lycos (http://www.lycos.com), Excite (http://www. excite.com), Infoseek (http://www.infoseek.com), WebCrawler (http://www.webcrawler.com).

Кожний з наведених засобів пошуку дозволяє отримати перелік документів, які будуть суттєво відрізнятися один від одного. Це пов'язано з різними методами збирання інформації та алгоритмами ведення індексованої бази даних, що закладені в роботу кожної з пошукових систем. Для того, щоб можна було звернутися одночасно до цілого ряду пошукових систем з однієї сторінки браузера, розроблені спеціальні інтерфейсні програми – метапошукові системи, в яких можна почергово вводити ключові слова в текстовому вікні кожного з представлених пошукових серверів.

Найбільш зручні метапошукові системи: AccuFind (http://www.accufind.com); Metafind (http://www.metafind.com); Metasearch (http://www.metasearch.com).

Засоби локального пошуку забезпечують пошук інформації безпосередньо на сервері фірми і т.п.

Автономні утиліти встановлюються на комп'ютері користувача. До них можна віднести WebCompass (http://www.quarterdeck.com) і Copernic (http://www.copernic.com).

Автономні браузери: WebWhacker (http://www.ftg.com), Teleport Pro (http://www.tenmax.com) і т.п.

1.4. Методика пошуку

Методика пошуку включає правила формування запиту на пошук, методи звуження області пошуку, управління процесом пошуку, вибір форми представлення результатів.

Запити на пошук описують умови, яким повинні відповідати результати пошуку. В запитах задаються слова або фрази, які будуть шукатися, вони називаються ключовими.

Правила формування запиту:

Ім'я власне (повинно починатися з прописної букви): Слово.

1. Пошук слова без врахування регістра: **слово**.
2. Ключове слово з будь-яким закінченням: **слово*.**

3. Ключове слово з будь-яким закінченням, що складається з одного символу: **слово?**.
4. Неподільна ключова фраза: "**слово1 слово2 ...**".
5. Ключове слово обов'язкове: **+слово**.
6. Ключове слово повинно бути відсутнім: **-слово**.

В запиті можливо задавати логічні вирази, які швидше за все застосовуються при розширеному пошуку (Advanced search). Логічні вирази будуються шляхом застосування ключових слів, круглих дужок і логічних операцій AND, OR, NOT (указані операції можуть позначатися, як - &, | , !)

Приклади логічних виразів:

1. Вираз:

слово1 AND слово2 AND NOT слово3

еквівалентний

+слово1+слово2-слово3.

2. Вираз:

"фраза" AND (слово1 OR слово2)

еквівалентний

("фраза" AND слово1) OR ("фраза" AND "слово2").

Деякі пошукові системи підтримують метакоманди, повний перелік, яких можна отримати за допомогою довідкової системи. В системі AltaVista метакоманди застосовують для наступних видів пошуку:

1. Пошук Web-сторінок з указівкою заголовків: **title:заголовок**;
2. Пошук у тексті сторінок: **text:слово**;
3. Пошук слова серед посилань на Web-сторінці: **anchor:слово**;
4. Пошук сторінок, які мають посилання на визначену адресу: **link:адреса**;
5. Пошук графічного файлу на Web-сторінці: **image:ім'я.jpg**;
6. Пошук сторінок з аплетом: **applet:ім'яапплета**;

Рекомендації щодо формування запитів

В якості ключових слів у запиті треба використовувати якомога точне слово або словосполучення, яке найбільш точно характеризує об'єкт пошуку.

Не потрібно використовувати слова, які часто зустрічаються типу "Internet", "web", "program", бо можливий результат пошуку може бути дуже великим.

Для областей знань, де термінологія ще не устоялася (наприклад, в області комп'ютерних технологій) можна використовувати слова-синоніми, з'єднуючи їх логічною операцією OR.

При недостатньому числі результатів пошуку можна варіювати ключовими словами "run", "runs", "running" або використовувати символи-джокери "run*". Область пошуку.

Більшість пошукових систем (Yahoo, AltaVista і інші.) дозволяють перед виконанням запиту уточнити область за тематичним каталогом категорій. Для цього треба спочатку вибрати одну або декілька категорій, а потім виконати запит. Існує можливість вибору мови, місця пошуку (Internet, UseNet, і т.д.), держави або домену. Можливо задати часові межі для дати останнього оновлення інформації про об'єкти, які шукаємо.

1.5. Управління процесом пошуку

Звичайно процес пошуку являється циклічною процедурою, яка складається з послідовних запитів на уточнення запиту та перегляду інформації, що найдена. Якщо найдене посилання, яке максимально задовольняє мету пошуку, то доцільно виконати пошук подібних документів за допомогою кнопки More like this.

Стратегія пошуку індивідуальна, але корисно враховувати певні практичні рекомендації.

Починати пошук слід із пошукових серверів, які є спеціальними в даній області (тематиці). Першим об'єктом пошуку можуть бути огляди посилань, які регулярно

розробляють користувачі Internet. Має рацію пошук у першу чергу документів за часто наведеними питаннями FAQ (Frequently Asked Questions) за якоюсь темою. В таких випадках перший запит на пошук повинен фрази типу "**Поиск ...**", "**Обзор ...**" або "**FAQ ...**".

Якщо використання пошукових серверів не приводить до результату, то доцільно використовувати сервери організацій (університетів, видавництв, фірм), які працюють у даній області. За допомогою контактів з вказаними організаціями можливо отримати інформацію, яка не представлена в Internet (рекламні матеріали, копії публікацій, безкоштовні CD і т.п.).

Якщо необхідно мати швидкий доступ до Web-сторінок, то посилання на них тримають в каталогах **Избранное**, копіюючи адреси сторінок. Виклик Web-сторінки проводиться подвійним натиском основної клавіши маніпулятору "миша" на відповідній адресі.

1.6. Результати пошуку

Пошуковий сервер в результаті виконання запиту виводить загальну кількість знайдених об'єктів та список їх анотацій. Кожний об'єкт в анотації описується заголовком або назвою об'єкта, адресою ресурсу, де розташований об'єкт, коротким описом та характеристиками.

Характеристиками звичайно є розмір, дата знаходження об'єкта в мережі та ступінь відповідності запиту, виражена у відсотках (%) або в кількості використаних ключових слів.

Можна управляти об'ємом інформації в анотації, порядком анотацій в списку й числом анотацій на сторінці. Якщо список великий, то найбільш важливим параметром є порядок. Можливі наступні варіанти умов сортування результатів пошуку використання заданих ключових слів у документі:

1. Ключові слова в заголовку Web-сторінки;
2. Ключові слова в списку ключових слів Web-сторінки (тег <META>);
3. Довжина й дата документа.

1.7. Обмеження доступу

8.1. Використання властивостей оглядача.

Ввести команду **Свойства** із меню **Сервис**, вибрати вкладку **Безопасность** та рівень безпеки, ввівши команду **Другой**. В діалоговому вікні встановити відповідні налагодження.

8.2. Установлення фільтрів.

Ввести команду **Свойства** з меню **Сервис**, вибрати вкладку **Содежание** натиснути кнопку **Включить**. Відібрати потрібну категорію, наприклад, **Насилие**, використати повзунок для фільтрації вказаної категорії. Положення повзунка зліва – найменша можливість перегляду і справа – найбільша.

1.8. Робота в Internet Explorer з поштою

Створення поштової скриньки

Розглянемо створення поштової скриньки на сайті www.ukr.net. Заходимо на відповідний сайт (рис. 1). Вводимо команду **Реєстрація** та заповнюємо відповідні вікна (рис. 2). Після заповнення полів вводимо команду **Зареєструвати скриньку.**

Отримаємо пароль підтвердження на мобільний телефон та вводимо його **в** відповідне поле запиту сайту. Поштова скринька заєрестрована. Входимо до неї ввівши логін та пароль в вікна **пошта** (рис. 3).

Вводимо команду **Увійти** після чого відкривається вікно поштової скриньки (рис. 4).

Для відправлення повідомлення на іншу скриньку вводимо команду **Написать письмо** (рис. 5) та заповнюємо відповідні поля.

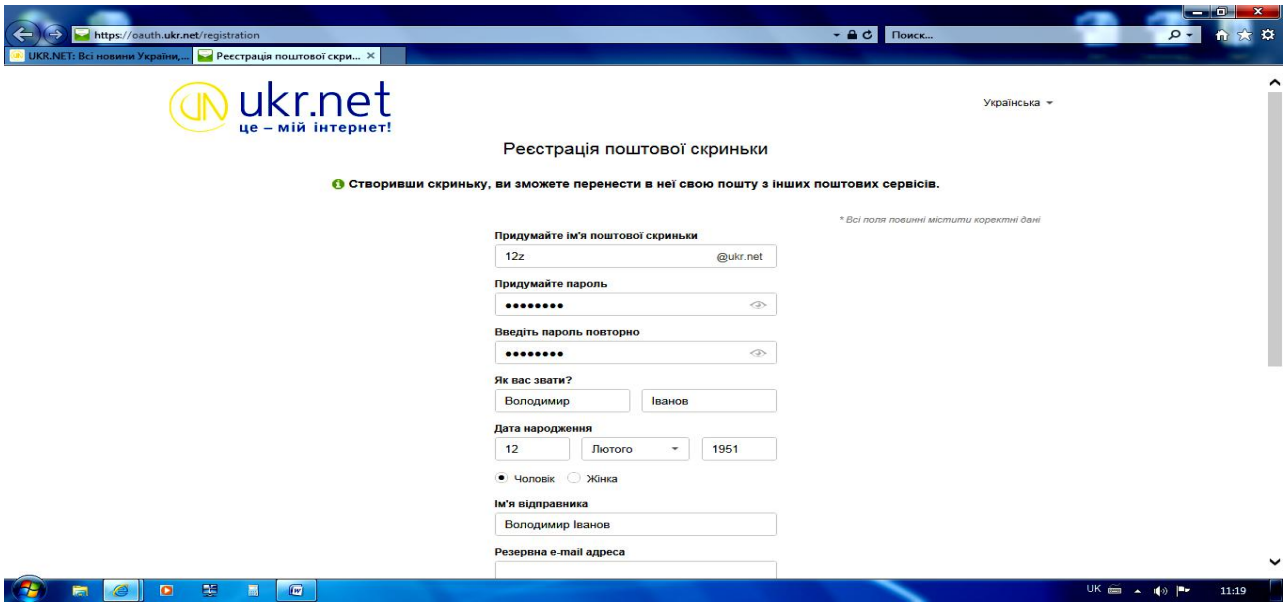


Рис. 2. Заповнення полів реєстрації

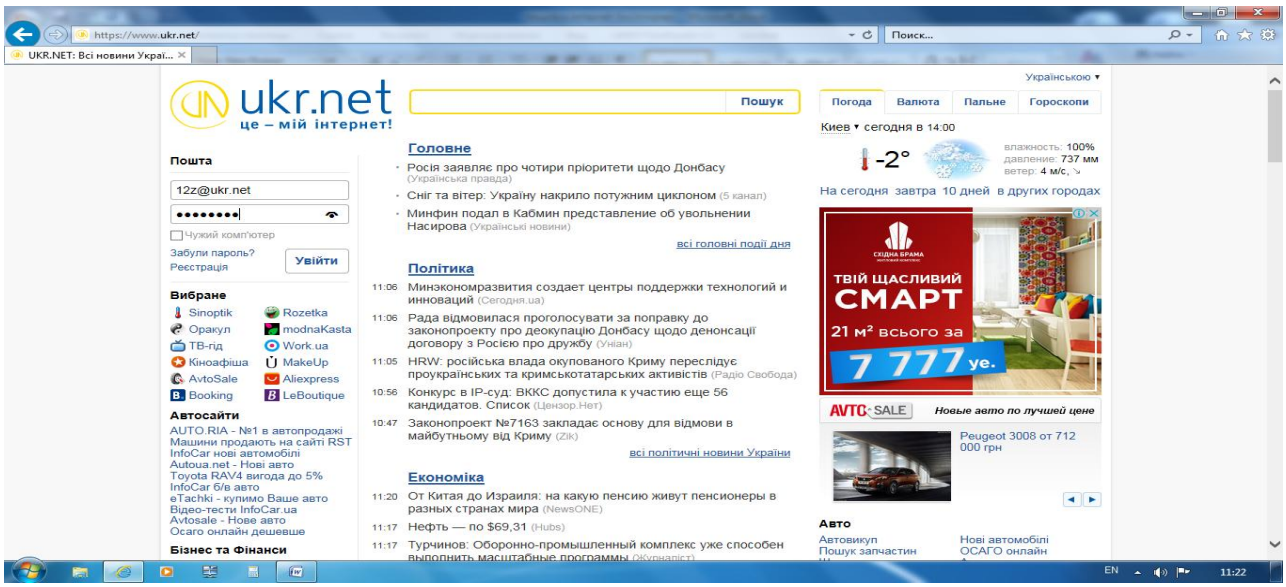


Рис. 3. Введення логіну та паролю для входу в поштову скриньку

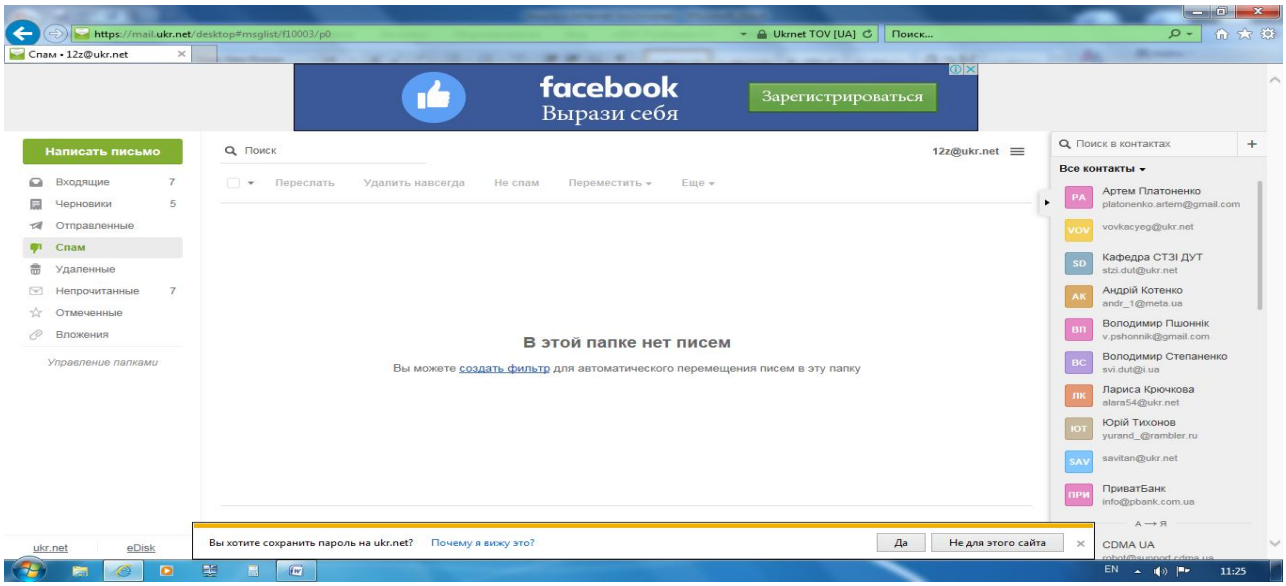


Рис. 4. Вікно поштової скриньки

Робота з поштовою скринькою

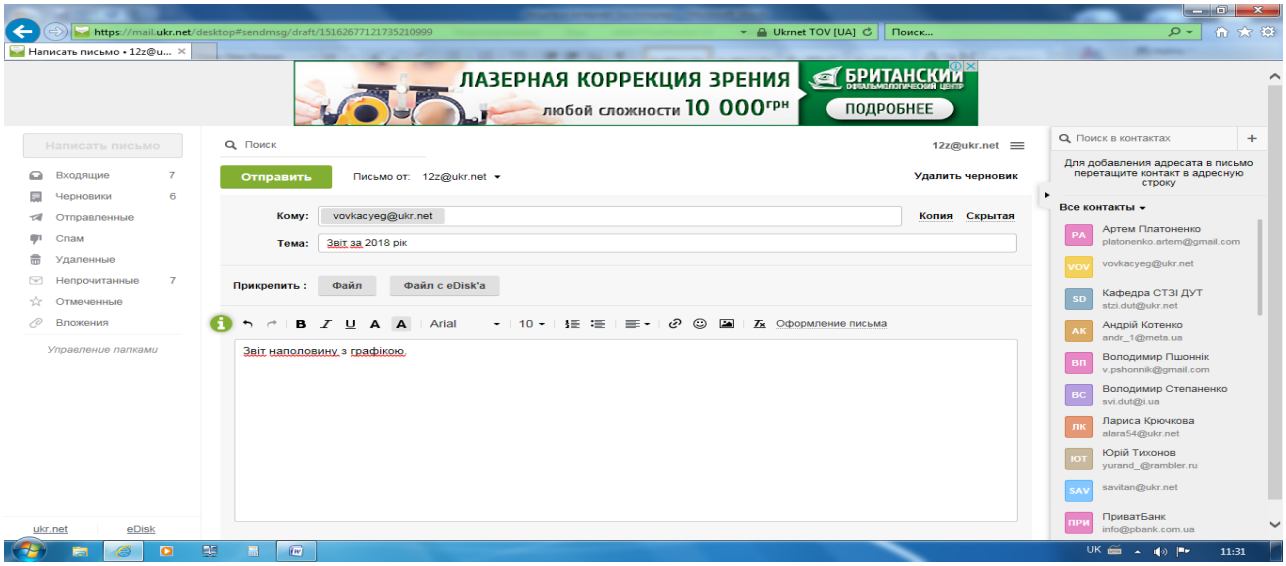


Рис. 5. Заповнення полів для листа

При необхідності уложення файлу(лів) вводимо команду **Файл** та відбираємо потрібний файл (рис. 6). Після відбору файлу(лів) вводимо команду **Открыть**

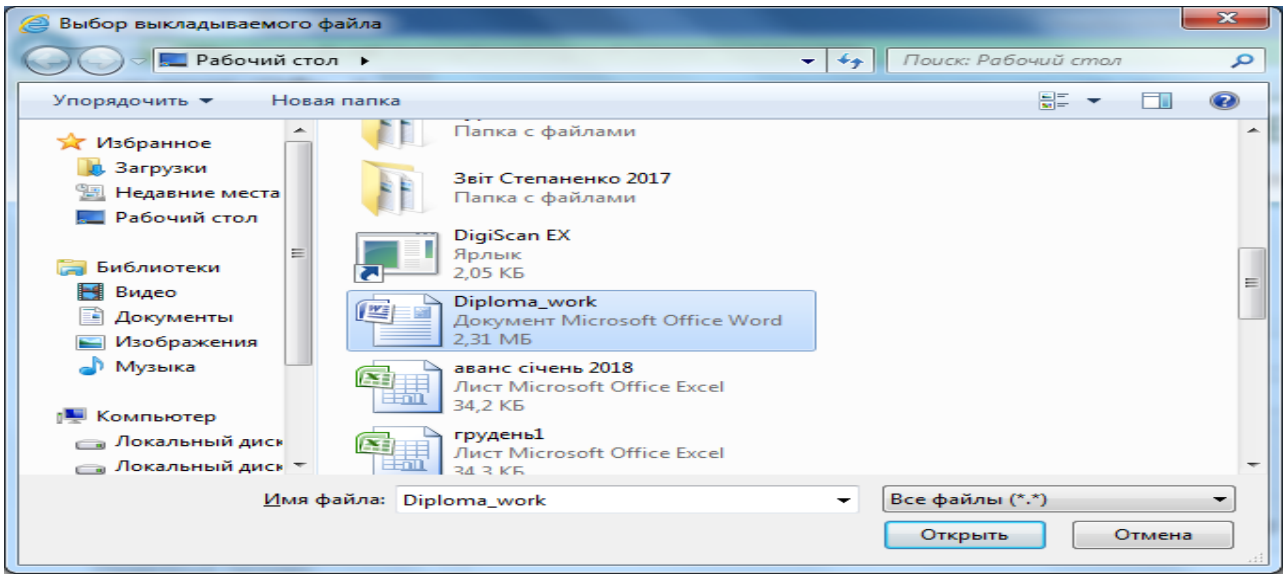


Рис. 6. Відбір файлу для листа

В вікні поштової скриньки з’явиться відповідне зображення (рис. 7).

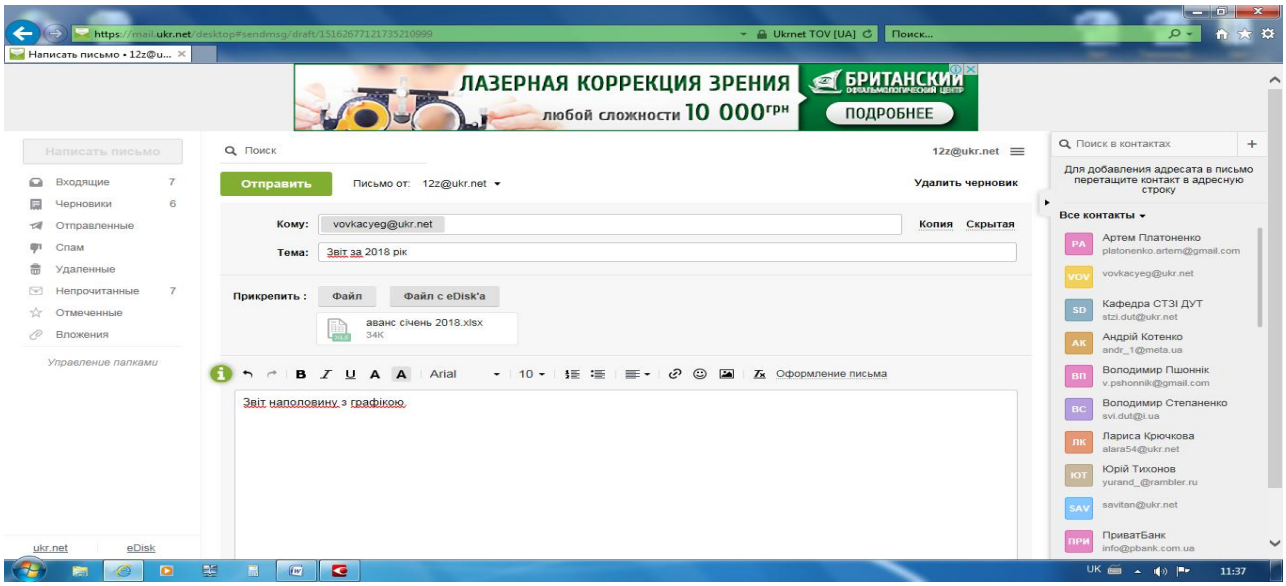


Рис. 7. Поштова скринька з вкладеним в лист файлом

Для відправлення листа вводимо команду **Отправить**. Якщо адреса отримувача вказана правильно то отримаємо таке повідомлення (рис. 8).

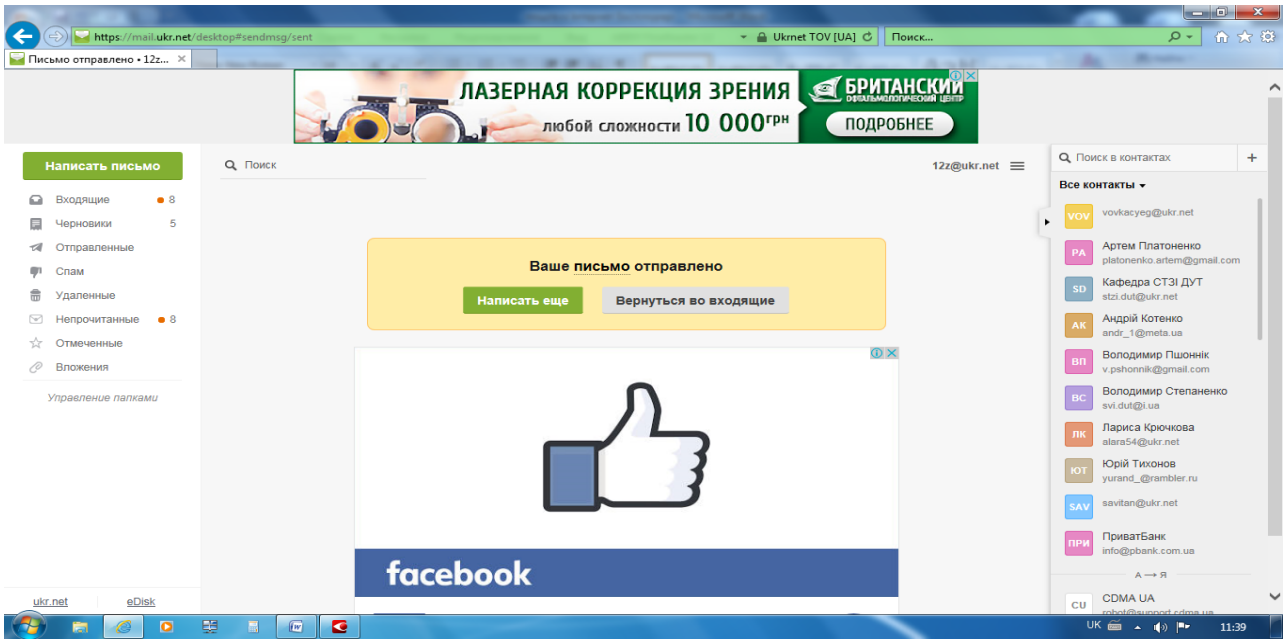


Рис. 8. Повідомлення про відправлення листа

Всі листи, що надійшли у скриньку знаходяться в папці **Входящие** (рис. 9). Читати їх зміст та копіювати, видаляти можна відомими способами, що використовуються в Windows. Тоді повідомлення переміщуються в відповідну папку.

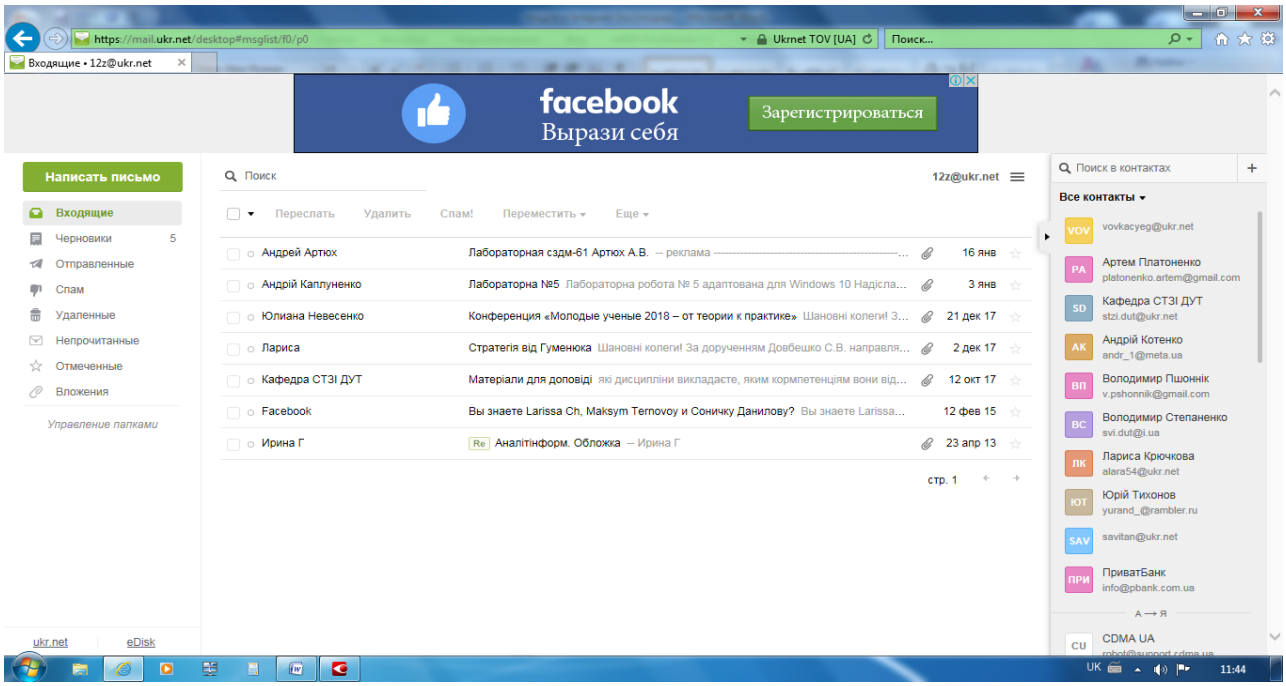


Рис. 9. Папка **Входящие**

2. Хід роботи

Для виконання роботи попередньо запустіть програму Internet Explorer відомими вам способами та розгляньте його головне меню.

1. Вивчення можливостей запиту на розширений пошук**.**

Використати пошуковий сервер згідно додатку 5, отримати довідкову інформацію про можливість розширеного пошуку. Провести розширений пошук Web-сторінок. За допомогою метакоманд формулювати запит так, щоб знайти всі Web-сторінки, які містять посилання на одну і ту ж адресу (прийняти довільну). Уточнити пошук, ввівши обмеження домену UA.

2. Пошук інформації у мережі Internet

В додатку 1 знайдіть тему завдання (номер теми відповідає номеру вашого комп'ютера в локальній мережі). Студент виконує завдання, фіксує для кожного завдання мету пошуку, засоби пошуку, запити пошуку та характеристики результатів пошуку. Робота завершується виконанням індивідуального завдання (розмір файлу 1-2 сторінки, число гіперпосилань більше 10) та збереженням інформації на диску “C” у каталозі “**Мои документы**”. Пошукові сервери взяти з додатка 5.

Провести пошук FTP-серверів, які мають програму WinZip, скопіювати програму на свій комп'ютер на диск “C” в каталог “ **Мои документы**».

3. Провести пошук останніх новин

Студент виконує завдання, фіксує для кожного завдання мету пошуку, засоби пошуку, запити пошуку та характеристики результатів пошуку. Робота завершується виконанням індивідуального завдання (розмір файлу 1-2 сторінки) та збереженням інформації на диску “C” у каталозі “**Мои документы**”. Пошукові сервери взяти з додатка 5.

4. Провести бесіду через Internet (IRC Internet Relay Chat)

Вийти на сервер http://www.galachat.com або сервер http://www.chat.-janus.net.ua та провести бесіду на протязі 10-15 хвилин в інтерактивному режимі.

Розташуйте в каталогах “Избранное” декілька посилань (4-6) на Web-сторінки. Отримайте доступ до вказаних Web-сторінок з каталогів “Избранное”.

3. Контрольні питання

1. Internet: історія, призначення, власник, основні характеристики.
2. World Wide Web призначення, основні характеристики .
3. Елементи мережі: вузли, лінії зв'язку, комп'ютери, операційні системи.
4. Модеми, швидкість передачі даних.
5. Протоколи обміну даними Transmission Control Protocol і Internet Protocol (TCP/IP) у сучасній мережі Internet.
6. Технологія клієнт-сервер у сучасній мережі Internet.
7. Постачальники послуг Internet.
8. Основні сервіси мережі .
9. IP-адреси комп'ютера.
10. Принципи формування доменної адреси комп'ютера.
11. Домен верхнього рівня в США й інших країнах світу.
12. Буквені доменні адреси і цифрові IP-адреси.
13. Таблиці доменних адрес і IP-адрес на серверах DNS (Domain Name Service,).
14. Програма- браузер (browser) для різних підсистем мережі Internet (Telnet, FTP, Gopher, WWW).
15. Робота програми-браузера в режимі On-Line (на лінії) і в режимі Off-Line (за межами лінії).
16. Елементи робочого вікна браузера.
17. Налагоджування програми-браузера.
18. Гіпертекстові посилання для завантаження в браузер повної HTML-сторінки.
19. Структура WEB сторінок.
20. Проблеми кодування кирилиці.
21. Програми перегляду (браузери) Netscape Navigator і Microsoft Internet Explorer.
22. Виклик із браузера інших засобів перегляду файлів різних форматів різних підсистем мережі Internet (Telnet, FTP, Gopher).
23. Об'єкти пошуку потрібної інформації у Internet.
24. Технологія пошуку інформації у Internet. Виклик у браузер початкової сторінки пошукової системи (тематичного каталогу або автоматичного індексу).
25. Простий та розширений пошук інформації у Internet.
26. Використання складних операторів у запитах.
27. Створення поштової скриньки.
28. Робота з поштовими повідомленнями
29. Ранжирування результатів пошуку. Розмітка документа

Додаток 1

Теми завдань із Internet

1. Internet і Intranet.
2. Безпроводові мережі.
3. Безпека інформації у Internet
4. Види підключення до Internet.
5. Глобальні мережі.
6. Додатки в мережах.
7. Економічні критерії вибору провайдера Internet.
8. Захист інформації в хмарних технологіях.
9. Захист мереж.
10. Кабельні мережі.
11. Комутатори їх характеристики та функції в мережах.
12. Корпоративні мережі.
13. Криптографія в мережі Internet.
14. Локальні мережі.

15. Маршрутизатори їх характеристики та функції в мережах
16. Мережеве встаткування.
17. Мережеві сніфери.
18. Методи ефективного пошуку інформації.
19. Операційні системи в мережах.
20. Програми контролю трафіку мереж.
21. Режими моніторингу мереж.
22. Робота в пірінгових мережах.
23. Робота з поштою в мережах.
24. Розрахунок мереж.
25. Сумісна робота в Internet.
26. Технологія Fast Ethernet.
27. Функції брандмауера.
28. Функції Проксі-сервера.
29. Функції сервера доменних імен (DNS).
30. Хмарні технології.

ЛАБОРАТОРНА РОБОТА 35. СТВОРЕННЯ WEB-СТОРІНОК

Мета роботи: навчитися створювати Web- сторінки в HTML, та вивчити технологію публікації матеріалів в Інтернеті

Зміст

1. Теорія
1.1. Мова HTML
1.2. Мова HTML і WEB-дизайн
1.3. Вставка звуку і відеозображення.
1.4. Поняття про динамічні ефекти.
1.5. Web-компоузери.
1.6. Розміщення WEB-сайту в Інтернеті
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1 Мова HTML

Для створення Web-сторінок Web-дизайнери використовують гіпертекстові редактори, наприклад, HotMetal PRO, Hot Dog Professional, Netscape Editor, Webedit, HTMLWriter, HTML Assistant, HTMLed, де використовується мова HTML – Hyper Text Markup Language (мова для розмічування гіпертекстових документів). Сучасні редактори (FrontPage, програмні додатки до MS Word тощо) дають змогу створювати Web- сторінки методом конструювання без застосування кодів мови HTML (оскільки код вони створюють автоматично). Вивчаючи дану тему, ми створюватимемо Web-сторінки двома способами: 1) за допомогою мови HTML і 2) методом конструювання.

Для підготовки html – файлу можна використати текстовий редактор Notepad. Після написання html-файл потрібно зберегти на диску з деякою назвою з розширенням назви htm чи html. Програмування тут суто символічне. Програма мовою HTML (html-файл) має таку загальну структуру:

<HTML>
<HEAD>
<TITLE> Назва вікна Web- сторінки </TITLE>
</HEAD>
<BODY параметри>
<!--Далі йде текст, наприклад, такий.—>
SELPHY CP400 – компактний надшвидкісний сублімаційний принтер для прямого друку чудової якості фотографій з роздільною здатністю 300 точок на дюйм.

Для фотодруку сумісна цифрова камера підключається прямо до компактного фотопринтера SELPHY за стандартом PictBridge.

За допомогою простого меню камери можна вибрати розмір відбитку, тип матеріалу, наявність або відсутність полий і кількість копій.

</BODY>
</HTML>

Команди мови HTML називаються тегами. Теги бувають одинарними і парними. Більшість тегів є парними, як наприклад, тег означення HTML-файлу: <HTML> ... </HTML>.

Парні теги позначають початок і кінець ділянки дії відповідної команди. Теги записують у кутових дужках. Тег, що закриває ділянку дії, має косу риску (не забувайте її писати, інакше тег працюватиме неправильно). Тег може містити параметри, які користувач записує через пропуск у першому тезі, наприклад, <BODY TEXT=”red”>. Зазвичай назви тегів прийнято писати великими буквами, але можна й малими.

У середині пари тегів <HEAD>...</HEAD> описують заголовок документа. Основною частиною заголовка документа є заголовок Windows-вікна, який пишуть в середині пари тегів <TITLE>...</TITLE>.

У середині пари тегів <BODY параметри>...</BODY> записують (тобто програмують) те, що має відображатися у вікні браузера. Щоб на екрані відобразити звичайним способом стандартний текст, жодного програмування не потрібно – достатньо набрати цей текст. Якщо ж дизайнер хоче подати текст спеціальним чином, щоб він якнайкраще виглядав, потрібно застосувати до тексту теги форматування. У цьому, зокрема, і полягає суть програмування мовою HTML.

Розглянемо основні параметри тегу BODY:

BACKGROUND = "шлях до графічного файлу" – задає картинку для тла;

BGCOLOR = "white" – задає білий колір тла, якщо не використовується тло-картинка;

TEXT = "black" – задає колір тексту (тут – чорний) на сторінці.

Тег <!-- текст --> позначає коментар. Текст у середині тегу виводитися на екран не буде. Коментар можна писати також у середині парного тегу <COMMENT> текст-коментар </COMMENT>.

Оформлення тексту для Web-сторінок

Розглянемо теги, які використовують для форматування тексту.

Спочатку розглянемо основні одинарні теги для розміщення тексту.

<P> — цей тег означає початок нового абзацу, але його прийнято записувати в кінці попереднього. Наступне речення починатиметься з нового, вирівняного до лівого краю, абзацу без відступу.

 — наступний за цим тегом текст буде наведено у новому рядку без пропуску рядка.

<HR> — буде проведена горизонтальна лінія.

Розглянемо парні теги форматування символів тексту:

<B> текст </B> — напівжирний шрифт тексту;

<I> текст </I> — шрифт-курсив;

<U> текст </U> — підкреслений шрифт;

_{текст} — нижній індекс, наприклад, H2O;

^{текст} — верхній індекс, наприклад, 1а вулиця, а2;

<BIG> текст </BIG> — великий шрифт;

<SMALL> текст </SMALL> — малий шрифт;

<EM> текст </EM> — виокремлений курсивом текст (те саме, що тег I);

<B> <I> текст </I> </B> — напівжирний курсив. Цей приклад демонструє застосування принципу вкладення тегів.

Зауважимо, що тег <P> може використовуватися як парний: <P> текст абзацу </P>.

Окремим типом абзацу є заголовок. Є шість видів заголовків, які відрізняються розмірами символів:

Теги	Результат на екрані
<H1>Заголовок 1</H1>	Заголовок 1.
<H2>Заголовок 2</H2>	Заголовок 2.
<H3>Заголовок 3</H3>	Заголовок 3.
<H4>Заголовок 4</H4>	Заголовок 4.
<H5>Заголовок 5</H5>	Заголовок 5.
<H6>Заголовок 6</H6>	Заголовок 6.

Заголовок за замовчуванням вирівнюється до лівого краю вікна.

Якщо вирівнювання заголовка чи іншого елемента на сторінці потрібно задати явно, то використовують теги вирівнювання:

<CENTER> елемент </CENTER> — вирівнювання до центру;

<LEFT> елемент </LEFT> — вирівнювання до лівого краю;

<RIGHT> елемент </RIGHT> — вирівнювання до правого краю.

Зауваження. Теги заголовків не варто використовувати для створення звичайних абзаців з різними розмірами шрифту.

1.2. Мова HTML і WEB-дизайн

1. Тег завдання параметрів шрифту FONT.

Щоб задати назву конкретного шрифту, його розмір і колір, використовують парний тег FONT з параметрами FACE, SIZE та COLOR, наприклад,

<FONT FACE = "Decor, Arbat, Kudriashov" SIZE = +2 COLOR = "red"> текст </FONT>

Якщо на комп'ютері клієнта встановлено шрифт Decor, то він буде застосований до даного тексту, інакше браузер застосує шрифт Arbat чи Kudriashov, інакше – деякий свій стандартний шрифт, наприклад, Times New Roman.

Розміри символів шрифту можуть бути від 1 до 7. Розмір 3 вважається стандартним, він орієнтовно відповідає 10 пунктам. Розмір 7 є найбільшим. Число 2 як значення параметра SIZE означає другий розмір шрифту, число +2 означає, що розмір шрифту має бути на дві одиниці більший, ніж стандартний, тобто п'ятий, число –2 означатиме перший розмір шрифту — на дві одиниці менший, ніж стандартний.

Колір тексту буде червоний. Основні кольори мають такі назви:

black	чорний	white	білий
gray	темно-сірий	silver	сірий
maroon	малиновий	red	червоний
green	зелений	lime	яскраво-зелений
navy	темно-синій	blue	синій
teal	бірюзовий	aqua	блакитний
purple	бузковий	fuchsia	рожевий
olive	темно-зелений	yellow	жовтий

Різних можливих відтінків цих кольорів є 16 мільйонів. Відтінки задають спеціальними шістнадцятковими кодами, як це прийнято в графічних редакторах, наприклад, один з відтінків сірого кольору має код #ff7800.

Зауваження. У тексті можна використовувати так званий мнемо-код &quot, який відобразить на екрані лапки. Замість мнемо-коду можна використати числовий код &#34. Коди інших спецсимволів (<, >, & тощо) можна знайти у довідниках. Ще одна новинка: адреси тепер прийнято записувати в парному тезі <ADDRESS>...</ADDRESS>.

2. Створення списків.

Є три типи списків: ненумерований, нумерований, означення. Список може мати заголовок, який охоплюють тегами <LH>...</LH>, наприклад,

<LH>Це заголовок списку</LH>.

Ненумерований список утворюють за допомогою парного тегу <UL> ...</UL> і одинарних тегів <LI>, наприклад, так:

```
<LH> Мої улюблені предмети:</LH>
<UL>
<LI>інформатика
<LI>англійська мова
<LI>історія
</UL>
```

На екрані отримаємо:

Мої улюблені предмети:

- інформатика
- англійська мова
- історія

Нумерований список створюють за допомогою парного тегу <OL>... </OL> з необов'язковим параметром TYPE і одинарних тегів <LI> так:

<LH> Мої улюблені предмети:</LH>
<OL TYPE="1">
<LI>Інформатика
<LI>Англійська мова
<LI>Історія
</OL>

На екрані отримаємо:

Мої улюблені предмети:

1. Інформатика
2. Англійська мова
3. Історія

Значення "i" чи "I" параметра TYPE задає нумерацію римськими малими (i, ii, iii, iv,...) чи великими (I, II, III, IV, ...) цифрами, а значення "a" чи "A" латинськими малими (a, b, c, d, ...) чи великими (A, B, C,...) літерами.

Список означень використовують для тлумачення термінів, створення словників тощо. Його утворюють за допомогою парного тегу <DL>...</DL> і двох одинарних тегів <DT> і <DD> так:

<LH>Заголовок</LH>
<DL>
<DT> термін
<DD> тлумачення 1
<DD> тлумачення 2
...
</DL>

Наприклад,

<LH>Я знаю такі нові терміни:</LH>
<DL>
<DT> HTML
<DD> <I>мова для розмічування гіпертекстових Web-сторінок</I>
<DT> браузер
<DD> <I>програма для перегляду Web-документів</I>
<DT> тег
<DD> <I>засіб для записування команд мовою HTML</I>
</DL>

На екрані отримаємо:

Я знаю такі нові терміни:

HTML
мова для розмічування гіпертекстових Web-сторінок
браузер
програма для перегляду Web-документів
тег
засіб для записування команд мовою HTML

3. Створення таблиць.

Таблиці створюють за допомогою таких тегів:

<TABLE параметри>
<TC>Заголовок таблиці</TC>
Тут пишемо теги для заповнення
клітинок таблиці рядок за рядком
</TABLE>

Для заповнення клітинок таблиці використовують такі парні теги (зауважимо, що закриваючі теги можна опускати):

<TR>...</TR> формують рядок таблиці;

<TH>текст</TH> формують клітинку-заголовок рядка чи стовпця;

<TD>текст</TD> формують текст кожної клітинки.

Заголовки рядків та стовпців виводитимуться товстішим шрифтом. Створимо на Web-сторінці таблицю-витяг з відомості успішності студента за три перші семестри з трьох предметів: інформатики, математики та історії:

```
<CENTER>
<TABLE BORDER=3 BGCOLOR=" yellow" BORDER-COLOR="green">
<TC><I>Мої оцінки за три семестри:</I></TC>
<TR> <TH></TH>
<TH>I семестр </TH>
<TH>II семестр </TH>
<TH>III семестр</TH>
</TR>
<TR> <TH ALGN=”left”>Інформатика</TH>
<TD>100/TD>
<TD>100/TD>
<TD>100/TD>
 </TR>
<TR> <TH ALGN=”left”>Математика</TH>
<TD>90/TD>
<TD>90</TD>
<TD>90</TD>
</TR>
<TR> <TH ALGN=”left”>Історія</TH>
<TD>95</TD>
<TD>88</TD>
<TD910</TD>
</TR>
</TABLE>
</CENTER><P>
```

Щоб об'єднати у рядку декілька послідовних клітинок, наприклад, дві в одну, у відповідному першому тезі <TH> чи <TD> записують параметр ROWSPAN=2.

Щоб об'єднати у стовпці дві клітинки в одну, використовують параметр COLSPAN=2.

Колір рамки таблиці задають параметром BORDERCOLOR="колір рамки", а колір тла клітинок параметром BGCOLOR="колір фону". Товщину рамки в пікселях задають параметром BORDER=”товщина рамки", наприклад, 3. Якщо значенням параметра є число нуль або параметра немає, то рамка буде невидимою.

4. Вирівнювання елементів.

За замовчуванням більшість елементів на сторінці, наприклад, текст, таблиці, списки, текст у клітинках таблиці, браузер вирівнює до лівого краю екрана чи клітинки. Часто тип вирівнювання потрібно змінити. Лінії можна вирівнювати до центру екрана чи до правого краю. Таблиці вирівнюють відносно екрана або відносно тексту, який її облямовує. Текст у клітинках таблиці вирівнюють до центру чи до країв у горизонтальному чи вертикальному напрямках. Для цього до об'єктів застосовують теги вирівнювання CENTER, LEFT, RIGHT або в тегах <HR>, <TABLE>, <TH>, <TD> та в інших використовують параметр ALIGN зі значеннями

"left" зліва,

"center" до центру,

"right" справа,
"top" вгорі,
"middle" посередині,
"bottom" внизу.

Останні три значення може мати також параметр VALIGN.

Для вдалого розташування таблиць чи рисунків варто проекспериментувати з параметрами WIDTH і HEIGHT, які задають ширину і висоту елемента в пікселях або відсотках до розмірів усього екрана, наприклад, <TABLE WIDTH=300> задає ширину таблиці 300 пікселів; <TABLE WIDTH=50%> задає ширину таблиці у півсторінки у горизонтальному напрямку.

Для проведення ліній різної довжини і товщини застосовують параметри WIDTH і SIZE, наприклад, тег <HR SIZE=30 COLOR="red"> замість звичайної лінії дає червону полосу товщиною 30 пікселів.

Довідка. Інформацію можна подати у вигляді таблиці без рамок за допомогою парного тегу <PRE>...</PRE>. Текст у середині цього тегу оформляють засобами табуляції. Браузер такий текст переформатовувати не буде.

5. Вставка графічних і відеофайлів.

Графічні зображення (фотографії, картинки, піктограми тощо) зберігаються на серверах в окремих файлах з розширеннями bmp, jpg, gif та іншими і відображаються на Web-сторінці за допомогою команди, що описується одинарним тегом <IMG> з параметрами:

<IMG SKR="адреса графічного файлу" ALT="альтернативний текст" ALIGN="left" WIDTH=240 HEIGHT=200>

Обов'язковим є лише перший параметр SRC. Альтернативний текст – це текст, який виводитиметься замість картинки, якщо браузер не може прийняти графічний файл або якщо режим відображення графіки вимкнено. Параметр ALIGN задає місце розташування картинки на екрані, а параметри WIDTH і HEIGHT – її розміри за шириною і висотою в пікселях або відсотках.

Зображення можна подати в рамці (що рекомендують робити), якщо його використовуватимуть як гіперпосилання. Для створення рамки навколо зображення призначений параметр BORDER="товщина рамки в пікселах".

Праворуч і ліворуч від картинки, яку облямовує текст, можна зробити вільний простір: HSPACE = "кількість пікселів". Можна створити вільний простір також над і під рисунком: VSPACE = "кількість пікселів".

За допомогою тегу IMG можна вставити також відеофільм, який запускатиметься в момент відкриття Web-сторінки:

<IMG DYNSRC="адреса відео-файлу">.

6. Адреси файлів.

Для виклику віддалених файлів, тобто файлів, які є на серверах у мережі Internet, адресу записують із зазначенням назви протоколу доступу http і URL-адреси файлу, наприклад,

"http://www.polynet.lviv.ua/ourpage.htm ".

Для доступу до файлів на локальному диску використовують протокол доступу file:

"file:///диск:/ шлях до файлу".

Наприклад, "file:///d:/mycatalog/mypage.htm".

Назву протоколу можна інколи не писати, наприклад,

SRC="c:/windows98/JIec.bmp".

Якщо графічні чи інші файли є в тому ж каталозі, що основний html-файл, то достатньо зазначити лише назву файлу, наприклад,

SRC= "myfoto.gif".

Якщо файл є в деякому сусідньому каталозі images, то шлях до нього можна подати так: "../images/myfoto.gif". Отже, тег IMG може мати такий конкретний вигляд:

<IMG SRC="c:/windows98/Лес.bmp" ALT="Ліс">.

7. Вставка гіперпосилань.

Гіперпосилання є двох видів: 1) на файл; 2) на деяке місце на даній сторінці: початок сторінки (top), кінець сторінки (bottom), на позначений текст. Гіперпосилання вставляють за допомогою парного тегу <A>...</A> з параметром HREF = "адреса файлу". Тут замість адреси можуть стояти слова top чи bottom чи текст, що є позначкою.

Гіперпосиланням може бути текст або деяке графічне зображення. Розглянемо випадок, коли гіперпосиланням є текст. Нехай у реченні "Мене звуть Олена" слово "Олена" потрібно зробити гіперпосиланням на файл "file2.htm" чи "newinf.htm", що містить додаткові відомості про Олену. Це роблять так:

Мене звуть <A HREF = "newinf.htm"> Олена</A>.

У результаті цього на Web-сторінці слово Олена буде підкреслене і зображене іншим кольором. Колір гіперпосилання визначається у тезі BODY параметром LINK = "колір". Крім цього корисними є ще два параметри:

VLINK= "інший колір"

– змінює колір гіперпосилання на інший після першого використання;

ALINK = "ще інший колір"

– змінює колір щойно активізованого гіперпосилання на ще інший.

Тепер розглянемо як деяке графічне зображення зробити гіперпосиланням. Для цього в середині тегу <A>...</A> потрібно використати тег IMG. Наприклад, щоб фотографія Олени, що є у файлі "olena.gif", була в рамці й стала гіперпосиланням на файл new-inf .htm, пишуть так:

<A HREF = "newinf.htm"><IMG SRC = "olena.gif" BORDER =8 ></A>

Клацнувши на Web-сторінці на фотографії Олени, відкриємо файл newinf.htm з додатковою інформацією про неї.

Будь-яку піктограму (картинку) можна вставити автономно чи як гіперпосилання, оскільки вона зберігається також у графічному файлі.

Розглянемо другий тип гіперпосилань – посилання в межах сторінки. Спочатку потрібно позначити місце на сторінці, куди здійснюватиметься перехід. Якщо з деякого місця перехід має виконуватися на початок сторінки, то в те місце html-файлу, що відповідає початку сторінки, вводять тег, який називається якорем:

<A NAME="#початок"></A>.

Аналогічно позначають деяке місце в кінці файлу:

<A NAME="#кінець"></A>.

Якір можна кинути в будь-якому місці тексту так:

<A NAME="#моя позначка"x/A>.

Тепер на сторінці розміщують гіперпосилання на створені позначки (якори):

<A HREF="#початок' або "#кінець" або "#моя позначка"> текст гіперпосилання </A>.

Якщо одна сторінка займає декілька екранів, то в кінці сторінки варто вставити гіперпосилання для переходу на початок, наприклад, так:

А тепер можете перейти <A HREF="#початок">на початок</A> сторінки.

1.3. Вставляння звуку і відеозображення.

Важливо пам'ятати, що звукові файли мають розширення назв au, wav, mid, midi, ra, а відеофайли – avi, vivo, mpeg. Щоб вставити звук чи відео, достатньо як значення параметра HREF у тезі гіперпосилання задати шлях до відповідного звукового чи відеофайлу, який вже є на диску, наприклад,

Тепер <A HREF="mysound.wav"> послухайте мене (150К) </A>.

Текст «послухайте мене (150К)» стане гіперпосиланням, клацнувши на якому можна почути привітання, застереження, деяку інформацію, яка була заздалегідь записана, наприклад, за допомогою програми Фонограф у файл "mysound.wav" обсягом 150 Кбайт. Оскільки звукові та відеофайли завантажуються довго, рекомендують зазначати у гіперпосиланнях їхні обсяги в кілобайтах.

Щоб звуковий чи відеоефект повторювався декілька разів, наприклад, 2, у тезі <A> використовують параметр LOOP=2.

Щоб звук з деякого файлу пролунав у момент запуску сторінки, потрібно використати тег <BGSOUND SRC = "адреса звукового файлу">. Інший спосіб
використайте тег <EMBED SRC=" адреса звукового файлу"> і, окрім звукового ефекту, отримаєте на екрані магнітофонну панель для регулювання тривалості й сили звуку, припинення звучання, продовження тощо.

1.4. Поняття про динамічні ефекти.

Динамічними називаються ефекти, коли графічні зображення на Web-сторінці змінюються з часом, елементи сторінки змінюють розміри або навіть свій зміст після клацання над ними мишею, текст «біжить» уздовж екрана тощо.

Розглянемо ефект тексту, який біжить у полосі, що має висоту HEIGHT ="висота в пікселях" і тло BGCOLOR ="колір тла". Ефект створюється за допомогою парного тегу <MARQUEE>...</MARQUEE>, а саме:

<MARQUEE BGCOLOR="green" HEIGHT = 40> Олена Олена</ MARQUEE>

Обидва слова "Олена Олена" будуть пробігати в полосі справа наліво, заходитимуть за край екрана і з'являтимуться знову справа. Даний тег рекомендують застосовувати до заголовків сторінки.

Ефект відбивання від країв екрана забезпечує параметр BEHAVIOR = "alternate", а зупинити рядок біля лівого краю екрана може значення цього параметра "slide". Значення "right" параметра DIRECTION забезпечить ефект руху у протилежний бік.

Обмеження кількості проходів, наприклад, числом 5, задається параметром LOOP=5. Полосу можна відцентрувати за допомогою параметрів HSPASE і VSPACE. Швидкість руху задає параметр SCROLLAMOUNT=3, де конкретне значення вибирають з діапазону від 1 (повільно) до 10 (швидко).

Інші динамічні ефекти створюють за допомогою процедур з використанням мов програмування Visual Basic Script чи JavaScript.

Зауваження. Немає єдиного стандарту мови HTML. Деякі теги чи їхні параметри не діють у всіх браузерах. Деякі теги і параметри для різних браузерів називаються по-різному. Якщо в написанні тегу, назви параметра чи в його значенні допущено синтаксичну помилку, то тег чи параметр не діятимуть.

1.5. Web-компоузери.

Загальна назва програм для автоматизованого створення Web-сторінок без застосування користувачем мови HTML – Web-компоузери. Розглянемо відповідні можливості Web-додатків до програми MS Word. Щоб створити Web-сторінку чи цілий Web-сайт, потрібно під час створення нового документа перейти на закладку Web-сторінки і скористатися майстром чи створити нову сторінку. У другому випадку алгоритм дій дизайнерів такий:

командою Формат => Фон задають колір тла чи спосіб замальовування екрана деякою текстурою з меню;

вводять текст, вибираючи шрифт, його розмір, колір, вирівнювання тощо;

створюють списки як у звичайному текстовому редакторі;

вставляють лінії командою Вставити => Горизонтальна лінія => вибирають вигляд лінії з меню;

за допомогою команди Таблиця створюють і форматують таблиці;

використовують команду Вставити для вставляння картинок, фотографій, відеофайлів, звуку, гіперпосилань, біжучих рядків тощо;

записують створений файл на диск і переглядають його браузером.

Зауваження. Програма-компоузер автоматично створює html-файл, який можна переглянути і модифікувати з метою внесення деяких змін у Web-сторінку. Щоб створити мовою html цікаві сторінки вручну, потрібно мати адреси графічних файлів для тла сторінки, горизонтальних ліній тощо.

1.6. Розміщення WEB-сайту в Інтернеті

В Інтернеті існують безкоштовні сервіси, які дозволяють не тільки з конструктора, «зібрати» свій власний сайт, але й опублікувати його, прописати в пошуковій системі й у міру розвитку сайту одержувати під нього практично необмежений простір.

Варіантів для розміщення web-сторінок (хостинга) досить багато. Якщо сайт являє собою комерційний проект, то найкраще обзавестися власним сервером і високошвидкісним виходом у мережу або орендувати місце в компаній, що можуть забезпечити власника сайту всім необхідним. Для навчального проекту в мережі можна знайти величезну кількість посилань на free web pages, де провайдери надають своїм клієнтам безкоштовне місце під сторінку, наприклад див. табл. 1:

На сервері http://www.44.ru/cgi-bin/start.pl є можливість установлювати свої власні скрипты й доступ до них за FTP.

Для швидкого створення сайту, що не претендує на роль чого-небудь суперпрестижного, досить зручний сервер http://www.narod.ru/, усі користувачі якого одержують при реєстрації 100 Мегабайт дискового простору, який згодом може бути автоматично збільшений до великого обсягу.

Таблиця 1

Перелік можливих сайтів для безкоштовного розміщення WEB сторінки

781313.ru/site_cat.php	Promotion.su
cat.rusbic.ru	dmoz.org
catalog.deport.ru	povezlo.su
catalog.monty74.ru	Nofollow.ru
catalog.rufox.ru	Webplus.info
catalog.yuga.ru	Rubo.ru
dir.ikernel.org	piter.nev.ru
faststart.ru	dir.org.ru
gendilana.ru/cncat	Zabor.com
goon.ru	rosfirm.ru
http://chttpru/	http://www.httpava.ru/
http://narod.ru/	http://www.az.ru/
http://www.agava.ru/	http://www.lgg.ru/
http://www.az.ru/	http://www.zk.ru/
http://www.bizland.com/	http://www.intergrad.com/
http://www.crosswinds.net/	http://www.dp.ru/
http://www.fortunecity.com/	http://www.netcity.ru/
http://www.freeservers.com/	http://www.httpail.ru/
http://www.fsn.net/	http://httping.agava.ru/
http://www.geocities.com/	http://www.ussr.to/
http://www.newmail.ru/	http://i-connect.ru/
http://www.spree.com/	http://www.viaduk.net/
http://www.tripod.com/	http://http.vibor.ru/
http://www.virtualave.net/	http://www.artnet.ru/generator

http://www.xoom.com/	http://windoms.sitek.net/
ilinks.ru	Fis.ru
in-catalog.com	linkstroy.ru
irdir.info	ins.org.ru
lermont.ru	Liveinternet.ru
nobius.ru	catalogr.ru
openlinks.ru	rosmarket.ru
precat.ru	yaca.yandex.ru
refer.ru	yp.piter.com
sabrina.ru	www.yell.ru
s-catalog.ru	miruslug.info
t0psites.com	Webproverka.com
topstat.ru	regtorg.ru
webcat.info	www.spr.ru
webest.info	Rambler TOP 100
wmcap.ru	Vsego.ru

Для того щоб одержати ці можливості, необхідно завантажити сторінку http://www.narod.yandex.ru/, де відразу ж буде запропоновано зайняти ім'я для нового сайту.

Ім'я сайту повинне мати вигляд: ваше_ім'я.narod.ru. Довжина імені може досягати 14 знаків, крім букв дозволяється використовувати тире й цифри. Користувачі пошти www.yandex.ru мають можливість автоматично створити персональний сайт, ім'я якого буде збігатися з іменем їх поштового логіна.

Після реєстрації можна відправитися в «майстерню», де перебуває безліч шаблонів для створення різних тематичних сторінок: «Моя головна сторінка», «Про мене», «Мої інтереси» і т.д.

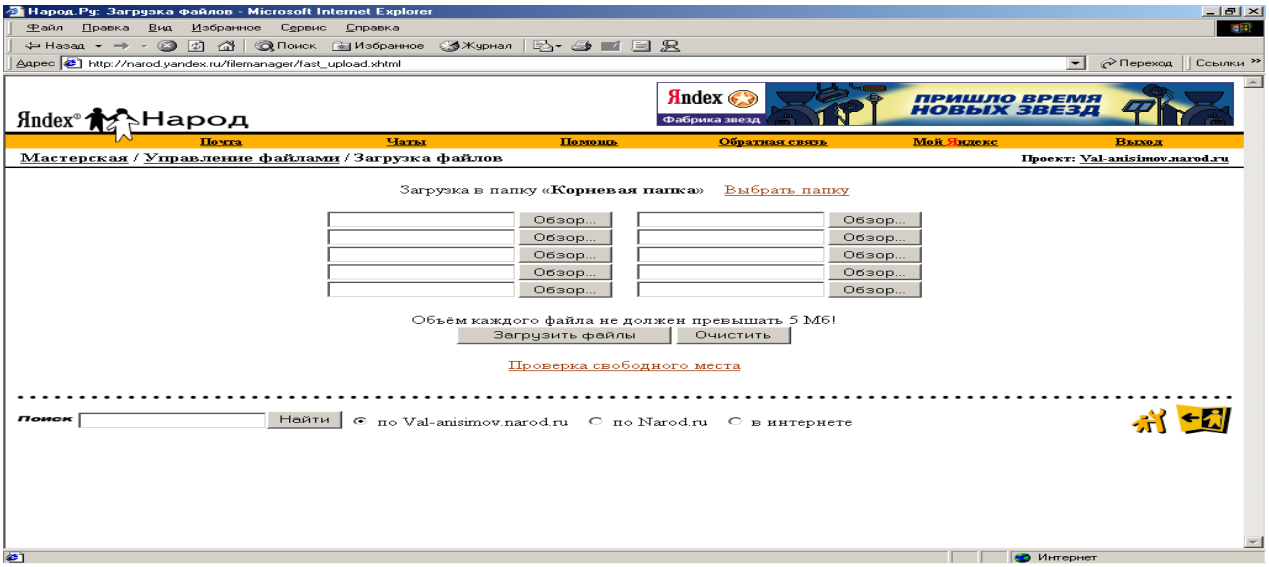


Рис. 1. Вікно завантажити файли

Якщо Вас не влаштовують ті шаблони, які пропонує система, Ви можете використовувати простий набір інструментів і створити свій власний дизайн. Не залишаючи розділ «майстерня», можна одержати доступ і до Html-Коду сторінки, що редагується, однак створювати власний дизайн із використанням мережного інструментарію чи навряд доцільно, тому що поки Ви будете експериментувати з дизайном, Вам доведеться платити за трафік.

На http://www.narod.ru/ працює так звана служба модераторів, яка відслідковує відповідність сайтів користувацькій угоді. Крім роботи з усунення порушників на http://www.narod.ru/ також існує ценз для різних аудиторій. За замовчуванням робота з

пошуком і каталогом відбувається в «сімейному» режимі, тобто людина не бачить «недитячі» сайти, до яких ставиться еротика, фінансові піраміди й тому подібні.

Тому що ніхто не обмежений необхідністю використовувати наявні шаблони – можна створити сайт із використанням будь-якого редактора або перенести на http://www.narod.ru/ готовий сайт із будь-якого іншого місця. Для виконання лабораторної роботи необхідно використовувати раніше створений макет сайту.

Для цього необхідно також, не залишаючи розділ «майстерня», вийти в режим «керування файлами й Html-Редактор», потім у режим «завантажити файли» і перекачати раніше створені Html-Файли зі свого комп'ютера на сервер (рис. 1). При цьому слід перейменувати головну сторінку сайту на index.htm і перевірити гіперпосилання, які тепер повинні адресуватися до сторінок сайту, які розташовані на сервері http://www.narod.ru/, а не на жорсткому диску користувача.

Щоб відредагувати свою сторінку, зайдіть в «майстерню», у розділ «керування файлами». Відзначте сторінку, яку Ви прагнете відредагувати, і натисніть кнопку «редагувати». Ви потрапите в шаблон вашої сторінки, де зможете внести необхідні зміни. Для того щоб вилучити сторінку, треба відзначити її й нажати кнопку «Вилучити».

Можна змінити сторінку в тому ж розділі «керування файлами», за допомогою кнопки «властивості» (у вікні властивостей треба вибрати закладку «текстовий редактор»). При цьому треба мати на увазі, що якщо потім Ви розв'яжете відредагувати цю сторінку за шаблоном, зміни, внесені Вами в текстовому редакторі, будуть загублені.

Природно, оригінальну сторінку, зроблену не за стандартним шаблоном, можна відредагувати на комп'ютері користувача, а потім знову завантажити її на сервер.

Якщо не працюють посилання на файли, перевірте, чи правильно Ви прописали шляхи до файлів, на які у Вас не працюють посилання: порядок і імена папок, ім'я файлу і його наявність, а також зверніть увагу на правильність використання регістру букв при написанні назв папок і файлів.

2. Хід роботи

Створити за допомогою HTML Web-сторінку яка включала б всі елементи сторінки розглянуті в розділі 1. Помістити сторінку на одному з Web-сайтів

3. Контрольні питання

1. Які гіпертекстові редактори можна використовувати для створення Web-сторінок Web-дизайнери гіпертекстові редактори?
2. Яку загальну структуру має html-файл?
3. Як інакше можна назвати теги в мові HTML, яких типів вони бувають?
4. Як задати шрифти в мові HTML?
5. Як створити списки в мові HTML?
6. Як створити таблиці в мові HTML?
7. Як провести вирівнювання елементів в мові HTML?
8. Як провести . вставку графічних і відеофайлів в мові HTML?
9. Як провести вставку звуку і відеозображення в мові HTML?
10. Як провести вставку гіперпосилань в мові HTML?
11. Що таке динамічні ефекти в мові HTML?
12. Що таке Web-компоузери?
13. Як розмістити створену Web-сторінку в мережі?
14. Як створити Web-сторінку на сайті?

ЛАБОРАТОРНА РОБОТА № 36. РОБОТА З ГРУПАМИ НОВИН

Мета роботи: отримати практичні навички по роботі з новинами

Зміст

1. Теорія
1.1. Загальні відомості про групи новин (телеконференції)
1.2. Підписка на групи новин
1.3. Завантаження, перегляд, сортування, фільтрація та пошук повідомлень
1.4. Підготовка і відправлення повідомлень у групу новин
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Загальні відомості про групи новин (телеконференції)

Групи новин (їх також називають телеконференціями) – це засіб, що дозволяє людям, що мають спільні інтереси, спілкуватися між собою за допомогою електронної пошти. Наприклад вчені, що працюють в певній галузі науки, мають свою групу новин, через яку вони обмінюються науковими статтями, різними оголошеннями, ведуть дискусії тощо. На групі новин автолюбителів можна знайти оголошення про продаж і купівлю автомобілів, запчастин, іншу подібну інформацію. Якщо, наприклад, у вас виникли складні технічні проблеми з вашим автомобілем, то ви можете послати в групу новин своє запитання, і серед її читачів знайдеться багато охочих, що надішлють вам відповідь чи дадуть пораду. Отже групи новин – це своєрідний варіант клубів спілкування за інтересами, в роботі яких можуть брати участь усі бажаючі. Для цього не треба вступати ні в які організації чи сплачувати членські внески.

Групи новин бувають керовані і некеровані. Керівник – це досвідчений фахівець, який переглядає повідомлення, що надійшли у групу новин, і вирішує, чи відповідають вони її тематиці і чи варто їх тут публікувати. Керівник часто сам відповідає на запитання дописувачів і публікує в групі новин свої статті. Переважна більшість груп новин є некерованими. Будь-яка інформація, що надійшла на їх адресу, публікується в них автоматично.

Термін зберігання повідомлень на сервері новин обмежений. Через певний час інформація, що втратила актуальність, вилучається, звільняючи місце для нових надходжень.

Групи новин створюються і припиняють свою роботу в міру того, як виникає чи зникає потреба в їх існуванні. Останнім часом їх популярність взагалі знизилась, бо можливість аналогічного спілкування надається сервісом WWW, через так звані форуми. Досить часто в кінці статті чи іншого повідомлення можна знайти посилання на веб-сторінку форуму, де всі бажаючі можуть задати питання автору, взяти участь в обговоренні, поділитися власним досвідом тощо.

Можливо, в майбутньому WWW поглине і цей сервіс, проте на сьогодні групи новин ще мають перспективу хоча б тому, що інформація в них поширюється через електронну пошту, безкоштовне користування якою сьогодні загальнодоступне, тоді як можливості безкоштовного доступу до WWW ще дуже обмежені.

1.2. Підписка на групи новин

Щоб отримати доступ до сервера новин, треба вибрати в меню Outlook Express **Сервис – Учетные записи – Новости – Добавить – Новости**… Потім ввести своє ім’я, електронну адресу та адресу сервера новин, наприклад news.lucky.net. Далі натиснути кнопки **Готово**, Закрити та дати позитивну відповідь на пропозицію завантажити список груп новин даного сервера. Цей список можна також викликати, натиснувши на панелі

інструментів кнопку **Группы новостей**, чи вибравши однойменну опцію контекстного меню папки даного сервера новин, яка щойно з'явилась на панелі папок.

Якщо список груп новин дуже довгий, то в ньому можна провести фільтрацію. Наприклад, якщо вас цікавлять новини, що стосуються комп'ютерів чи музики, то можна відфільтрувати назви груп за ознакою наявності в них слів **comp** чи **music.**

Щоб підписатися чи відмовитись від підписки на отримання повідомлень певних груп новин, треба в цьому списку двічі клацнути мишкою по обраній групі, або виділити її і скористатися кнопками **Подписаться** чи **Отказаться** от подписки. В результаті на панелі папок вашої програми, в папці сервера новин будуть створюватися чи вилучатися папки обраних вами груп.

1.3. Завантаження, перегляд, сортування, фільтрація та пошук повідомлень

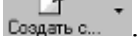
Звичайні налаштування програми забезпечують завантаження і оновлення переліку повідомлень у папках груп новин тоді, коли ви відкриваєте ці папки для перегляду. Так само й текст повідомлення завантажується тоді, коли ви виділяєте його заголовок у переліку. Отже, ви можете переглядати повідомлення в папках груп новин так само, як ви переглядаєте листи в інших папках програми.

Як правило повідомлень у папці дуже багато, тому для ефективної роботи з ними треба вміти використовувати різні варіанти представлення, сортування, фільтрації та пошуку повідомлень. Звісно, повідомлення можна сортувати так само, як і листи, – клацнувши мишкою по відповідному заголовку стовпця в переліку. Однак робота з повідомленнями має й деякі особливості. Наприклад в групу новин можуть надходити відгуки на повідомлення, розміщені тут раніше. В переліку повідомлень такі повідомлення і відгуки на них зручно тримати об'єднаними в списки, які можна згортати і розгортати за допомогою мишки. Для цього треба встановити позначку в меню **Вид – Текущее представление – Сгруппировать сообщения по теме обсуждения**. Якщо, наприклад, ви хочете швидко переглянути відгуки на своє повідомлення в групі новин, виберіть там же опцію **Отобразить ответы на мои сообщения.** Багато інших корисних можливостей для роботи з повідомленнями у групах новин ви знайдете в меню **Сервис – Правила для сообщений – Новости**.

Пошук повідомлень в групі новин виконується за ключовими словами, розміщеними в полі **Тема**, за допомогою опції **Найти** в меню **Правка**. Тому поле **Тема** має бути максимально інформативним. Якщо, наприклад, ви надсилаєте в групу новин оголошення про продаж автомобіля, то слово продаю, марку і найголовніші характеристики автомобіля слід вказати у цьому полі, бо саме, переглядаючи інформацію в полі **Тема**, користувач вирішує, чи варто взагалі завантажувати це повідомлення. На відміну від листів, повідомлення в групу новин з незаповненим полем **Тема** програма Outlook Express взагалі не надсилає.

1.4. Підготовка і відправлення повідомлень у групу новин

Виконується аналогічно підготовці й відправленню листів, хоча набір кнопок на панелі інструментів при роботі з групами новин відрізняється від набору кнопок при роботі з листами. Так само й поля редактора, що застосовується для підготовки тексту повідомлень, дещо відрізняються від полів у редакторі листів.

Якщо ви бажаєте направити в групу новин зовсім нове повідомлення, яке, можливо, започаткує там нову тему для обговорення, то виділіть цю групу на панелі папок і натисніть кнопку **Создать сообщение** 

. Якщо ж ви відповідаєте на інше повідомлення в цій групі новин, тоді треба виділити це повідомлення в переліку і натиснути одну з кнопок 

.

Перша з них, що називається **Ответить в группу**, використовується щоб надіслати вашу відповідь в групу новин, отже з нею зможуть ознайомитись усі, хто підписався на цю групу.

Друга кнопка **Ответить отправителю** служить щоб надіслати звичайного листа авторові даного повідомлення. В групу новин нічого не передається.

Третя – **Ответить всем** надсилає вашу відповідь і в групу новин і автору.

Після натискання кнопки відкривається вікно відповідного редактора, де частина полів може бути вже заповнена деякою попередньою інформацією, яку ви можете скоригувати і доповнити. Закінчивши редагування повідомлення, натисніть кнопку **Отправить**.

2. Хід роботи

Перш ніж розпочати роботу з групами новин перегляньте декілька форумів, щоб мати уявлення про аналогічний сервіс на WWW. Відвідайте, наприклад:

http://itc-ua.com/forums/ – форуми з комп'ютерної справи,

http://tour.com.ua/wwwboard – форум, присвячений туризму, подорожам,

http://tour.com.ua/uitt – дошка об’яв,

http://www.1plus1.tv/forum/index.php3?f=0 – форуми на сайті каналу 1+1,

http://autoua.net/auto_f/wwwthreads.php?Cat= – форуми для автолюбителів,

http://forum.hostmaster.net.ua/ – тестові форуми.

Надішліть декілька власних повідомлень на будь-який тестовий форум.

Запустіть програму Outlook Express, встановіть на ньому обліковий запис якогось сервера новин, наприклад news.lucky.net та підпишіться в ньому на цікаві для вас групи новин і обов’язково декілька тестових груп. Ці групи, що мають у своїй назві слово test. Вони створені спеціально для того, щоб на них тренуватися працювати з групами новин.

Вибірково перегляньте повідомлення в групах новин. Випробуйте всі варіанти фільтрації й сортування повідомлень, що є в меню **Вид**.

Випробуйте всі можливості пошуку, представлені в меню **Правка**.

Надішліть нове повідомлення та візьміть участь у обговоренні наявних повідомлень у тестових групах новин. Враховуючи, що надіслані повідомлення можуть з’являтися в групах новин з певним запізненням, випробуйте декілька тестових груп, та виберіть для подальшої роботи ту, де повідомлення з’являються швидше.

В кінці заняття покажіть викладачеві папки з одержаними і відправленими листами і вашими повідомленнями в групах новин.

3. Контрольні питання

1. Що таке групи новин і якими вони бувають?
2. Чим відрізняються групи новин від форумів на World Wide Web?
3. Як підписатися і відмовитись від підписки на групу новин?
4. Як відбувається завантаження повідомлень з групи новин у ваш комп'ютер?
5. Як можна сортувати і фільтрувати дані у групах новин?
6. Як виконується пошук інформації в групах новин?
7. Як надіслати повідомлення в групу новин?

ЛАБОРАТОРНА РОБОТА 37. РОБОТА В ПІРІНГОВІЙ МЕРЕЖІ

Мета роботи: отримати навички роботи в пірінговій мережі

Зміст

1. Теорія
1.1. Вступ
1.2. Програма BitComet
1.3. Програма µTorrent
2. Хід роботи
3. Контрольні питання

1. Теорія

1.1. Вступ

Одна із сфер застосування технології пірінгових мереж – це обмін файлами. Виглядає це так: користувачі мережі викладають які-небудь файли в теку, файли із якої доступні для скачування іншим клієнтам. Архітектура BitTorrent передбачає наявність у файлу, що викладається в мережу, єдиного власника, який і зацікавлений в його розповсюдженні. Інший користувач мережі посилає запит на пошук певного файлу. Програма шукає у клієнтів мережі файли, відповідні до запиту, і показує результат. Після цього користувач може викачати файли із знайдених джерел. Сучасні файлообмінні мережі дозволяють викачувати один файл відразу з декількох джерел (так швидше і надійніше). Щоб переконатися, що цей файл у всіх джерелах однаковий, проводиться порівняння не тільки за назвою файлу, але і за контрольними сумами або хешами типу MD4, TTH, SHA-1. Під час скачування файлу користувачем (і після його закінчення) цей файл у даного користувача можуть викачувати і інші клієнти мережі, внаслідок чого особливо популярні файли можуть у результаті бути доступними для скачування з сотень джерел одночасно.

Зазвичай у таких мережах обмінюються фільмами і музикою, що є одвічним головним болем відеовидавничих і звукозаписних компаній, яким таке положення справ дуже не до душі. Проблем їм додає той факт, що припинити розповсюдження файлу в децентралізованій пірінговій мережі технічно майже неможливо – для цього потрібно буде фізично відключити від мережі всі машини, на яких знаходиться цей файл, а таких машин може бути дуже і дуже багато – залежно від популярності файлу їх кількість може досягати сотень тисяч. Останнім часом відеовидавці і звукозаписні компанії почали подавати до суду на окремих користувачів таких мереж, звинувачуючи їх в незаконному розповсюдженні музики і відео.

С самого початку творець BitTorrent програміст Брем Коен (Bram Cohen) заклав в нього декілька принципових відмінностей від інших пірінгових мереж: націленість на розповсюдження великих за розміром файлів і не зовсім децентралізована структура мережі. Первинний власник файлу генерує серію хеш-кодів, згодом використовувану клієнтами BitTorrent для перевірки його цілісності. Клієнт пірінгової мережі, щоб отримати файл, повинен завантажити набір даних з розширенням .torrent. У ньому міститься інформація про ім’я файлу, його розмір, хеш-коди сегментів (за замовчуванням розміром 256 КВ) і адресу розповсюджувача, у якого, у свою чергу, повинен бути запущений tracker-сервер для відстежування кількості завантажень файлу в мережі peer-to-peer. Архітектура BitTorrent припускає пірінговий обмін з використанням центрального tracker-сервера для обліку статистики. У міру того як файл частинами надходить з комп’ютера первинного власника в мережу, користувачі починають завантажувати його фрагменти один у одного. В той же час протокол BitTorrent вимагає фіксації кожного такого завантаження на tracker-сервері, навіть якщо сервер розповсюджувача не бере участь у транзакції.

Файли передаються частинами, кожен torrent, отримуючи ці частини, в той же час віддає (закачує) їх іншим клієнтам, що знижує навантаження і залежність від кожного клієнта-джерела і забезпечує надлишковість даних.

Протокол був створений на мові Python 4 квітня 2001 року. Запуск першої версії відбувся 2 липня 2001 року.

Існує множина програм-клієнтів для обміну файлами за протоколом BitTorrent.

Роздача може містити як один файл, так і декілька, наприклад, вміст теки.

Для кожної роздачі створюється файл метаданих з розширенням .torrent, який містить наступну інформацію:

- URL трекера;
- загальну інформацію про файли (ім'я, довжину і ін.) в даній роздачі;
- контрольні суми (точніше хеш-суми SHA1) сегментів файлів, які роздаються;
- Passkey користувача, якщо він зареєстрований на даному трекері. Довжина ключа встановлюється трекером.
- (Необов'язково) хеш-суми файлів цілком;
- (необов'язково) альтернативні джерела, що працюють не за протоколом BitTorrent. Найбільш поширена підтримка так званих web-сидів (протокол HTTP), але допустимими також є magnet URI.

Трекер (англ. tracker – система відстежування). Працює за протоколом HTTP. Трекер потрібний для того, щоб клієнти могли знайти один одного. Фактично, на трекері зберігаються дані про вхідні порти клієнтів, унікальним чином ідентифікуючи об'єкти, що беруть участь в закачуваннях. За стандартом, імена файлів на трекері не зберігаються, і дізнатися їх за хеш-сумами не можна. Проте на практиці трекер часто окрім своєї основної функції виконує і функцію невеликоговеб-сервера. Такий сервер зберігає файли метаданих і опис поширюваних файлів, надає статистику закачувань за різними файлами, показує поточну кількість підключених користувачів і ін.

Розмір сегменту регулюється при створенні торрента і, як правило, вибирається розмір, відповідний ступеню двійки. При виборі розміру необхідно дотримувати баланс, пов'язаний з механізмом роботи протоколу. Розмір сегменту найчастіше лежить в діапазоні від 128 Кб до 2-4 Мб, хоча на дуже великих роздачах (близько сотні гігабайт) можуть використовуватися сегменти розміром 32-64 Мб.

Якщо роздача складається з декількох файлів, то в процесі хешування вони прочитуються підряд і розглядаються як безперервний потік даних. Тому найчастіше сегмент, що містить кінець одного файлу, також містить і початок наступного. Разом з тим для того, щоб переконатися в правильності викачаного сегменту, необхідно мати його всього цілком. Саме тому, не дивлячись на те, що більшість клієнтів підтримує скачування не всіх файлів в роздачі, а тільки деяких, майже завжди буде викачаний також і початковий і/або кінцева частина файлів, не вибраних для скачування.

Оскільки хеш-кодування в .torrent-файлі включають імена і структуру тек роздачі, то перейменування файлів із збереженням можливості їх роздавати в загальному випадку неможливе. Проте, деякі клієнти підтримують зміну структури, наприклад, створення або перейменування тек і перейменування або переміщення файлів.

Файл метаданих є словником у bencode форматі. Файли метаданих можуть розповсюджуватися через будь-які канали зв'язку: вони (або посилання на них) можуть розміщуватися на домашніх сторінках користувачів мережі, розсилатися, публікуватися в блогах або стрічках новин RSS. Також є можливість отримати info частину публічного файлу метаданих безпосередньо від інших учасників роздачі завдяки розширенню протоколу "Extension for Peers to Send Metadata Files". Це дозволяє обійтися публікацією тільки магнет-посилання. Отримавши яким-небудь чином файл з метаданими, клієнт може починати скачування.

1.2. Програма BitComet

Після установки BitComet відкривається вікно (рис. 1):

Заходимо у верхню вкладку **Файлы**, вибираємо **Создать Торрент** (рис. 2).

Відкривається діалогове вікно створення торрент-файла (рис.3), на зображення нанесені пояснення.

Коли торрент-файл створився, видаляється завдання (рис. 4).

Далі викладаємо створений файл торрент на трекер, оформляємо роздачу.

На різних торрент-трекерах оформлення роздач здійснюється по-різному, як правило, це просто і описано в правилах користування торрента.

Опишемо на прикладі Torrents.ru. Створюємо нову тему з описом файлу, який викладатимемо (як описувати, розказано в правилах Торрента) і прикріплюємо Торрент-файл (рис. 5):

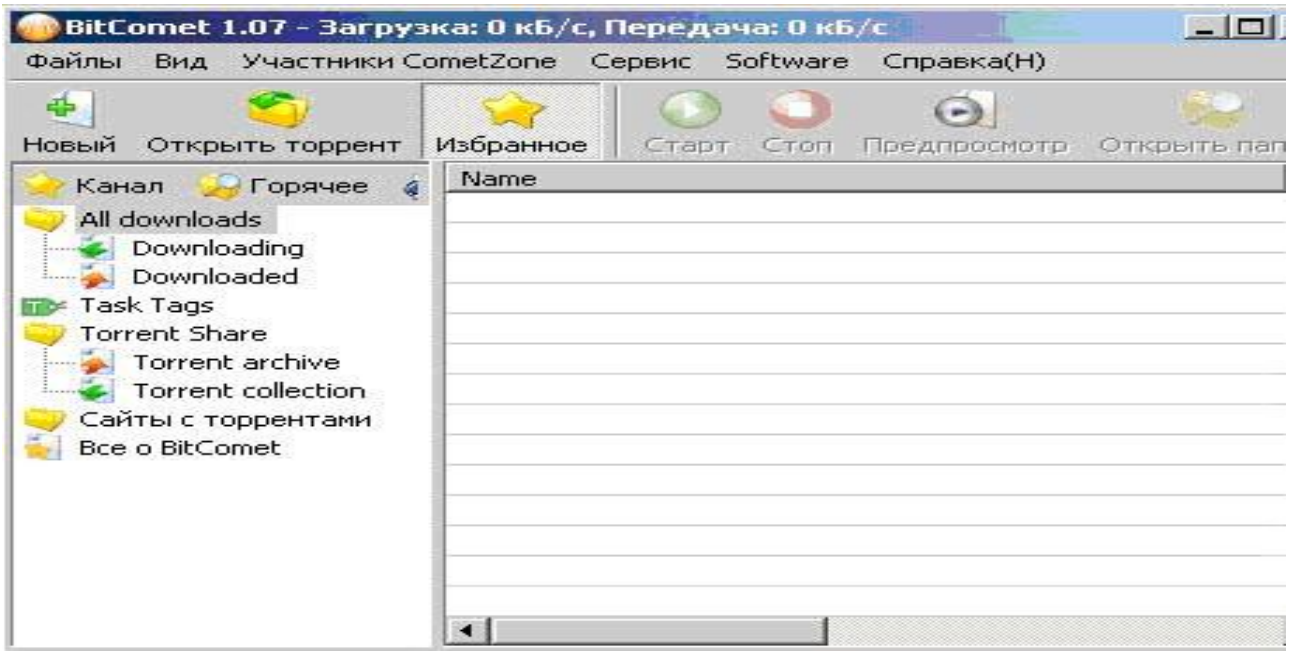


Рис. 1. Вікно BitComet

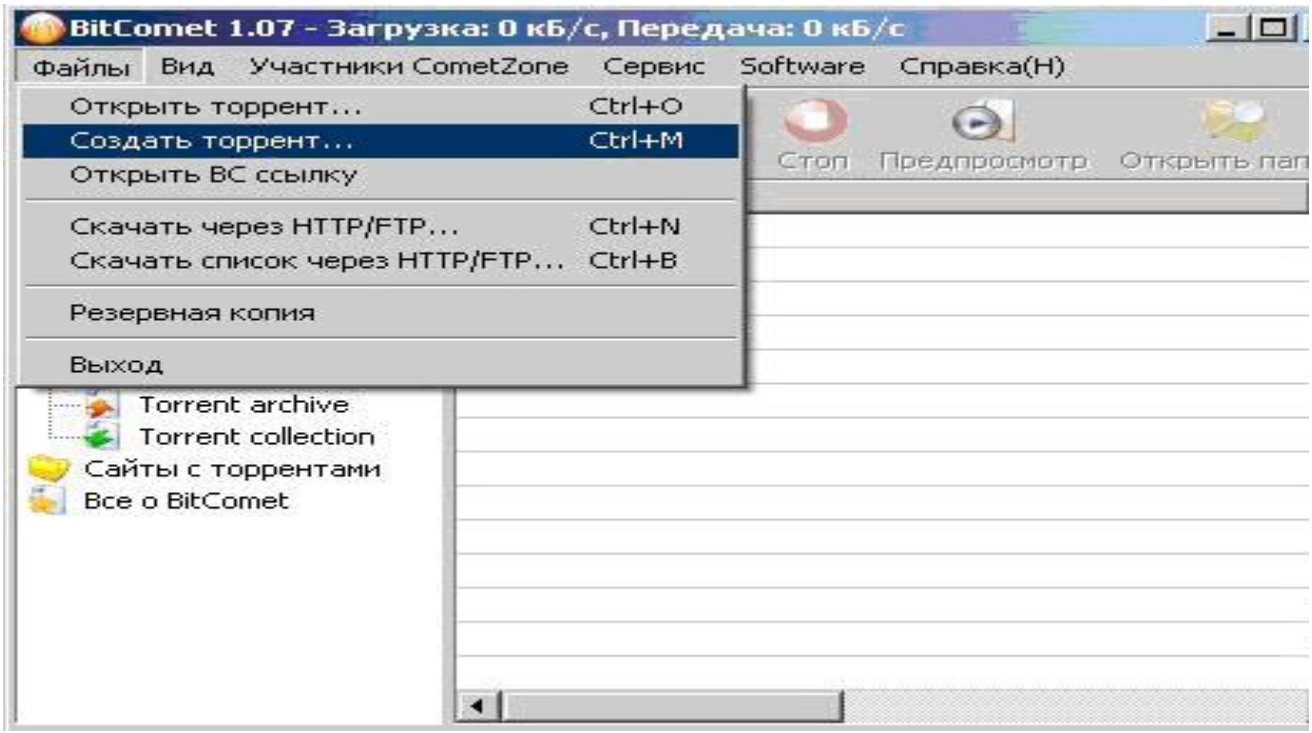


Рис. 2. Вікно команди створення Торрент

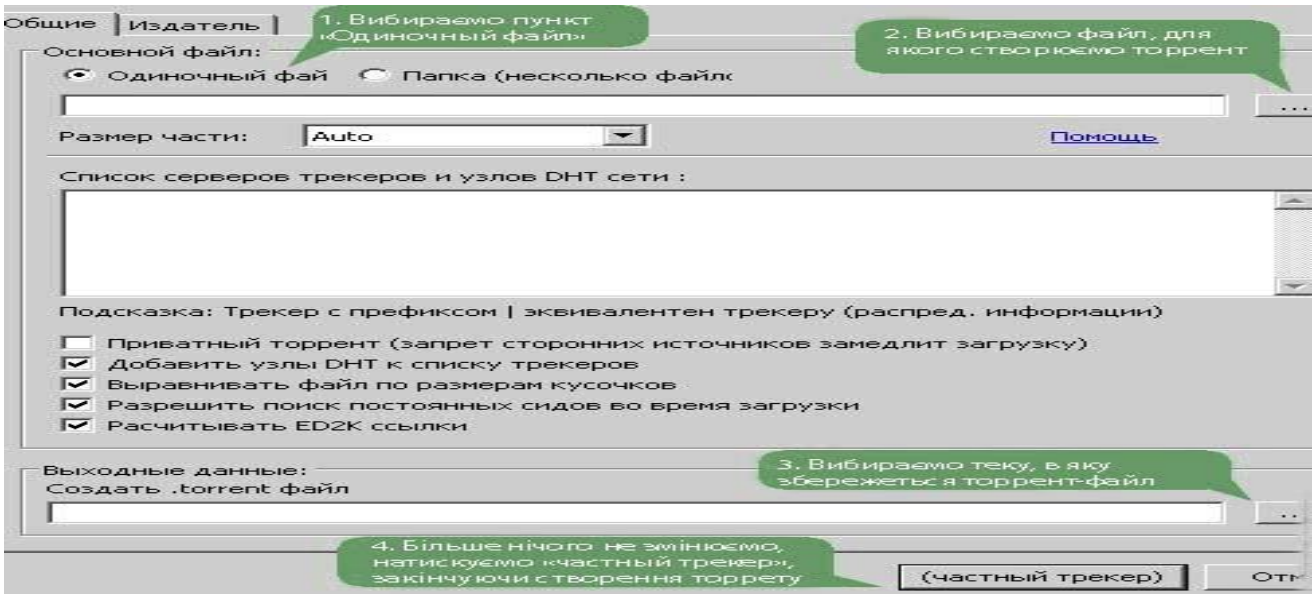


Рис. 3. Вікно створення торренту

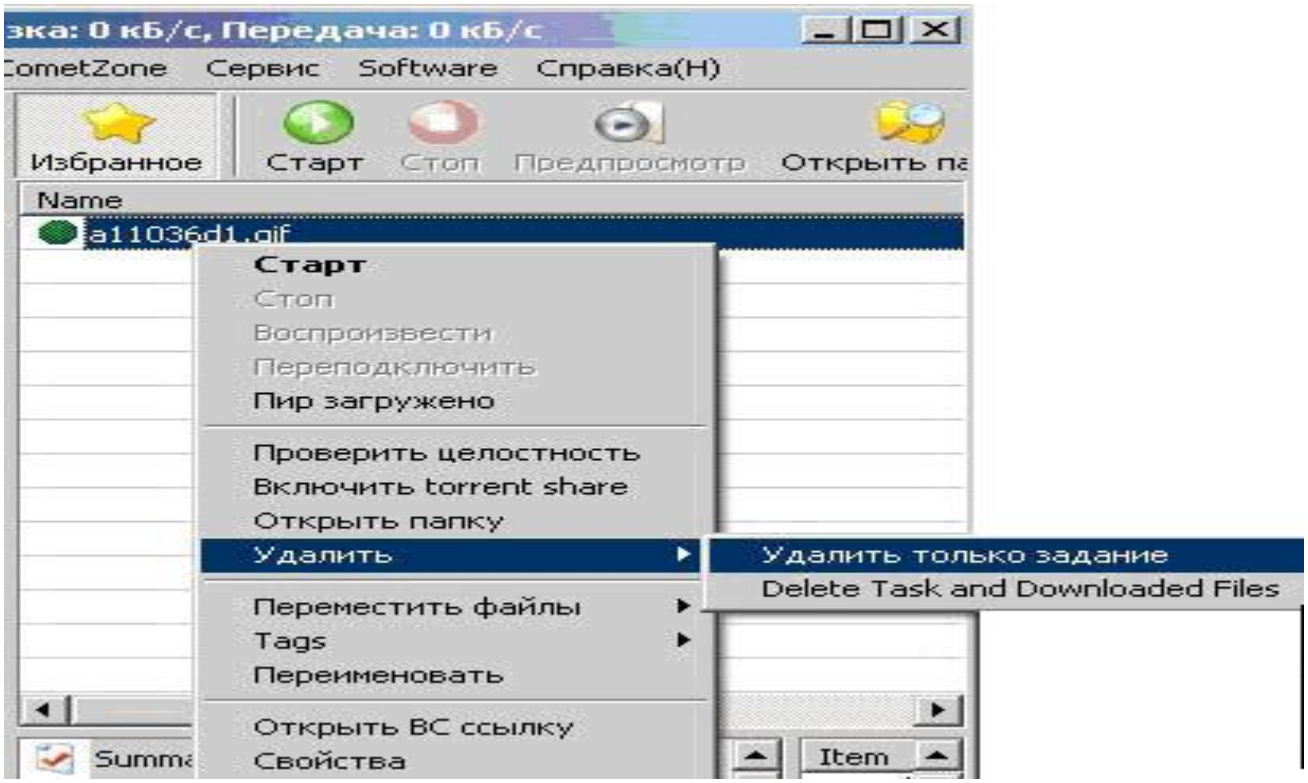
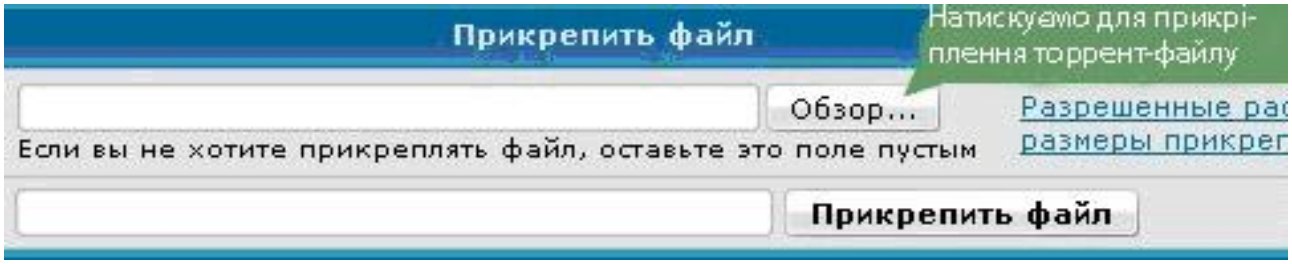


Рис. 4. Видалення завдання



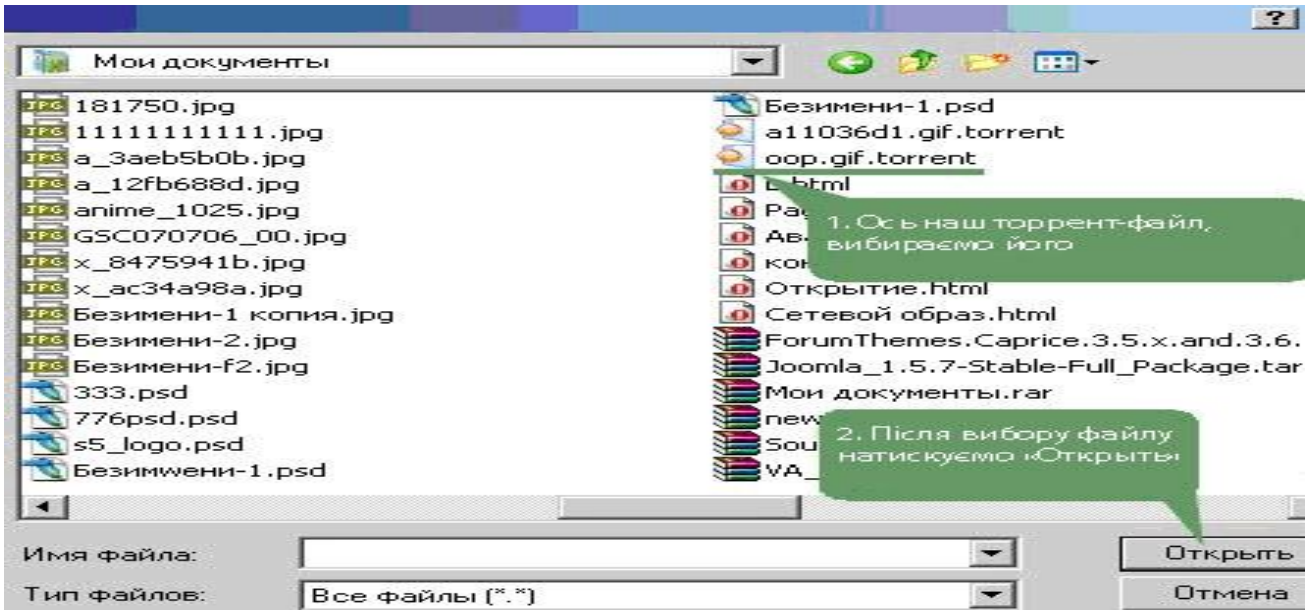


Рис. 5. Створення нової теми

Тепер викладений торрент-файл слід поставити на закачування в ту теку, де знаходиться оригінальний файл (рис. 6).

Далі програма і трекер перевірять наявність файлу.

1.3. Програма µTorrent

Викачуємо останню версію µTorrent на офіційному сайті. Там же, в розділі «Download», викачуємо файл «Language Pack» – це доповнення програми для підтримки російськомовного інтерфейсу. Файл русифікації «utorrent.lng» близько 400 кб, зберігаємо його в теку з програмою, там, де знаходиться файл запуску програми – utorrent.exe.

Після встановлення відкривається стартове вікно програми (рис. 7):

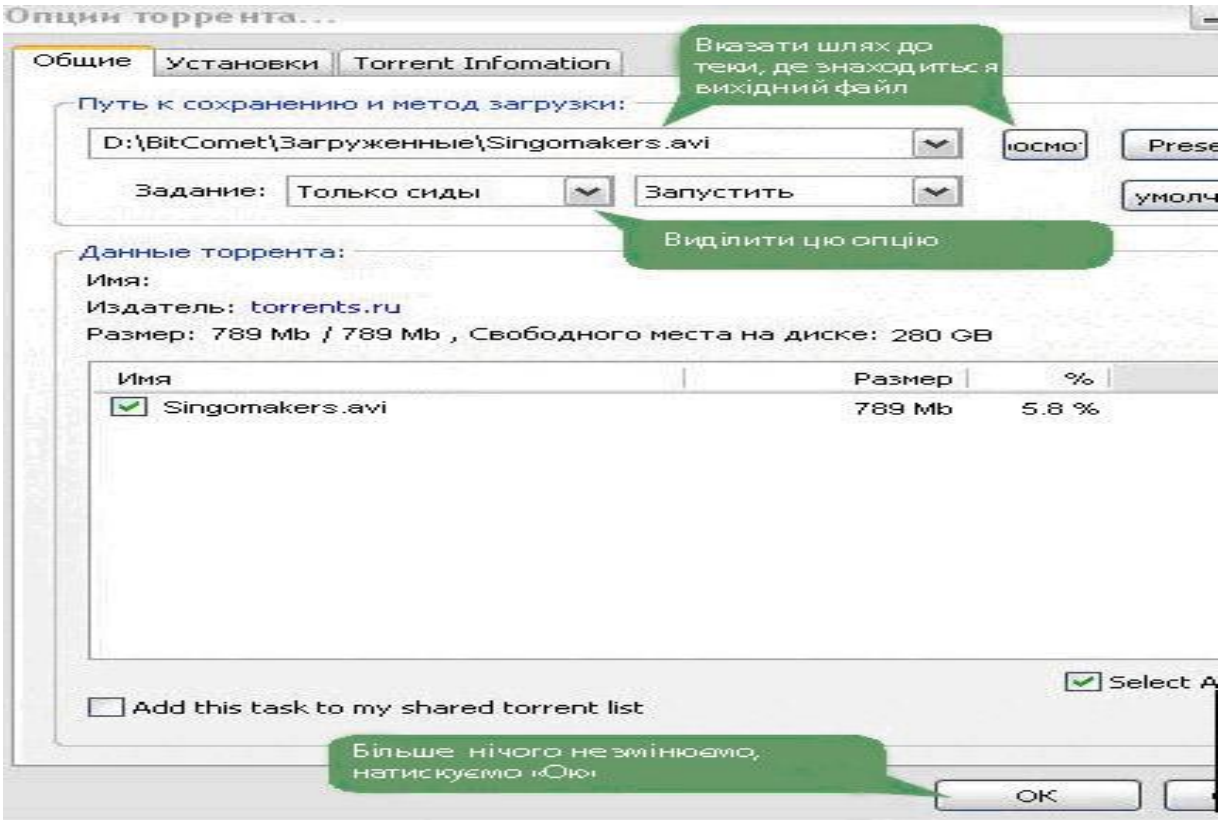


Рис. 6. Постановка файлу на закачування

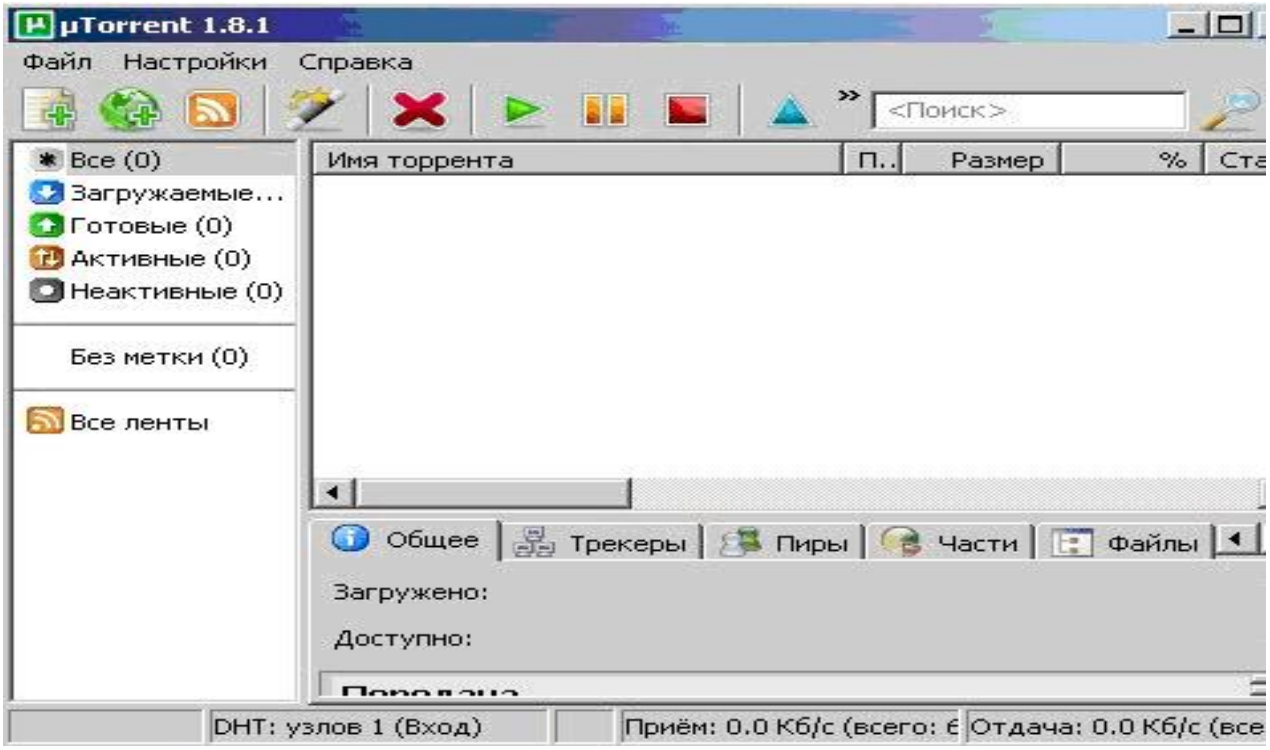


Рис. 7. Стартове вікно програми

Отже, створюємо торрент-файл, для цього входимо у верхнє меню **Файл** у вкладку **Создать новый торрент** (рис. 8).

Відкрилося вікно створення торрент-файлу. Вибираємо файл або групу файлів для створення торрент-файлу. Натискаємо **Создать и сохранить** (рис. 9).

Необхідно підтвердити, що є бажання продовжити створення торрент-файлу без вказівки трекера. Все, торрент-файл збережений у Вас на комп'ютері. Далі викладаєте його на будь-якому трекері і користувачі зможуть викачувати Ваш файл(и).

Якщо Ви хочете викачати що-небудь з трекера, то просто викачайте відповідний торрент-файл, автоматично відкриється діалогове вікно µTorrent, там слід вказати деякі параметри закачування (рис. 10):

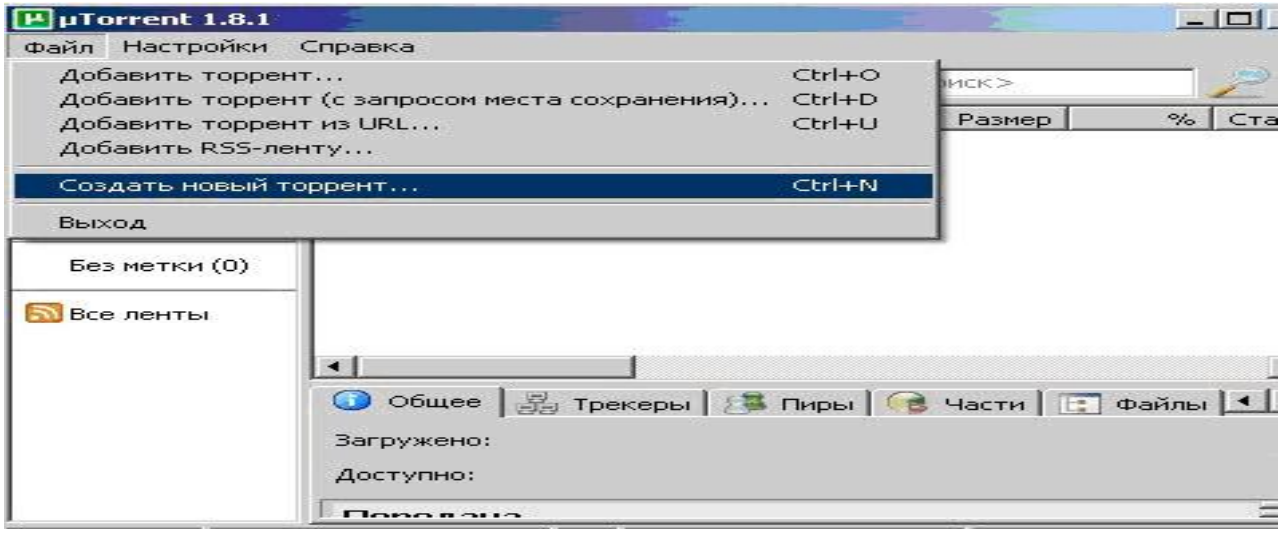


Рис. 8. Вікно команди створення торрент-файлу

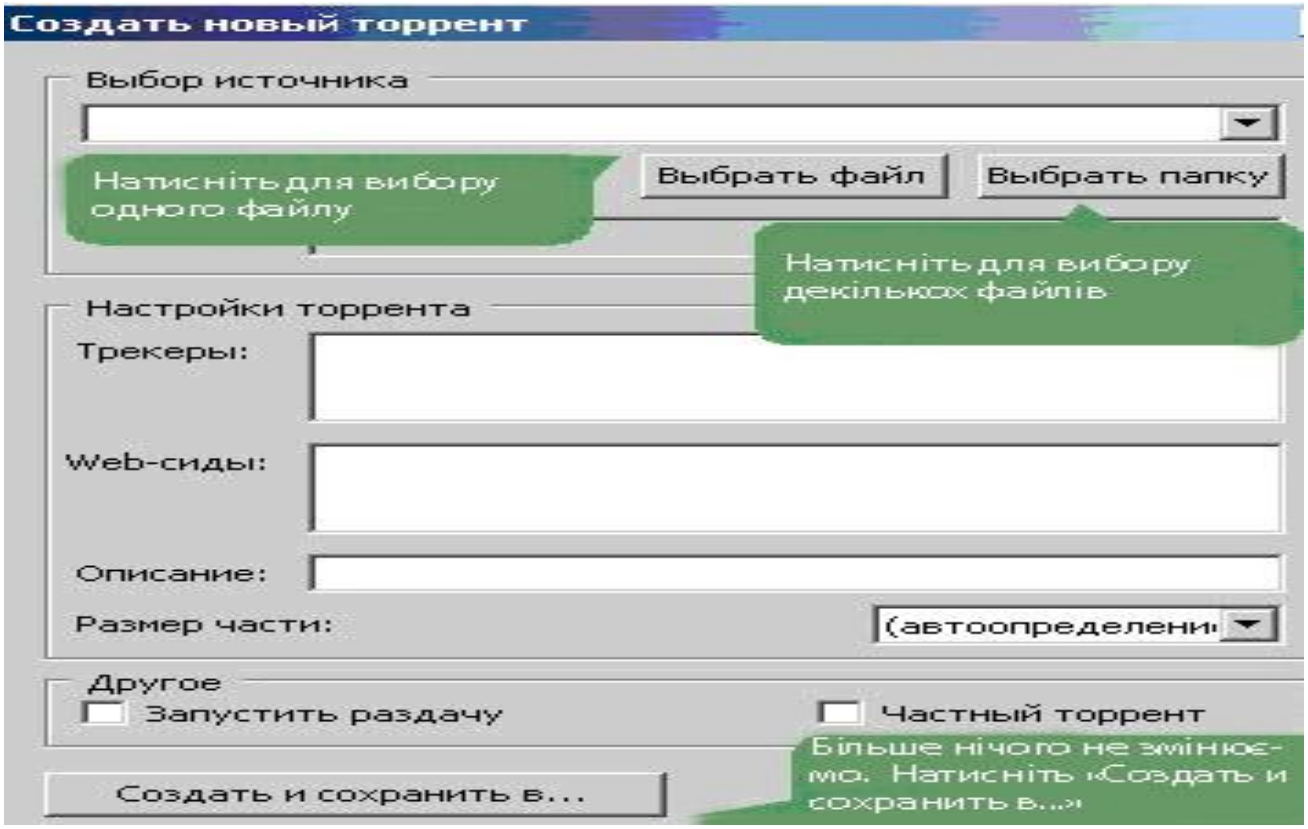


Рис. 9. Вікно створення торрент-файлу

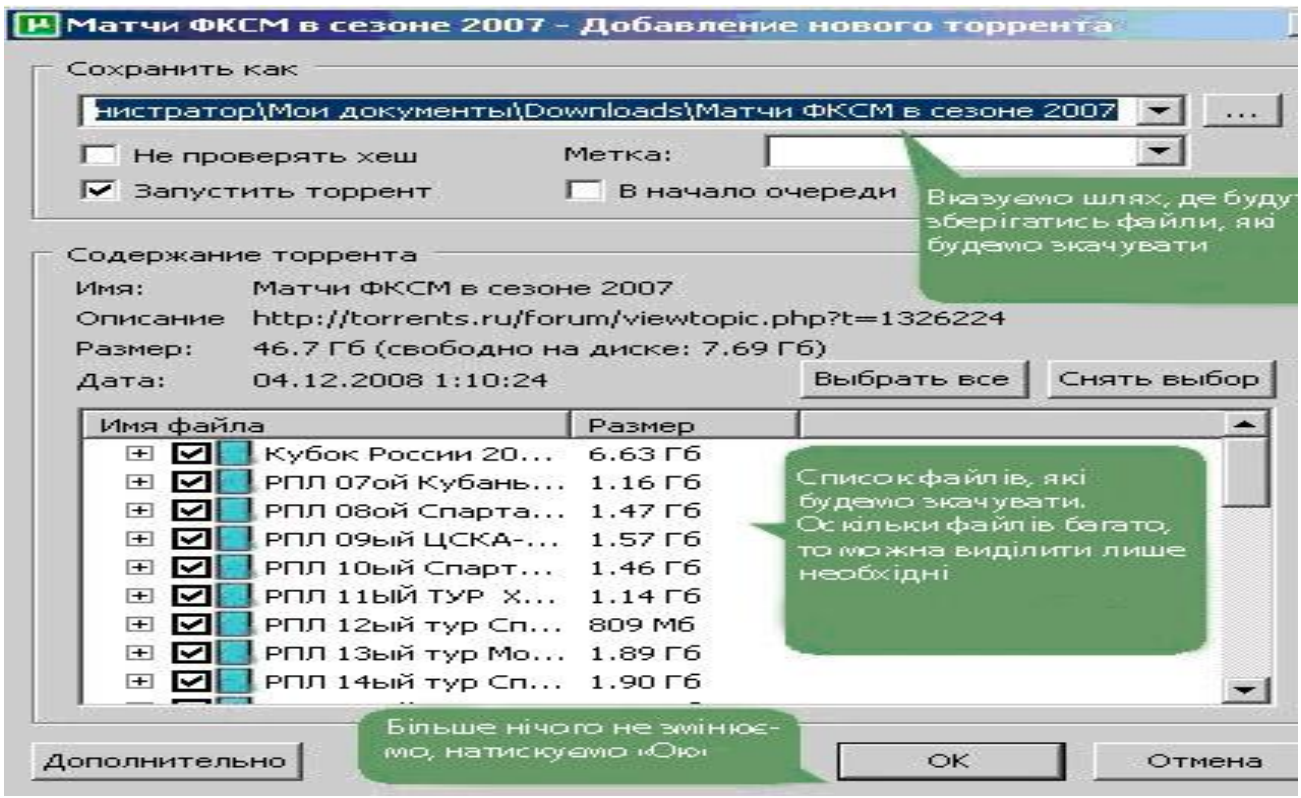


Рис. 10. Відбір параметрів закачування файлів

Після підтвердження параметрів, які відібрання, програма тут же почне викачувати необхідний файл (рис.11).

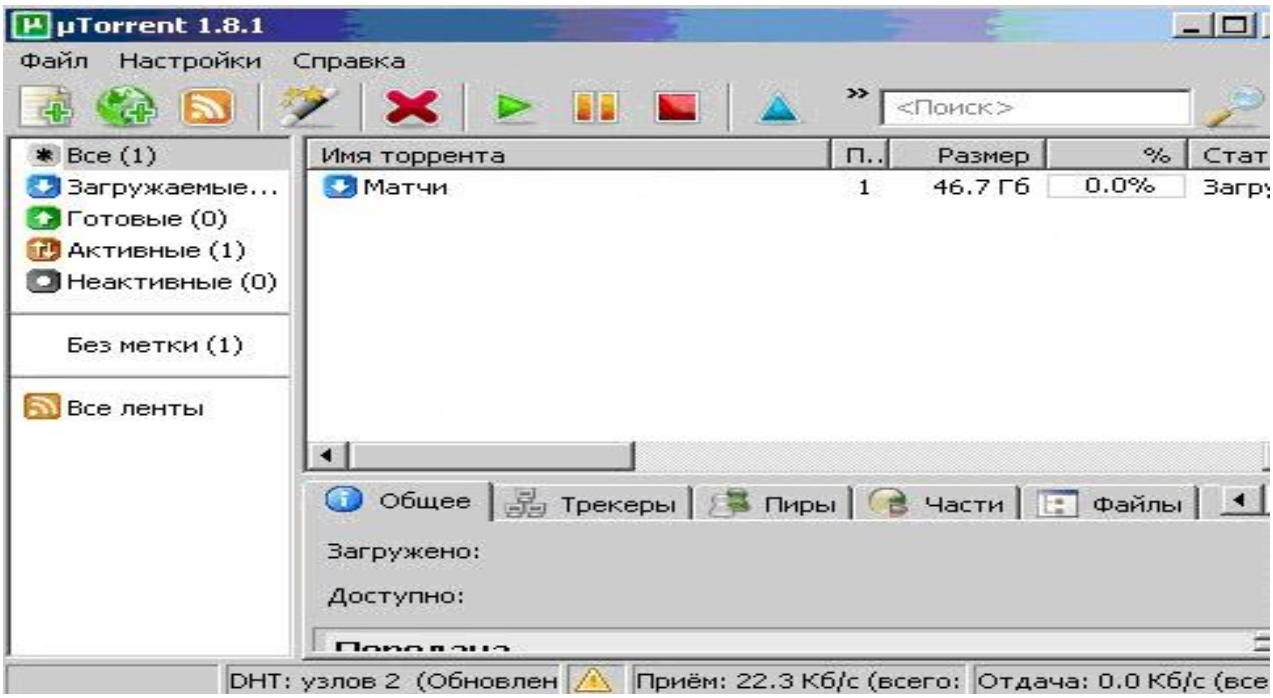


Рис. 11. Вікно закачування файлу

2. Хід роботи

1. Встановіть програму BitComet та µTorrent на своєму комп'ютері.
2. Створіть Торрент використавши файли свого каталогу на сервері.
3. Викладіть файл торрент на трекер.
4. Встановіть файл торрент на закачування.
5. Проведіть закачування файлів з мережі за допомогою кожної програми та покажіть викладачеві.

3. Контрольні питання

1. Для чого використовуються пірінгові мережі?
2. Які особливості протоколу протоколом BitTorrent?
3. Яка структура файлу метаданих з розширенням .torrent?
4. Для чого призначений трекер?
5. Яке призначення програми BitComet та особливості її роботи?
6. Яке призначення програми µTorrent та особливості її роботи?

ЛАБОРАТОРНА РОБОТА 38. ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

Мета роботи: отримати навички використання хмарних технологій

Зміст

1. Теорія
1.1. Загальні поняття
1.2. Огляд хмарних технологій
2. Хід роботи
2.1. Реєстрація акаунта
2.2. Робота в акаунті
3. Контрольні питання.
Додаток 1
Додаток 2
Додаток 3

1. Теорія

1.1. Загальні поняття

Останні роки все більшої популярності набувають так звані хмарні технології або хмарні обчислення (Cloud computing).

Хмарні технології (*cloud computing*) визначають як динамічно масштабований вільний спосіб доступу до зовнішніх обчислювальних інформаційних ресурсів у вигляді сервісів, що надаються за допомогою мережі Internet. Вперше термін був використаний у даному контексті в 1997 році на лекції Рамнат Челлаппа (*Ramnath Chellappa)*, де він визначив його як нову "обчислювальну парадигму, при якій межі обчислювальних елементів залежатимуть від економічної доцільності, а не тільки від технічних обмежень".

Поява першої технології, що можна охарактеризувати як хмарну, приписується компанії *Salesforce.com*, заснованої в 1999 році. Вона надала доступ до свого додатку через сайт за принципом – програмне забезпечення як сервіс (*Software as a Service [SaaS]*). Наступним кроком стала розробка хмарного Web-сервісу компанією Amazon у 2002 році. Цей сервіс дозволяв зберігати інформацію і робити обчислення. В 2006 Amazon запропонувала сервіс під назвою *Elastic Compute cloud* (*EC2*) як Web-сервіс, що надав можливість його користувачам запускати свої власні програми. У цьому ж році компанія Google почала впроваджувати *SaaS* сервіси під назвою «*Google Apps*» та платформи як сервіси (*Platform as a Service [PaaS]*) під назвою «*Google App Engine*». Компанія Microsoft зробила свою першу презентацію *PaaS* під назвою «*Azure Services Platform*» на Конференції з професійного розвитку 2008 року *(Professional Developer's Conferens [PDC]),* що стала суттєвим поштовхом до розвитку хмарних технологій.

Хмарні технології – це парадигма, що передбачає віддалене опрацювання та зберігання даних.

Хмара – це деякий ЦОД (дата-центр, сервер) або їх мережа, де зберігаються дані та програми, що з'єднуються з користувачами через Інтернет.

Використання хмарних технологій дозволяє споживачам використовувати програми без установки і доступу до особистих файлів з будь-якого комп'ютера, що має доступ до мережі Інтернет. За допомогою цих технологій можна вести значно ефективніше управління підприємством за рахунок централізації управлінських та облікових відомостей, опрацювання, пропускної здатності та надійності зберігання даних.

Простим прикладом хмарних технологій є сервіси електронної пошти, наприклад, Gmail, Meta і т.д. Потрібно всього лише підключення до Інтернет, і можна відправити пошту, при цьому додаткового програмного забезпечення або сервера не потрібно.

Хмарні технології – це технологія, яка надає користувачам Internet доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервіса, тобто якщо, є підключення до Internet то можна виконувати складні обчислення,

опрацьовувати дані використовуючи потужності віддаленого сервера. Спрощену схему хмарних технологій представлено на рис. 1 та найбільш відомі сервіси на рис. 2.
Послуги які можливо отримати при використанні хмарних технологій:

1. Використання програмного забезпечення

2. Платформа як сервіс (Software as a Service (SaaS)) – дає доступ до інтегрованої платформи для розробки, тестування та підтримки різноманітних проектів

3. Інфраструктура як послуга (Infrastructure as a Service (IaaS)) – представлення комп'ютерної інфраструктури у вигляді віртуалізації, що включає в себе операційні системи та системне програмне забезпечення, а також апаратну частину сервера.

4. Віртуальне робоче місце (Desktop as a Service (DaaS)) – користувач має змогу власноруч налаштовувати своє робоче місце і тим самим створити собі комплекс програмного забезпечення необхідного йому для роботи.

Загалом, ця технологія має як плюси так і мінуси. Вона доволі економічна і доцільна для організацій, корпорацій, фірм і т.і. Вона не потребує значних ресурсів вашого пристрою (будь-то, КПК, планшет, смартфон, нетбук або комп'ютер), але вона вимоглива щодо доступу до Internet.

Це означає, що ви повинні мати безперебійний швидкісний Internet.

Другим мінусом є те, що хоча надавачі послуг і стараються працювати онлайн, але завжди бувають випадки, коли сервер може бути оффлайн і тоді доступ до ваших послуг буде недоступний.

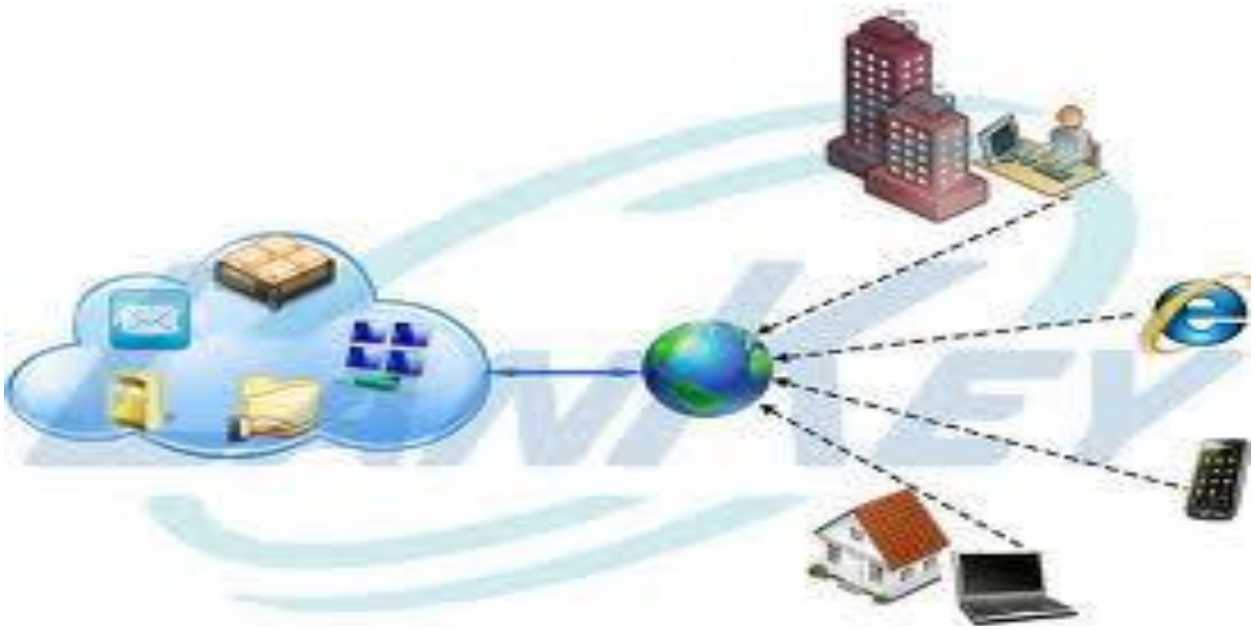


Рис. 1. Схема хмарних технологій

Рис. 2. Найбільш відомі сервіси хмарних технологій

1.2. Огляд хмарних технологій

Як показує практика, відповідно до потреб сучасних умов праці зручнішим за локальне редагування документу є розміщення необхідного файлу в хмарне сховище, доступ до котрого може бути розмежований для ролей конкретних користувачів. Одні користувачі можуть змінювати файл, інші – тільки читати та рецензувати зміни. Загалом використання таких хмарних сервісів є простим у користуванні та не потребує особливих налаштувань. Актуальним залишається лише питання: На ринку так багато пропозицій, котру ж з хмар варто обрати?

Один з порівняно молодих гравців ринку хмарних сховищ онлайн і редакторів документів – компанія Adobe зовсім недавно анонсувала повноцінне рішення для створення PDF-файлів та спільної роботи з ними. Раніше такий інструмент існував, але в обмеженій версії під назвою Buzzword. Зараз він інтегрований в комплексний продукт, що просувається як єдине рішення за передплатою (для роботи потрібно реєстрація Adobe ID). В даний час Web-версія Adobe Acrobat нагадує свій десктопний варіант, в ній є інструменти для редагування та форматування (раніше можна було тільки налаштовувати шрифти). Додаток дозволяє експортувати створені документи у формати PDF, DOC, ODT і RTF, а також EPUB. Крім Web-редактора у складі сервісу Acrobat.com надається файлообмінний сервіс Adobe SendNow, в який можна завантажувати файли в будь-якому форматі різного розміру (безкоштовно – до 100 Мб, платно – до 2 Гб), після чого організовувати до них спільний доступ для колег по роботі (через систему запрошень поштою), вести облік розісланих запрошень (через повідомлення про отримання), шукати серед завантажених файлів за назвою і описом. Частина можливостей доступна тільки в платній версії. Третій сервіс, пропонований Adobe – Adobe CreatePDF – онлайн-конвертер файлів. Він складається з трьох компонентів: перетворювача будь-якого текстового документа в PDF, інструменту для об’єднання декількох файлів (текстових, графічних і так далі) в єдиний PDF-документ і віртуального принтера, що дозволяє друкувати прямо в PDF-файл, що розміщується на цьому Web–сервісі.

Прикладами використання хмарних технологій можуть бути Google Apps для навчальних закладів та Office 365 для навчальних закладів.

Google Apps для навчальних закладів. Сервіс Google Apps для навчальних закладів об’єднує окремі служби, за допомогою яких співробітникам одного навчального закладу можна ефективніше спілкуватися та співпрацювати з співробітниками свого або іншого

навчального закладу. Ці служби є простими в налаштуванні, не потребують додаткового обслуговування і ними можна користуватися безкоштовно. Адміністратори веб-сайтів (веб-порталів) можуть за власним вибором поєднувати окремі служби для розміщення даних на сайті, а також для спілкування та співпраці.

Office 365 для навчальних закладів. За допомогою Office 365 для навчальних закладів можна надати для викладачів, інших співробітників та студентів можливість безкоштовно працювати з електронною поштою, створювати веб-сайти, редагувати та зберігати документи в глобальній мережі Інтернет, обмінюватися миттєвими повідомленнями та проводити веб-конференції (рис. 3). Як і в сервісі Google Apps для навчальних закладів в Office 365 для навчальних закладів є аналогічна служба для роботи з різними документами – це служба OneDrive (SkyDrive). У службі OneDrive кожному користувачу надається певний обсяг вільного місця для зберігання даних в «хмарі», які синхронізуються з даними на персональному комп'ютері користувача. Використовуючи службу OneDrive можна надавати спільний доступ до документів для інших користувачів.

Сервіси Google Docs & SpreadSheets від Google з'явився на ринку в результаті злиття двох розробок – табличного процесора від Google і текстового редактора Writely від Upstartle в бета-версії 2006 році. Пізніше до сервісу додалися можливість переглядати презентації та файлове сховище, які перейшли в статус релізу в 2009 році. Сервіс інтегрований з поштовим клієнтом Gmail і являє собою універсальний редактор для файлів MS Office / OpenOffice.

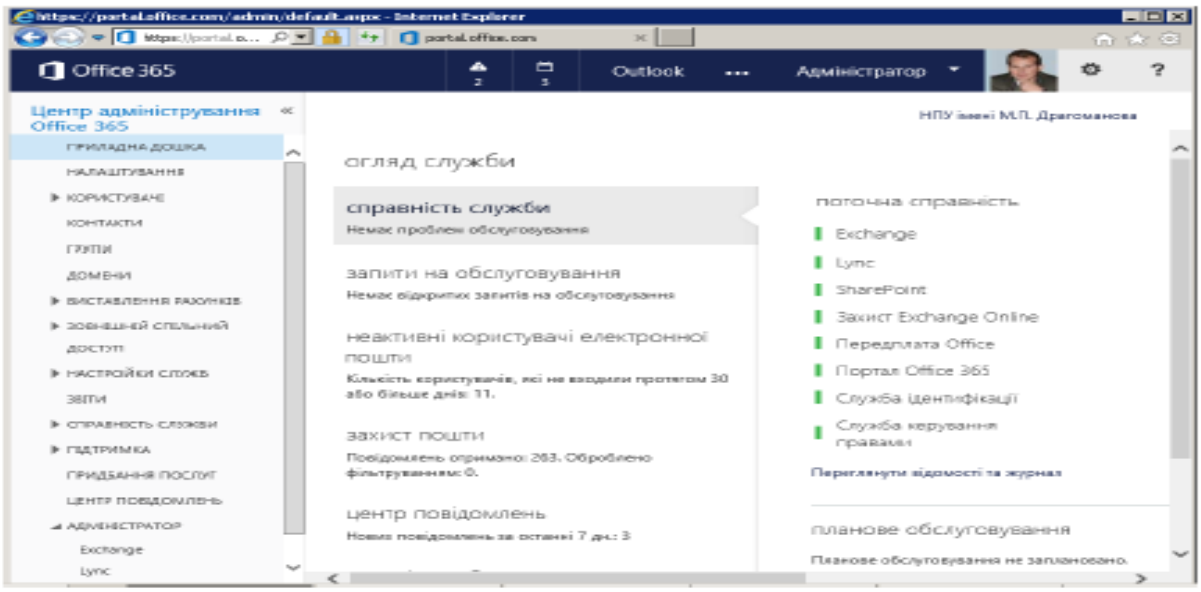


Рис. 3. Office 365 для навчальних закладів

PDF. Інтерфейсом сервіс Google схожий на Open Office.org. Документи можуть редагуватися спільно користувачами, які отримали запрошення (мати обліковий запис в Google для цього необов'язково), в ході процесу рецензування та редагування доступний перегляд змін і чат.

Файловий обмінник працює безкоштовно з квотою 1 Гб, додатковий обсяг можна отримати за гроші. Google Docs & SpreadSheets підтримує "хмарний" друк документів (віддалену відправку файлів в чергу принтера), а також надає базові можливості для організації зберігається в сервісі контенту.

Слід відмітити такі функціональні можливості основних продуктів компанії Google

- створення Web-сайтів – *Google Sites*;
- ведення календаря, робочого графіку, складання навчальних планів, тощо – *Google Calendar*;
- створення документів різних форматів – *Google Docs*;

- сумісне редагування документів різних форматів – *Google Cloud Connect*;
- електронна пошта з пошуковою системою та захистом від спаму – *Google mail (Gmail)*;
- створення 3D-моделей – *SketchUp*;
- ведення щоденників навчальних проектів – *Blogger*;
- створення фотоальбомів, редагування фотографії, сумісна робота з іншими програмами редагування графічних файлів – *Picasa*;
- моніторинг трафіку на Web-сайт і ефективність різних маркетингових заходів – *Google Analytics*;
- автоматичне перекладання Web-сторінок із різних мов – Google translate.

В табл. 1 наведена класифікація деяких хмарних технологій.

Таблиця 1

Класифікація деяких хмарних технологій відповідно до їх використання

Продукти компаній			Функції
IBM	Microsoft	Google	
WebSphere	SharePoint Online	Google Docs	Перенесення до мережі Internet додатків, що виконуються на ПК
WebSphere, FileNet Content Services	SharePoint Online	Google Docs	Доступ до прикладних пакетів, що розраховані на високі обчислення
WebSphere, FileNet Content Services	SharePoint Online, Lync Online (Lync Client)	Google Cloud Connect, Google Drawings	Сумісний одночасний доступ декількох осіб до редагування документів різних форматів
WebSphere, InfoSphere Warehouse, LotusLive Connections	Lync Online, Exchange Online	Google Wave, Google Groups, Gmail	Комунікація
WebSphere, InfoSphere Warehouse, LotusLive Connections	SharePoint Online, Lync Online (Lync Client), Exchange Online	Google Wave, Google Groups, Gmail, Google Sites, Blogger	Підтримка механізмів обміну повідомлень між користувачами
Cognos Connection	Systems Management Server, Hyper-V (кодове ім’я Viridian)	Google Code	Підтримка системи контролю версій, інструменти управління проектами та спостереження за помилками
InfoSphere Warehouse	Systems Management Server, Hyper-V	SketchUp	Інтерактивні інструменти моделювання

WebSphere, InfoSphere Warehouse	SQL Server, Lync Online, Exchange Online	Google Wave, Google Groups, Gmail, Google Sites, Blogger	Соціальні мережі для користувачів
WebSphere, InfoSphere Warehouse	SQL Azure, SQL Server	Google Wave, Google Groups	Створення та розгортання на базі обчислювальної інфраструктури сервісів різних рівнів
Tivoli Netcool/OMNIbus, Tivoli Live Monitoring Services	System Center Server Management Suites, System Center Client Management Suite System Center Essentials Plus 2010 Suites	Google Analytics	Моніторинг трафіку на Web-сайт і ефективність різних маркетингових заходів

З представлених на ринку хмарних сервісів для зберігання та редагування документів найбільш зручними і оптимальними за співвідношенням “ціна/якість” для виконання завдання з розміщення документа в мережі для надання до нього вибіркового доступу одному або декільком особам виглядають сервіси від Adobe і Google. З плюсів першого можна відзначити зручний інтерфейс користувача і розумну цінову політику, а з мінусів – відсутність підтримки кирилиці в редакторі документів. Google же відрізняється де-факто безкоштовністю сервісу і підтримкою безлічі мов, у тому числі і української, але слабким опрацюванням в області сумісності форматів (у таблиці 2 подано деякі характеристики означених вище ресурсів)

Таблиця 2

Деякі характеристики хмарних технологій

Функція-сервіс	Acrobat.com	Google Docs&SpreadSheets	MS Office WebApps/ Docs.com	Zoho Docs
Об'єм сховища	безкоштовно:2Гб, платно: 15-100Гб	безкоштовно:1Гб, платно: 20Гб-1Тб	безкоштовно:25Гб	платно: 1 Гб, 3 долари за кожні додаткові 5Гб за місяць
Термін зберігання	7 днів (необмежене пролонгування)	необмежено	необмежено	необмежено
Довільний формат файлу	так	так	так	ні
Підтримка кирилиці в редакторі	ні	так	так	так
Авторизація для користувачів	Adobe ID	Google Id, персональне запрошення	Windows Live ID, Facebook Id	Google ID, Facebook ID, Yahoo ID, Звичайна реєстрація
Підтримка PDF	так	так	ні	так
Формати документів	PDF, DOC, RTF, ODT, EPUB	DOC, ODT, TXT, RTF, TXT, HTML	DOCX, XLSX, PPTX	DOC, ODF, ODT, SWX, RTF, TXT, HTML, PDF, LaTex
Контроль отримувачів	так	так	так	так
Вимоги	Adobe Flash, Snockwave Flash, JavaScript	Adobe Flash, JavaScript	MC Silverlight, JavaScript	JavaScript
Швидкість роботи інтерфейсу	висока	висока	середня	низька

2. Хід роботи

2.1. Реєстрація акаунта

Завантажте сторінку у браузер: **google.com.ua** (рис. 4). Розкрийте знак **Сервисы**  . Натисніть знак **Диск** 

(рис. 5). Введіть команду **Добавить аккаунт** (рис. 6). Введіть команду **Создать аккаунт** (рис. 7).

Заповніть пропоновані поля (рис. 8) і натисніть **Далее** (користувачу буде запропоновано наступну сторінку). Зайдіть в акаунт (рис. 9).

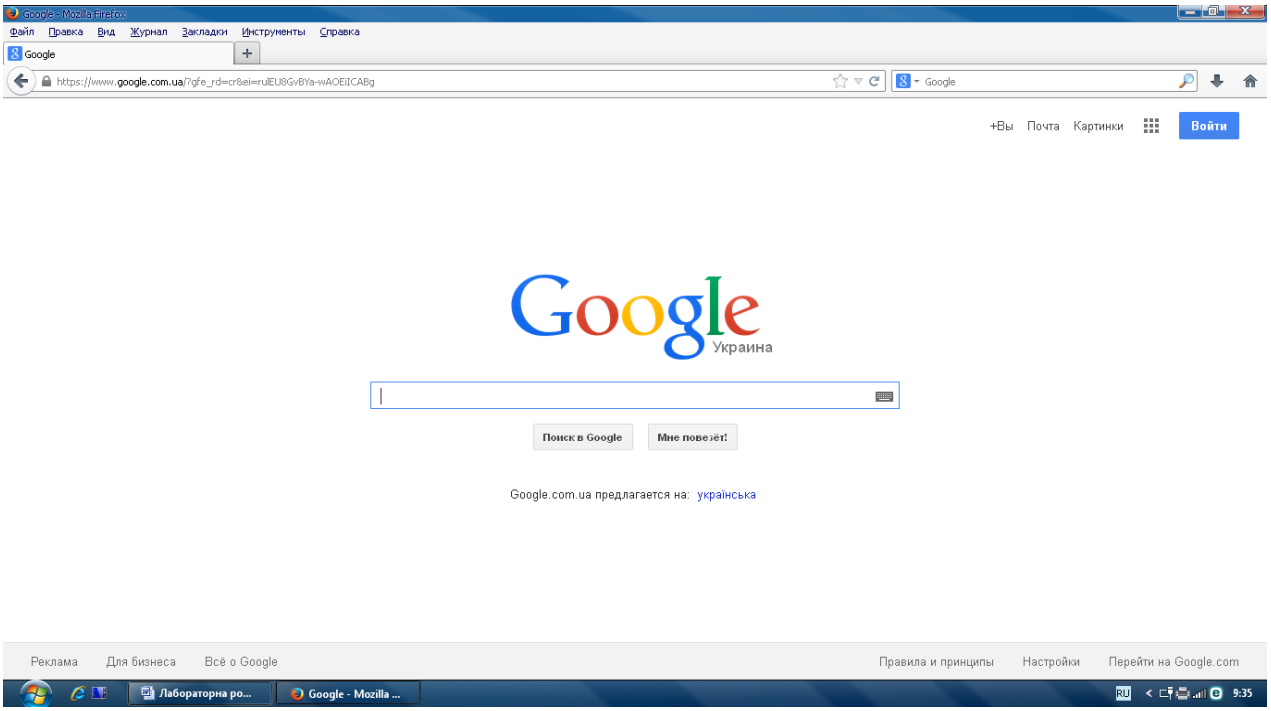


Рис. 4. Сторінка у браузері **google.com.ua**

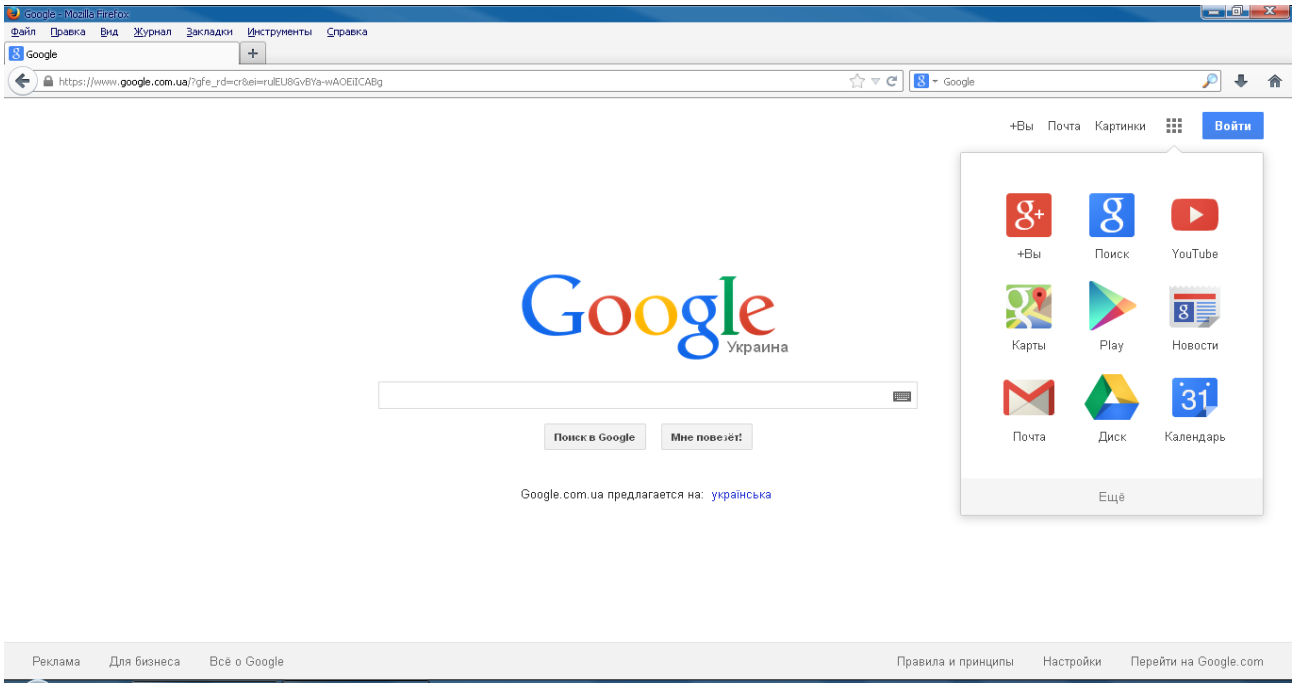


Рис. 5. Відбір параметрів

2.2. Робота в акаунті

За допомогою команди **Создать** (рис. 10) створіть декілька папок, таблицю (дод. 1), документ (дод. 2), презентацію взяти на вибір із додатка 3. Збережіть таблицю, документ, презентацію. Завантажте на хмарний диск два довільні файли з вашого комп'ютера (рис. 11–13).

Надайте до них загальний доступ (за допомогою контекстного меню, рис. 14 – 16).

Завершіть роботу в акаунті (клацніть по напису 

та відберіть команду **Выйти).**

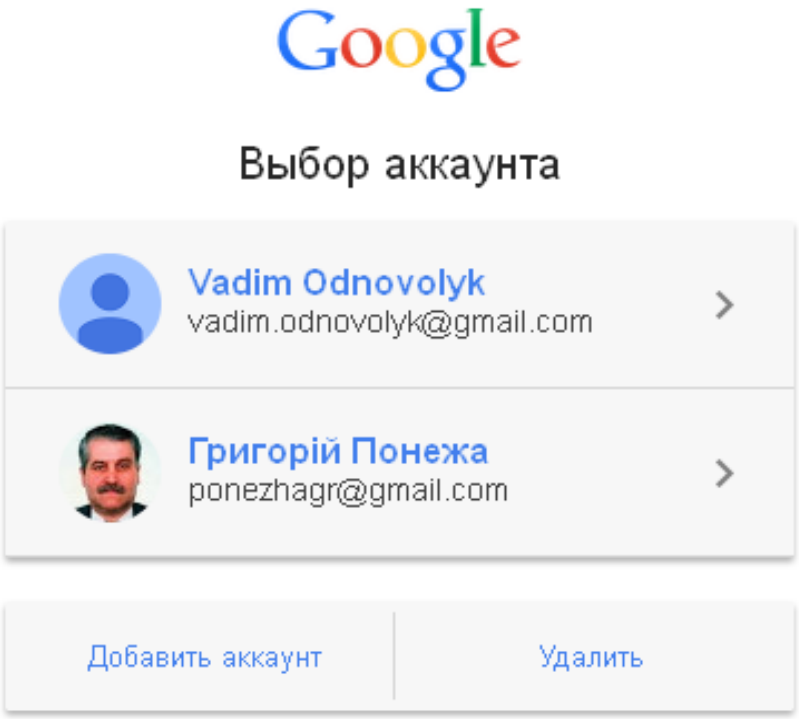


Рис. 6. Введення команди **Добавить аккаунт**

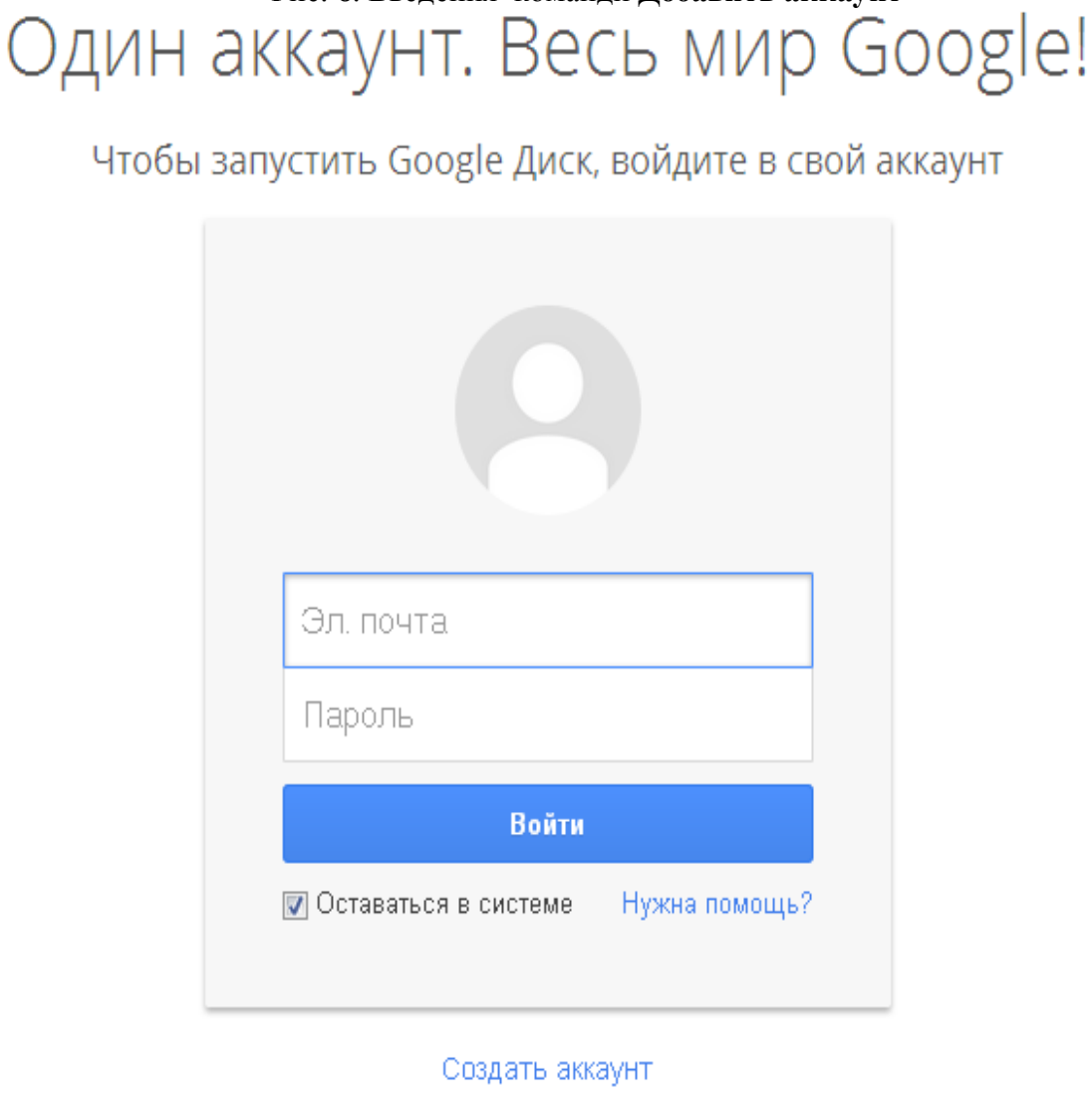


Рис. 7. Введення команди **Создать аккаунт**

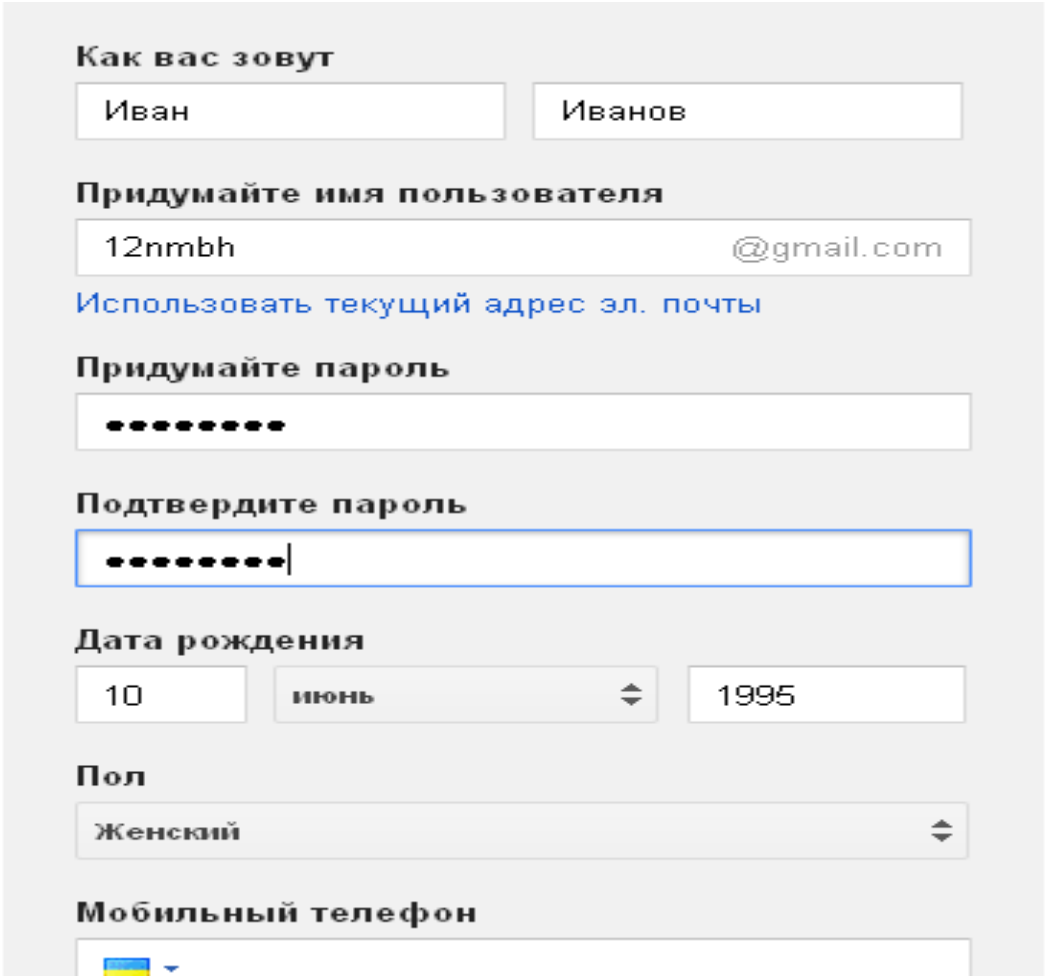


Рис. 8. Заповнення даних для акаунта

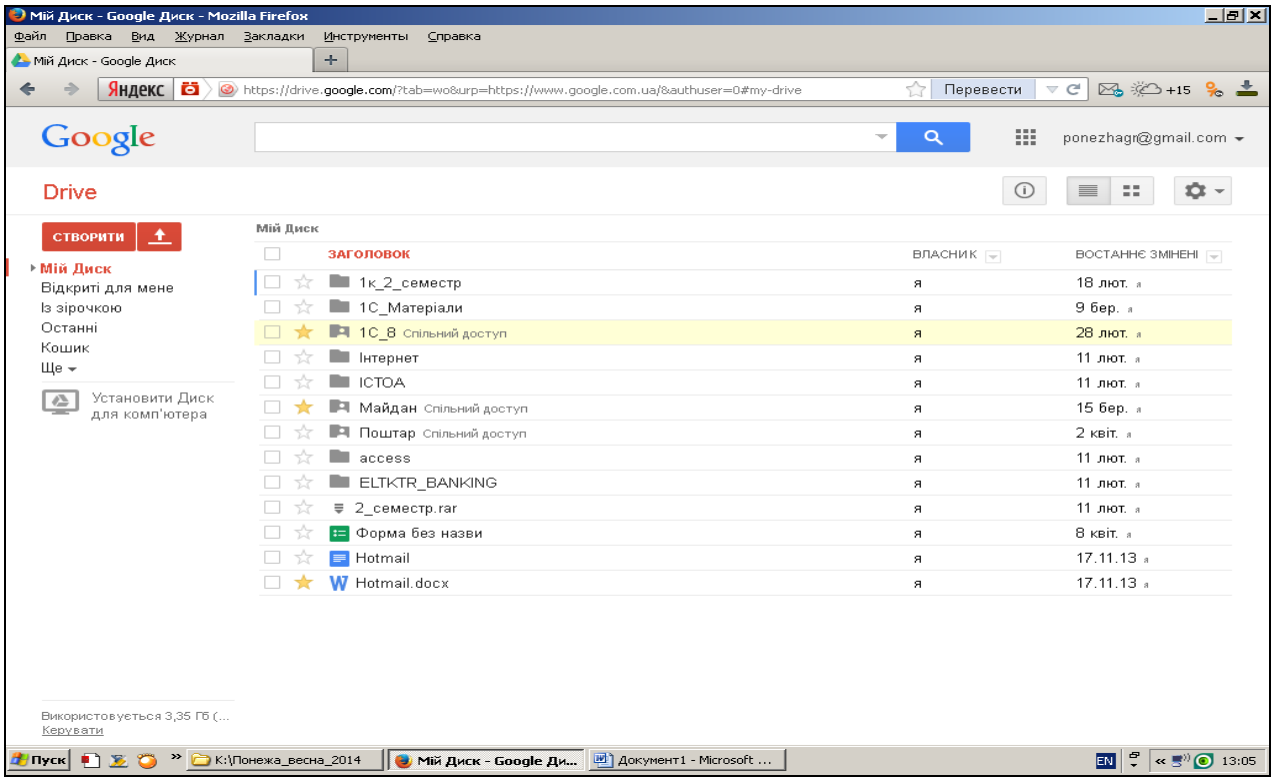


Рис. 9. Акаунт

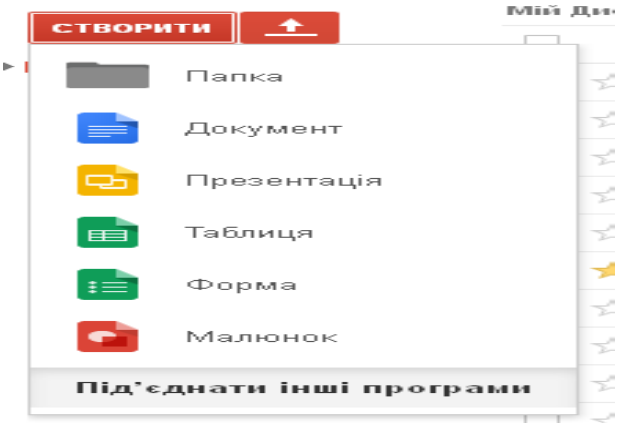


Рис. 10. Можливості команди **Створити**

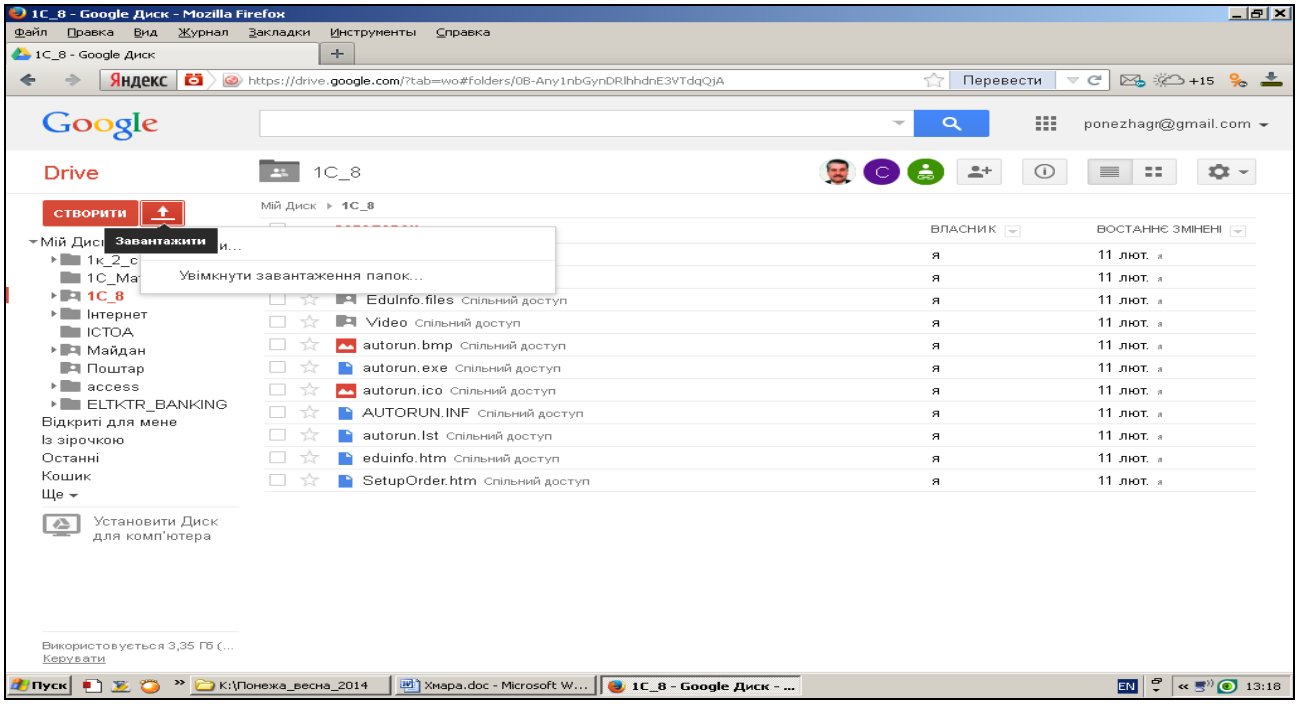


Рис. 11. Введення команди завантаження файлу або каталогу

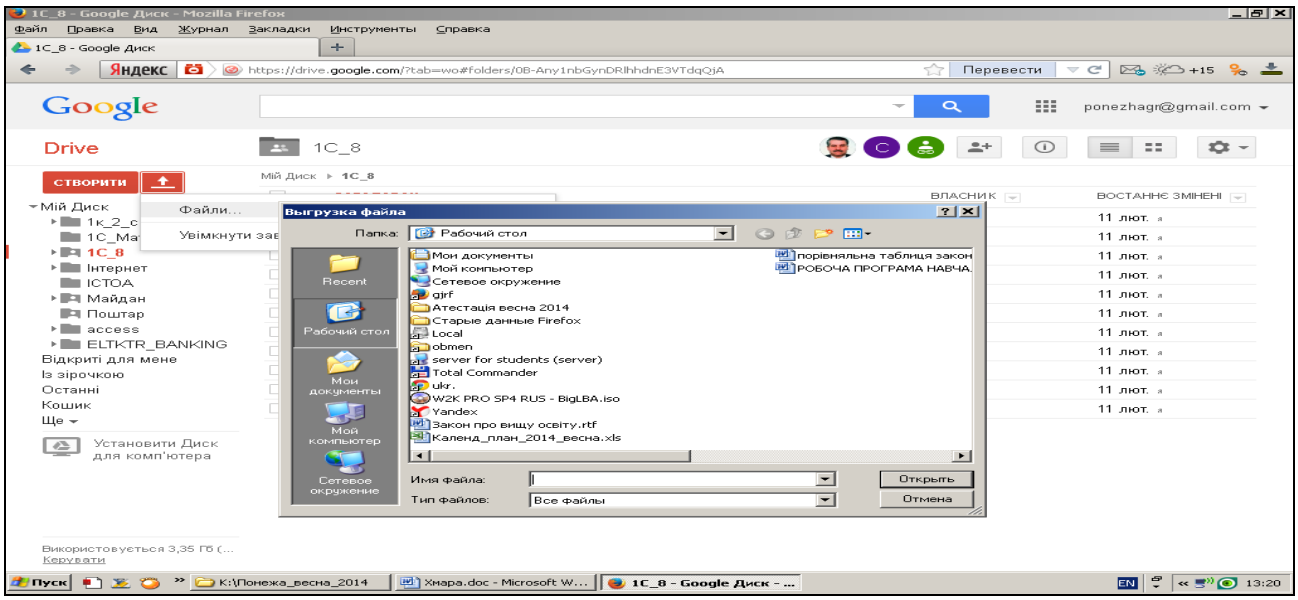


Рис. 12. Відбір потрібного файлу або каталогу

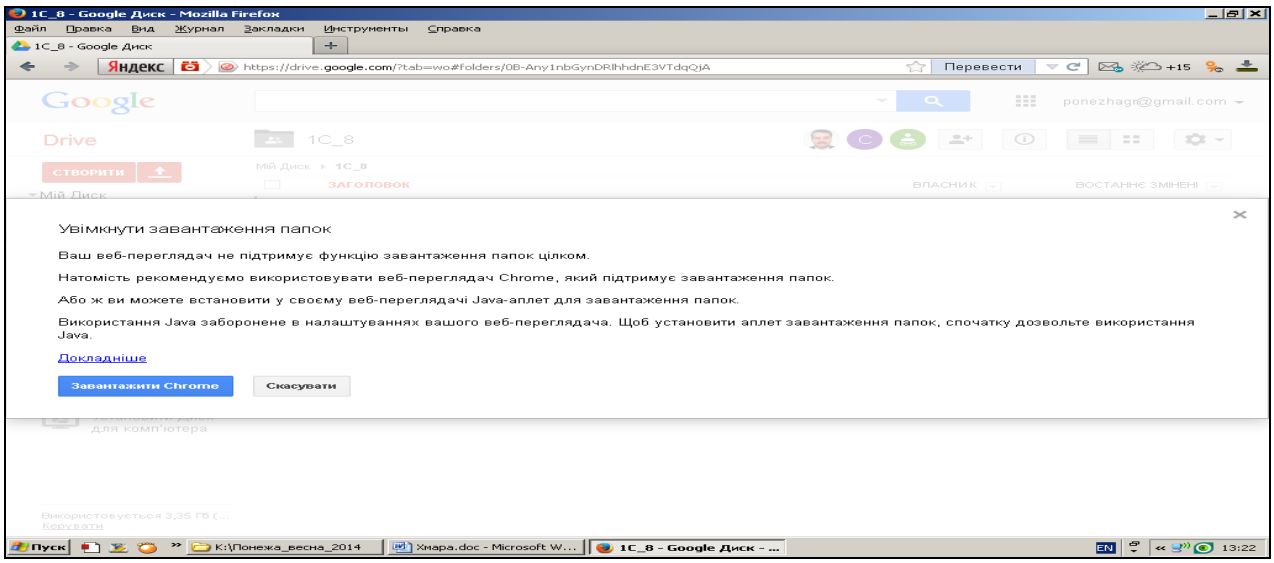


Рис. 13. Команда завантаження

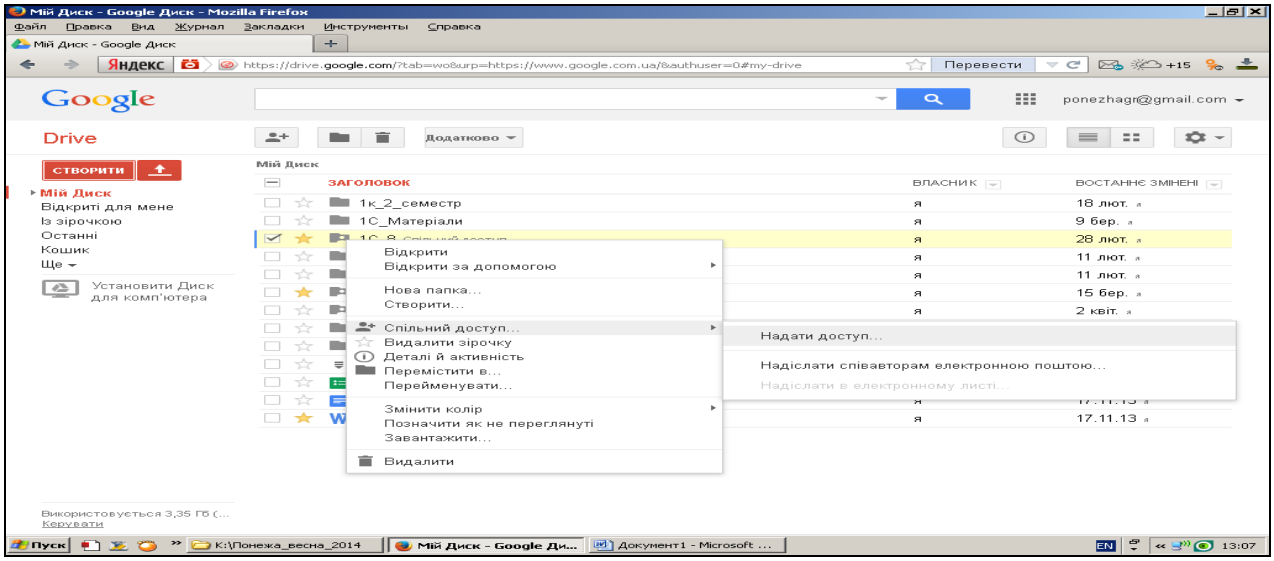


Рис. 14. Надання доступу

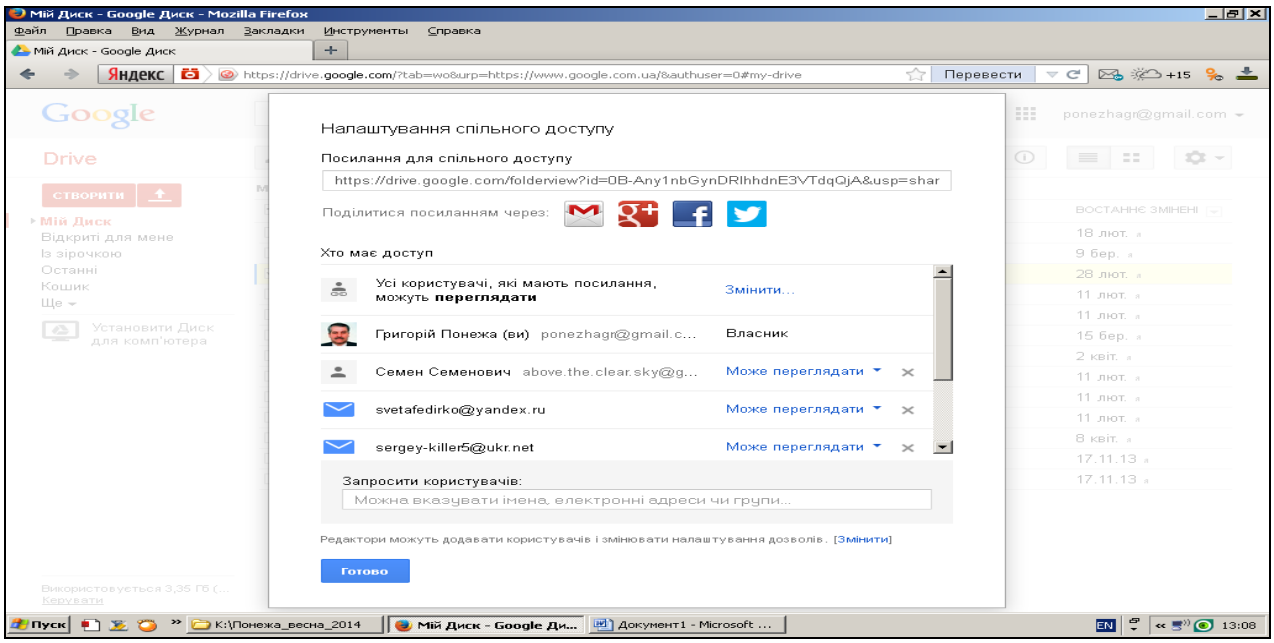


Рис. 15. Вибір параметрів доступу

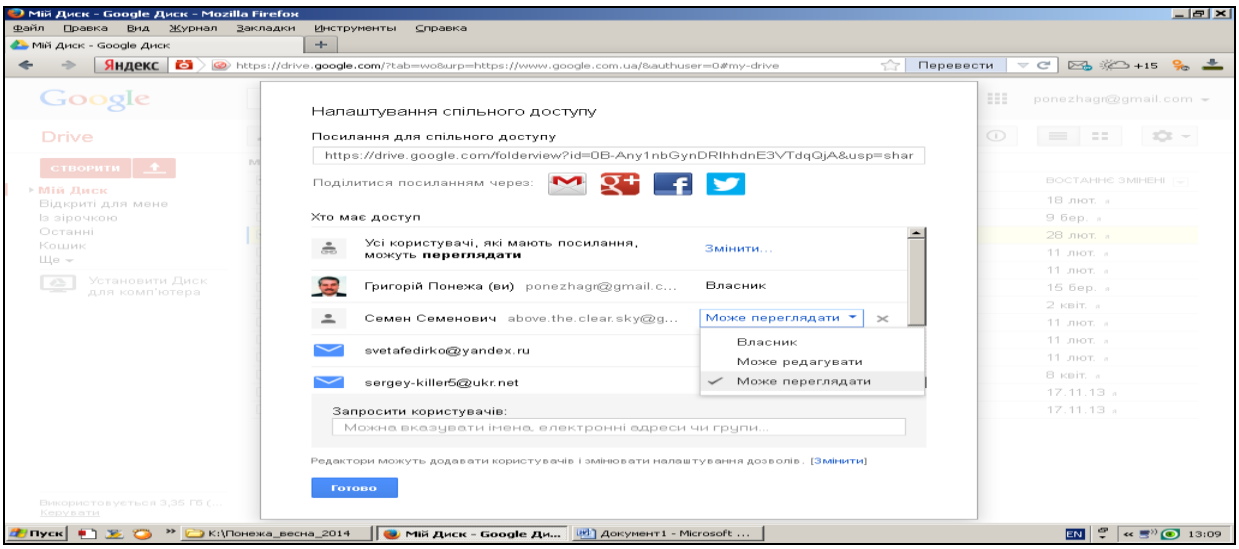


Рис. 16. Вибір параметрів доступу

3. Контрольні питання

1. Як визначаються хмарні технології?
2. Історія хмарних технологій.
3. Які послуги можна отримати з використанням хмарних технологій?
4. Які основні компанії існують з надання послуг в області хмарних технологій?
5. Як класифікуються хмарні технології відповідно до їх використання?
6. Вкажіть основні характеристики хмарних технологій.
7. Як провести реєстрацію акаунта на сайті **google.com.ua?**
8. Які можливості надає акаунт в розрізі роботи з файловою системою та різного типу документів?
9. Які можливості захисту інформації надає акаунт?

Додаток 1

Таблиця №1. Чисельна умова

Т №1	А	У	З
1	4	3	9
2	-1	-4	16
3	2	13	169
4			194

Таблиця №2. Аналітична умова

Т №2	А	У	З
1	4	=A1-1	=B1*B1
2	-1	=A2-3	=B2*B2
3	2	=4*A3+5	=B3*B3
4			=СУМ(C1:C3)

Таблиця №3. Результати 1–й ітерації пошуку рішення

T №3	A	У	З
1	4	3	9
2	-1	-4	16
3	1,999998	12,99999	168,999 8
4			193,999 8

Додаток 2

Тема: Створення, компіляція і виконання найпростішого програмного проекту.

Мета: Познайомитись з середовищем Borland Delphi та навчитись створювати найпростіші проекти.

Хід роботи:

У цій роботі ми створимо найпростіший додаток, що містить кнопки і найпростіші компоненти для виводу тексту, а також визначимо деякі оброблювачі подій. Роботу будемо виконувати в три етапи.

Етап 1. Створення простого додатка.

Розробка нового додатка починається зі створення проекту. Для цього в меню **File** виберете команду **New Application**.

Delphi створює проект, що містить три файли: Файл проекту *.dpr, Файл форми *.dfm, Файл модуля *.pas. При цьому в проектувальнику форм (Form Designer) Ви побачите нову форму, а в редакторі коду (Code Editor) – заготівку вихідного тексту модуля, що асоційований зі створеною формою.

Файл проекту являє собою текст, схожий на файл Pascal. Переглянути файл проекту можна виконавши команду меню **Project|View Sourse,** або **Ctrl-F12** і вибрати зі списку ім'я файлу проекту.

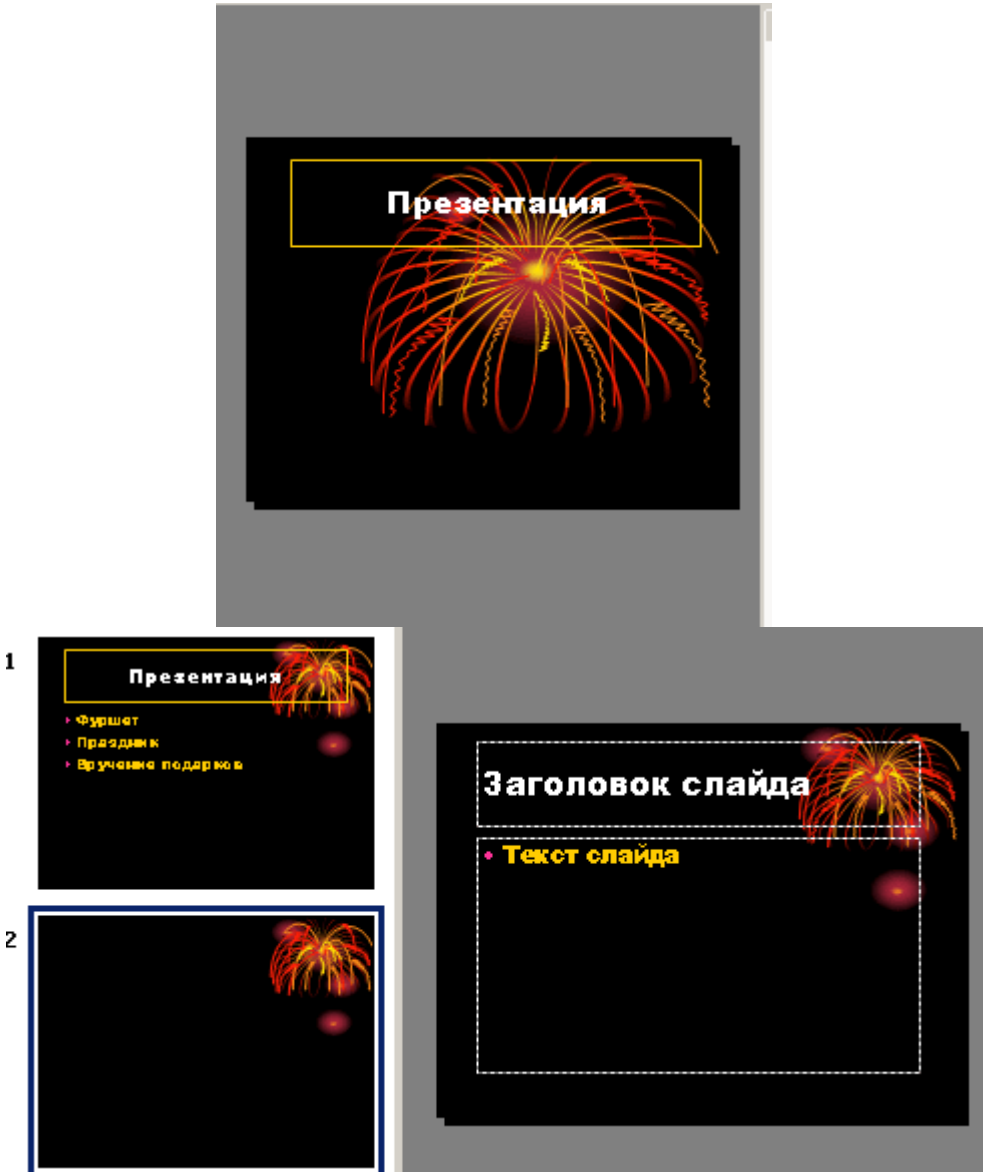
```
Program Project1;
Uses
Forms,
Unit ‘in Unit1.pas’{Form1};
{$R*.RES}
begin
Application.Initialize;
Application.CreateForm(TForm1,Form1);
Application.Run;
end.
```

Додаток 3

А)

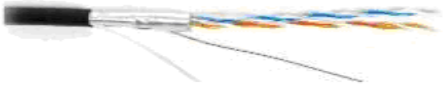

Заголовок
текст
Заголовок
текст
Заголовок
текст
Заголовок
текст
Заголовок
текст
Применить ко всем слайдам
Применить к выделенным слайдам
Показать крупные эскизы

Б)


Презентация
1
Презентация
Фуршет
Праздник
Вручение подарков
2
Заголовок слайда
Текст слайда

Додаток 1. Види кабелів

Вигляд кабелю	Короткий опис кабелю
	Кабель кручена пара, 100 пар, неекранований (UTP – Unshielded Twisted Pair).
	Кабель кручена пара, 32 пари, неекранований (UTP).
	Кабель кручена пара, 10 пар, неекранований (UTP).
	Кабель кручена пара, 4 пари, неекранований (UTP).
	Кабель кручена пара, 2 пари, неекранований (UTP).
	Кабель кручена пара, 1 пара, неекранований (UTP).
	Кабель кручена пара, 25 пар, фольгований (FTP – Folded Twisted Pair).

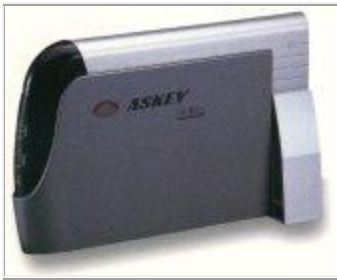
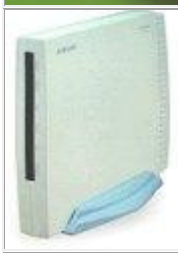
	Кабель кручена пара, 4 пари, фольгований (FTP).
	Кабель кручена пара, 2 пари, фольгований (FTP).
	Кабель кручена пара, 4 пари, екранований (STP – Shielded Twisted Pair).
	Кабель оптоволоконний, багато-модовий, 4 жили.
	Кабель кручена пара, 4 пари, фольгований (FTP).
	Кабель кручена пара, 2 пари, фольгований (FTP).
	Кабель кручена пара, 4 пари, екранований (STP – Shielded Twisted Pair).
	Кабель оптоволоконний, багато-модовий, 4 жили.
	Кабель оптоволоконний, одномодовий, 2 жили.

	Кабель оптоволоконний, одномодовий, 4 жили.
	Товстий коаксіальний кабель.
	Коаксіальний кабель для мереж кабельного телебачення.

Додаток 2. Модеми

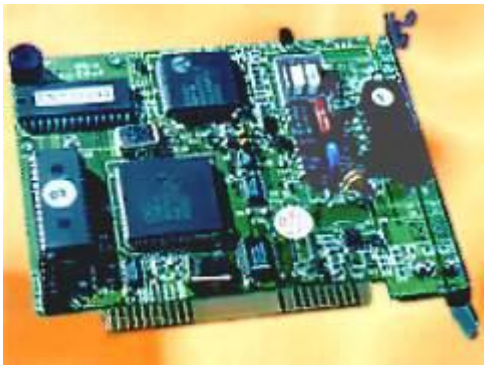
Зовнішні кабельні модеми

	PCX 1000 від Toshiba Цей модем перший з двох, що одержали DOCSIS сертифікат. Він побудований на Libit (тепер Texas Instruments) чипі, який об'єднує в собі модулятор-демодулятор і MAC чип від TurboNet Communications.
	DCM105 від Thomson Consumer Electronics Це другий з перших двох модемів, що одержали DOCSIS сертифікат. Він базується на наборі мікросхем Broadcom
	U.S. Robotics Cable Modem CMI і CMX від 3Com Corporation. CMI це внутрішній модем для ISA шини, який ще не одержав DOCSIS сертифікат. CMX - зовнішній кабельний модем, сертифікований на DOCSIS.
	SB2100 від General Instrument
	CM-100 від Arris Interactive (колишня Nortel Networks)

	CM010 від Askey Computer Corp. in Taiwan (використаний референсний дизайн від Cisco)
	UBR904 і UBR924 від Cisco. Ці модеми більше орієнтовані на SOHO ринок. Вони об'єднують в собі кабельний модем, маршрутизатор (router), і невеликий концентратор (hub).
	PD10d від Philips Electronics (використаний референсний дизайн від Cisco)
	Inforanger від Samsung Information Systems America (використаний референсний дизайн від Cisco)
	Sony Corp (використаний референсний дизайн від Cisco)
	Terayon мав кабельний модем сертифікований на DOCSIS 1.0 на початку вересня 1999р. Виходячи з прес реліза, він називається TeraJetTM, але цей продукт не міг бути знайдений на сайті компанії в день сертифікації. Наскільки відомо, це OEMпродукт, але ім'я справжнього виробника поки невідоме.
	DoxPort 101 це low-end модель. DoxPort 1010 (нижня фотографія) це high-end модель, яка була серед чотирьох сертифікованих в той час модемів.

	Best Data має Smart One DOCSIS 1.0 кабельний модем, сертифікований в грудні 1999р. Best Data створила модем спільно з TurboNet Communications, і продукт використовує TurboNet's MAC і PHY чип від Texas Instruments.

Внутрішні модеми






Додаток 3. Радіомодеми

Зовнішні радіомодеми

Внутрішні радіомодеми












Додаток 4. Список відкритих FTP серверів з коротким описом:

212.85.102.110 - зображення зі штрих-кодами
212.85.97.84 - файли у форматі psd, зображення й т.п.
213.59.94.99 - безліч різних програм, драйверів і дистрибутивів
46.242.48.16 - музика, дистрибутиви та інше
aspid.starlink.ru - серіали, музика, фільми й кліпи
bignosebird.com - різні файли в архівах
fkinodata.kiev.ua - безліч фільмів і відео
FTP сервера з новими HD і SD фільмами з різної тематики, іноді сервера бувають перевантажені: ftp://87.224.183.162/, ftp://188.73.134.180/, ftp://87.224.147.52/, ftp://188.73.177.25/
ftp.4players.de - німецький сервер для гравців
ftp.aecsoftware.com - програми
ftp.alta.ru - збіговисько різнопланових програм
ftp.aopen.ru - драйвери й інструкції до продукції фірми Aopen
ftp.arm.in.ua - версії Linux
ftp.asir.org - сервер, що спеціалізується на Freebsd
ftp.avtlg.ru - софт, гри й драйвери, різні Linux
ftp.bruker.de - програми й віртуальні образи дисків
ftp.cbn.net.id - різні програми під Windows, Linux і MAC у тому числі й на японському
ftp.cgd.ucar.edu - у папці pub файли студентів за папками, в інших каталогах безліч різнотипних файлів
ftp.comptek.ru - драйвери й інструкції до мережевого встаткування
ftp.cs.princeton.edu - небагато додатків під Linux і текстової інформації
ftp.csie.ncu.edu.tw - програми й дистрибутиви на Freebsd
ftp.ctm.ru - файли й керівництва до програми Rail-Тариф
ftp.daper.net - однойменний софт
ftp.demos.ru - різні файли
ftp.dlink.pl, ftp.dlink.ru, ftp.d-link.ru - сервери фірми D-link із програмами
ftp.ea.com - FTP сервер від відомого розроблювача ігор, компанії EA
ftp.ea.com.akadns.net - файловий сервер від однієї зі студій Electronic Arts
ftp.ents.ru - різнотипні файли, зображення, таблиці та ін.
ftp.espci.fr - французький сервер з користувацькими файлами
ftp.eu.uu.net, ftp.de.uu.net, ftp.archive.de.uu.net - програми, документи з Unix і Windows
ftp.fftw.org - збіговисько різнорідних файлів
ftp.foracom.ru - відео, музика, драйвера, документи й софт
ftp.futurenet.co.uk - різні програми для професійної роботи
ftp.gap-system.org - файловий сервер системи обчислювальної дискретної алгебри
ftp.gb.nrao.edu - різні користувацькі файли
ftp.gdc.ru - російський сервер з фото, відео й аудио матеріалами
ftp.gpntb.ru - файловий сервер державній публічної науково-технічної бібліотеки Росії
ftp.heapg.com - прошивання, драйвери й різні папки користувачів з документами
ftp.inist.ru - Oracle і різні програми, ОС
ftp.itojun.org - програми на Macos, Netbsd, Openbsd і інші файли
ftp.izmiran.rssi.ru - різні програми, у тому числі наукові
ftp.jpsoft.net - архіви зі старими DOS і OS/2 файлами
ftp.kaspersky.ee - сервер антивірусу Касперского
ftp.kde.org - файловий сервер KDE, графічної оболонки Linux
ftp.kfki.hu - угорський GNU сервер
ftp.komkon.org - книги на російському, тексти пісень, гумор і т.п.
ftp.lanit.ru - драйвера, технічна документація та ін.
ftp.martin.dk - документи за контролерами, прошивання й різні файли

ftp.math.ncu.edu.tw - сервер присвячений ОС Windows і Unix
ftp.mccme.ru - безліч книг з математики й наукових публікацій
ftp.net.pulawy.pl - польський сервер з драйверами, парою ігор, flash файлами й т.п.
ftp.netscape.com.edgesuite.net - різні програми й браузер Netscape
ftp.ni.com- сервер компанії National Instruments зі специфічним контентом
ftp.ntu.edu.tw - безліч дистрибутивів, середовищ розробок і програм під Linux
ftp.nuug.no, ftp.geologi.uio.no - норвезькі FTP сервера з музикою, відео й мн. ін.
ftp.ocs.ru - російський FTP сервер з різними файлами користувачів
ftp.olympus.ru - програми, браузери під Windows і Unix
ftp.pixil.org - файли за ОС Windows і інші
ftp.princeton.edu - файловий сервер університету Princeton з різними файлами
ftp.programbank.ru, ftp.prbank.ru - програми й ІС
ftp.relinfo.ru, ftp.mari.ru, ftp.mari-el.ru - музика, ігри, дистрибутиви й драйвера під Windows і Linux
ftp.rhd.ru - Fedora, RadHat і дистрибутиви до них
ftp.ru.openwall.com - специфічні програми, презентації та ін.
ftp.rzd-partner.ru - картинки й PDF файли з різною інформацією
ftp.sara.nl, ftp.tiscali.nl, ftp.de.debian.org, ftp.ee.debian.org, freepascal.stack.nl, ftp.twaren.net, ftp.cdpa.nsysu.edu.tw - FTP сервери за Linux, Debian з безліччю програм та ін.
ftp.sigma-soft.ru - програми для логістики й митниці від власника FTP сервера
ftp.skbkontur.ru - різні файли, у тому числі й бухгалтерські від ЗАТ
ftp.skpress.ru, ftp.skgroup.ru, ftp.pcweek.ru, ftp.pcmag.ru, ftp.crn.ru - FTP сервера російського IT видавництва, журнали, картинки та ін.
ftp.sovintel.ru - дистрибутиви до різних Linux і драйвери
ftp.spnet.net - болгарський сервер з дистрибутивами Linux і іншими файлами
ftp.tomsk.ru - безліч різнорідних файлів
ftp.ubi.com - файловий сервер Ubisoft з іграми, демонстраціями й патчами
ftp.unidata.ucar.edu - експериментальний FTP сервер з різнорідними файлами
ftp.urc.ac.ru - образи установчих дисків різних видів ОС та інші файли
ftp.usa.openbsd.org - FTP сервер з дистрибутивами на Openbsd
ftp.vgt.ru - мультфільми, музика, приколи, програми й ігри під Windows і Linux і багато ін.
ftp.vocord.ru - різноманітні прикладні програми й відео
ftp.westwood.com - різні додатки й файли від студії Westwood EA творців ігор із серії Command & Conquer
ftp://178.169.80.165/ - корисні книги, ISO, софт, музика, відео
ftp://188.126.44.223/ - ігри на PSP, малюнки, аудиокниги, музика, кіно, усе для CS
ftp://46.182.128.186/ - кліпи, музика, софт, Linux, програми
ftp://79.120.123.192/ - софт, відео, аудиокниги
ftp://84.22.139.7/ - нові ігри, операційні системи
ftp://87.224.147.100/ - гарна добірка фільмів, ігор, дистрибутивів Windows
ftp://87.224.251.217/ - книги, аудиокниги, програми, ігри, серіали, фільми
ftp://89.179.126.39/ - небагато фільмів
ftp://90.157.89.215/ - ігри, музика, відео, дистрибутиви
ftp://91.218.136.50/ - відео, софт, музика й ігри
ftp://95.154.90.4 - фільми для дорослих і для школярів вивчаючих анатомію
ftp://begemot.farlep.net/ - небагато ігор під Windows, додатків
ftp://cryptopro.ru/ - різні файли
ftp://files.3dnews.ru/ - різний софт і бенчмарки для Windows
ftp://ftp.aha.ru/- небагато додатків під Linux, Windows, Freebsd
ftp://ftp.basilka.ru/ - програми, книги, ігри, фільми, ISO образ ОС Windows 7 і Windows XP
ftp://ftp.biysk.ru/ - ігри, журнали, відео та інші файли
ftp://ftp.buster-net.ru/ - фільми, ігри, серіали, музика, софт

ftp://ftp.cisco.com/ - сервер компанії CISCO
ftp://ftp.des.tstu.ru/ - дистрибутиви Linux, додатки під Windows
ftp://ftp.dlink.ru/ - драйвери для мережевих пристроїв і їх опис
ftp://ftp.drweb.com/FTP сервер з усіма антивірусними продуктами від Dr. Web
ftp://ftp.dsip.net/ - різні файли й додатки
ftp://ftp.dvo.ru/ - безліч версій дистрибутивів Lunix
ftp://ftp.eimb.ru/ - FTP сервер про біологію
ftp://ftp.elcat.kg/ - книги, ігри, відео, програми
ftp://ftp.emt.ru/ - дистрибутиви, відео за CAD технологіям
ftp://ftp.fbo.gov/ - FTP сервер Federal Business Opportunities з перепискою англійською мовою
ftp://ftp.freebsd.org/ - усе про Freebsd
ftp://ftp.galaktika.ru/ - освітній сервер, програми, відео
ftp://ftp.gamesarchive.ru/ - велика кількість ігор, фільмів
ftp://ftp.gamma.ru/ - небагато додатків під Linux, Windows, Freebsd
ftp://ftp.hq.nasa.gov/ - FTP сервер NASA, презентації, файли й відео
ftp://ftp.inetik.ru/ - ігри, відео й софт, багато серіалів
ftp://ftp.infin.ru/ - ігри, сервер компанії Infin
ftp://ftp.intel.com/ - FTP сервер Intel'a, картинки, софт та ін.
ftp://ftp.jet.kg/-книги, ігри, відео, програми
ftp://ftp.kg/ - книги, ігри, відео, програми (George Carlin)
ftp://ftp.kraft-s.ru/- небагато додатків під Linux, Windows, Freebsd
ftp://ftp.lmp48.ru/ - фільми, ігри, програми (можливі тимчасові перерви в роботі цього сервера)
ftp://ftp.lviv.farlep.net/ - різні файли й додатки
ftp://ftp.mao.kiev.ua/ - софт, дистрибутиви Linux, різні файли
ftp://ftp.mgts.by/ - небагато дистрибутивів і додатків під Linux, Freebsd і Windows
ftp://ftp.microsoft.com/ - FTP сервер корпорації MS
ftp://ftp.mirrorservice.org/ - архів сайтів з Linux ін.
ftp://ftp.mkrovlya.ru/ - покрівельні роботи, відео, виставки й фото
ftp://ftp.netis.ru/ - дистрибутиви Linux, додатки під Windows
ftp://ftp.neva.ru/ - середня кількість софта для Freebsd, Linux і Windows
ftp://ftp.nhtsa.dot.gov/ - урядовий FTP сервер з відео й файлами FTP сервер музею з картинками й текстом
ftp://ftp.nstu.ru/ - ігри під Linux, додатки й дистрибутиви
ftp://ftp.nstu.ru/ - мало всякої всячини
ftp://ftp.oracle.com/ - сервер компанії Oracle
ftp://ftp.prbank.ru/ - різні файли й додатки
ftp://ftp.psu.ru/ - трошки софта
ftp://ftp.redcom.ru/ - небагато ігор і софта
ftp://ftp.rejoice.ru/ - ігри, ламалки паролів й патчи
ftp://ftp.relline.ru/ - небагато додатків для Windows і Linux
ftp://ftp.rsu.ru/ - FTP сервер Південного Федерального Університету, відео, програми, файли
ftp://ftp.ru/ - різні файли й додатки
ftp://ftp.sai.msu.su/ - небагато додатків для Windows і Linux
ftp://ftp.sbras.nsc.ru/ - різні офісні файли
ftp://ftp.sci-nnov.ru/ - небагато додатків під Linux, Windows, Freebsd
ftp://ftp.servplus.ru/ - сервер компанії з автоматизації торгівлі, відео
ftp://ftp.startrekftp.ru/ - серіали, ігри, фільми за всесвітом Star Trek, а також Lexx, X-files, і мн. ін.
ftp://ftp.svzserv.kemerovo.su/ - небагато додатків для Windows і Linux
ftp://ftp.symantec.com/ - FTP сервер компанії Symantec

ftp://ftp.tonk.ru/ - софт та інші файли
ftp://ftp.tonna.ru/ - фільми, аніме, документальна хроніка, музика, Linux iso-образи
ftp://ftp.totel.kg/ - книги, ігри, відео, програми
ftp://ftp.trinxp.com/ - різні файли й додатки
ftp://ftp.tvema.ru/ -відео, програмування, файли
ftp://ftp.ubisoft.com/ - FTP сервер від Ubisoft, ігри, демоверсії і т.д.
ftp://ftp.ufanet.ru/-офісні пакети, MS Office 2003-2010, Open Office, драйвери, ігри Command and conquer, Fallout 2
ftp://ftp.university.kg/ - антивіруси, інші файли для розробки ПЗ
ftp://ftp.veriton.ru/ - різні файли, драйвери
ftp://ftp.vfose.ru/ - книги з програмування на англійському, дистрибутиви й ігри
ftp://ftp.vsi.ru/ - небагато додатків для Windows і Linux
ftp://ftp.work.acer-euro.com/ - FTP сервер Acer, драйвера, утиліти, для всіх різновидів техніки
ftp://ftp.zoology.ubc.ca/ - зоологія, віруси, картинки
ftp://ftp1.duganet.ru/, ftp://ftp2.duganet.ru/ - відео, книги, анімація, софт, картинки, музика
ftp://ifarchive.org/ - ігри, емулятори, журнали, книги й статті з розробки ігор англійською мовою
ftp://ip137.118.dars-ip.ru/ - музика, ігри, програми
ftp://mc2.kiev.ua/ - книги, ігри, музика, софт, відео
ftp://mirror.yandex.ru/ - безліч дистрибутивів Linux
ftp://mirror2.corbina.ru/ - дистрибутиви Linux
ftp://nicosoft.ru/ - *FTP сервер* - музика, відео, ігри, софт і мн. ін.
ftp://niktest.g-service.ru/ - софт, ігри, програми
ftp://os2.fannet.ru/ - різні файли, додатки, ігри
ftp://sed.mgau.ru/ - різнотипні файли й додатки
ftp://stend.tomsk.ru/ - відео, аерографія, файли
ftp://sun-in.7upnet.kiev.ua/ - фільми, ігри, музика, програми
ftp://sunwayftp.kmdns.net/ - фільми, музика
ftp://tenzor.kmail.ru/ - фотошоп, дистрибутиви та інші файли
ftp://tigr.telenet.ru/ - програми, ігри (GTA 4 та ін.), hd аудио, відео
ftp://vintik7.myddns.ru/ - безліч HD відео, фільми, кліпи, музика й багато чого іншого
ftp://yakimus.kiev.ua/ - дистрибутиви, музика, відео, різні файли й додатки
ftp2.infograph.com - книги за програмами Brava і ін. на англійському
ftpg.corbina.ru, ftpg.corbina.net - безліч популярна онлайн ігор, дистрибутивів і іншого
home.dimonius.ru - безліч пікантного контенту, музики в тому числі дискографія Led Zeppelin
jrt-radio.dlinkddns.com:7000 - оболонка для FTP сервера з безліччю відсортованих музичних додатків різних жанрів
mirrors.industrium.ru - усе для дистрибутива Linux Crux
niihau.student.utwente.nl - FTP сервер голландського студента з різними файлами й програмами
opera.ftp.fu-berlin.de - емулятор на Andriod, ОС і т.п.
punck.cpms.ru - безліч програм Corel, Arconis, Photoshop, Archicad і т.п., ftp.stat.duke.edu - різні студентські файли й програми
rusunix.org - присвячений дистрибутиву Freebsd
softodrom.dlinkddns.com - ігри, фільми, програми й ін.
techsupport.services.ibm.com - сервер техпідтримки IBM, кілька програм і різні системні файли
topex.ucsd.edu - FTP сервер присвячений супутниковій геодезії
tug.org - програми до Linux

Додаток 5. Список пошукових систем Internet з коротким описом:

Google (www.google.com)

Це найшвидша і найбільша пошукова система. На даний час в ній проіндексовано понад 1,3 мільярда сторінок (з них повністю - трохи більше 700 мільйонів, про інші відомі тільки адреса і текст посилання). Google може знаходити інформацію на 117 мовах. Система добре працює з російськомовним ресурсам, є можливість вибрати мову інтерфейсу. На відміну від більшості пошукових систем, Google оцінює популярність ресурсу за кількістю посилань, що ведуть до нього з інших сторінок. Google – це пошукова система, яка використовує кількість посилань на веб-сайт, як основний параметр популярності сайту. Це є особливо корисним у пошуку хороших сайтів при простих пошукових запитах. Google має дуже велику базу даних проіндексованих сайтів і надає частину своїх результатів Yahoo і Netscape Search. Найбільшим придбанням Google з'явилася компанія YouTube. Правильність видачі результатів пошуку в Google.ru часто перевищує якість видачі результатів пошуку в пошукових системах, наприклад, у Яндексу. У своїй системі Google використовує механізм PageRank, що змінює "важливість" сайту при видачі результатів пошуку. PageRank залежить від кількості і якості посилань на ресурс (тобто майже те ж саме, що й індекс цитування у Яндексу). Але на відміну від Яндекс, вплив PageRank у Google не настільки значний. Всі сторінки Google кешує (заносить в свою базу) і дозволяє людині, що проводить пошук, дивитися документ, не відкриваючи його в першоджерелі, а беручи з кешу Google (що часто набагато швидше). Google – одна з небагатьох пошукових систем, яка повністю індексує всі сторінки, а не тільки найголовніші.

Пошукова система Google має також різноманітні сервіси та додаткові можливості пошуку, які постійно розширюються і вдосконалюються. Наприклад, рядок пошуку в Google можна використовувати як калькулятор. У рядку пошуку вводиться, припустимо, (20 +35) * 319 і система видає правильну відповідь. Добрий опис можливостей пошукача наведено на сайті компанії.

Yandex (www.yandex.ru)

Краща з пошукових систем російського виробництва. Вона індексує в основному російськомовні ресурси, при цьому за можливостями не поступається зарубіжним системам. Також в ній існує багато різних можливостей для удосконалення системи пошуку інформації. Це призводить до хороших результатів і потрібні посилання, як правило, виявляються вже в першій десятці результатів. Має "полегшену" версію (з мінімумом елементів дизайну) на http://www.ya.ru. Офіційно пошукова машина Yandex.Ru була анонсована 23 вересня 1997. Уже тоді пошуковик мав деякими перевагами – можливість перевірки документів на унікальність, облік морфології російської мови, можливістю пошуку з урахуванням відстані (наприклад, при пошуку точного словосполучення). Основною відмінною рисою Yandex був ретельно розроблений алгоритм оцінки відповідності відповіді запиту (релевантності), що враховує не тільки кількість слів запиту, знайдених в тексті, а й "контрастність" слова (його відносну частоту для даного документа), відстань між словами і положення слова в документі .

AltaVista (www.altavista.com)

Система AltaVista є однією з найбільш великих пошукових систем (за кількістю проіндексованих сторінок). Даний факт, а також можливість вести пошук за ускладненими критеріями відбору привели до великої популярності AltaVista. Ця пошукова система також пропонує додаткові послуги у вигляді пошуку за каталогами (взятими з Open Directory and LookSmart), а також службу під назвою "Ask AltaVista" ("запитай AltaVista"), результати якої беруться з Ask Jeeves. AltaVista почала надавати свої послуги в грудні 1995 року. В даний час AltaVista володіє пошуковою системою Raging Search. До недавнього часу AV була великим порталом, але з причин фінансового (і не тільки) характеру значно скоротила кількість сервісів.

Yahoo! (www.yahoo.com)

Один з перших (був заснований в 1994) і найбільш популярних пошукових серверів в Інтернет. На Yahoo складений великий структурований каталог категорій (categories). Спочатку пошук здійснюється в них, потім у власному архіві, потім – з використанням системи Google. Yahoo має базу даних в більш ніж 1 млн. проіндексованих сайтів. Yahoo є найстаршою пошуковою системою, яка почала надавати свої послуги в 1994 році. Секрет успіху Yahoo полягає в людях. Yahoo має близько 150 редакторів, для того, щоб складати і редагувати вміст своїх каталогів. Дивно, але ця неймовірно популярна система, яка обслуговує мільйони запитів щодня, зародилася як проста колекція закладок, яку поповнювали всього 2 людини – Девід Філо та Джеррі Янг.

Lycos (www.lycos.com)

Останнім часом – одна з найпопулярніших систем. У той же час ніяких особливих можливостей вона не надає – "AND" "OR", пошук фраз, обов'язкова присутність / відсутність слова; в розширених можливостях – пошук в назві, URL, імені хосту та / або назві домену; 25 мов, включаючи російську, – словом, весь "загальноприйнятий" набір. Можна вказати тип змісту ресурсу - авто, книги, ftp, download, новини і т.д. Очевидно, популярність Lycos - наслідок масштабу цього великого проекту.

Рамблер (www.rambler.ru)

До недавнього часу найвідоміша російська пошукова система. Але останнім часом його популярність різко впала. Зараз в цій системі використовується поліпшений механізм пошуку, змінився дизайн, але за якістю Rambler все одно не зрівнявся з Яндексом або Google.ru. На сайті присутня рейтинг-каталог ресурсів Rambler Top 100, один з визнаних джерел статистичної інформації про інтернет-проекти.

MSN (www.msn.com)

Пошуковик розроблений і запущений компанією Microsoft в 1997 році. На відміну від інших пошукових систем, раніше у MSN ніколи не було власного павука або каталогу. З 1997 року для видачі результатів пошуку використовувалися різні бази даних, такі як: Yahoo!, LookSmart, Altavista, DirectHit, Inktomi і RealNames. Тільки з початку 2005 року MSN запустив бета-версію власного пошукового алгоритму. Користувачі MSN Search, як і раніше, зможуть здійснювати пошук за всією мережею в цілому, а також за окремими тематичними категоріями, в тому числі і за енциклопедією Microsoft Encarta. Новий движок включає можливість локалізованого пошуку (Near Me) – система здатна автоматично визначати місцезнаходження користувача за IP-Адресою його комп'ютера. Є російськомовна версія.

Серед перерахованих вище пошукових систем найбільш популярною серед користувачів Інтернету є Google. На початку 2009 року компанія ComScore підвела останні підсумки аналізу ринку пошукових систем, які показали частки, займані на ринку основними пошуковими системами.

Рис. 2. Ринкові частки пошукових систем

У Internet Google також входить до трійки лідерів ринку.

Користувачі зазвичай говорять про те, що вони використовують пошуковик який їм подобається і змінювати його вони не хочуть. Проведений компанією Microsoft опитування дозволяє зробити дещо інші висновки. Можна відзначити кілька моментів. Дослідження показали, що люди замислюються над тим, який пошуковик використовувати, приблизно настільки ж, наскільки вони замислюються, якою дорогою піти на роботу або чи варто чистити зуби перед сном. З іншого боку, опитування показує наступне. Незважаючи на те, що дві третини користувачів кажуть, що використовується ними механізм їх влаштовує, менш 40% опитаних сподівається на прийнятний результат при відповіді на місцеві запити. Вибір пошуковика – скоріше, питання звички, ніж серйозно усвідомлена дія. Тому для розробників пошукових систем є, куди рухатися. Основна Прблема тут – людський фактор. На думку головного редактора онлайн-журналу Search Engine Land Денні Саллівана: «Зробити щось таке, щоб переманити маси на свій бік – дуже важко. Google, звичайно, не без гріха – але його похибки не настільки критичні, щоб все ось так відразу припинили ним користуватися». Щоб змусити відмовитися людини від використання знайомого і звичного йому пошукача, нова система повинна бути революційною і явно відрізняється від колишніх хоча б за якоюсь ознакою. Необхідно якісна зміна в цій галузі.

Метапошукові системи (searchbots)

Так як. різні пошуковики використовують різні алгоритми пошуку і приділяють "особливу" увагу різним ділянкам мережі, до яких вони найбільш адаптовані, логічно в багатьох випадках шукати відразу декількома пошуковими машинами. Цю можливість і пропонують searchbots, Автономні пошукові агенти. В основу роботи searchbots закладений наступний принцип: із запиту користувача генеруються запити, відформатовані в синтаксисі і логічних конструкціях кожного конкретного пошукового ресурсу. Таким чином, з одного запиту метапошукова машина робить безліч запитів, які потім розсилаються широкому колу пошукових машин (та / або каталогів). Зібравши результати, мета-пошукова система видаляє дубльовані посилання і, відповідно до свого алгоритмом, об'єднує/ранжує результати в загальному списку. Безумовно, автономні пошукові агенти стали значним проривом у розвитку технологій пошуку. Але використання цих пошуковиків приховує в собі певні проблеми.

Наприклад, іноді пошук із застосуванням мета-засобів може виявитися дуже повільним, адже цим системам доводиться координувати за часом надходження результатів обробки пошукового запиту від декількох серверів. Ще одним недоліком мета-засобів є те, що вони не дозволяють повною мірою використовувати можливості мови запиту кожного з застосовуваних пошукових засобів. Більшість вказаних систем погано розуміє (чи не розуміє зовсім) російську мову. Метапошукові системи не ведуть власної бази інтернет-сайтів, а лише обробляють результат, представлений іншими пошуковими машинами. Обсяг цієї обробки може бути різним. Найпростіші метапошукові системи дозволяють видалити повторювані посилання та створити єдиний список сайтів, впорядкований за релевантністю. Метапошукові системи, що з'являються останнім часом, дозволяють проводити кластеризацію (об'єднання) отриманих адрес сайтів за різними критеріями. Такі системи дозволяють виявляти в списку отриманих сайтів загальні ключові фрази і групувати сайти відповідно до них. Автономні пошукові агенти продовжують розвиватися - головним плюсом метапошукових систем є їх можливість шукати в базах безлічі каталогів і пошукових машин, що дозволяє швидко переробляти великі обсяги інформації й істотно економити трафік. Автономні пошукові агенти бувають двох класів. Одні, як і звичайні пошуковики, розташовуються на публічному онлайн-ресурсі інші – встановлюються на персональний комп'ютер.

Vivisimo (www.vivisimo.com)

Основною перевагою цього пошуковика є те, що він, крім видачі посилань на відповідні сторінки в Інтернеті, сортує інформацію за категоріями. За запитом користувача система будує дерево таке, в якому розміщені не тільки ключові слова, а й типи документів

(статті, новини). Якщо в кластерах-темах знову зустрічаються повторювані комбінації, то створюються підтеми (підкластери). Система пропонує не тільки зручний для сприйняття результат пошуку, але й не менш зручні засоби роботи з ним. Поруч із назвою кожного сайту є посилання, за допомогою яких можна відкрити посилання в новім вікні, у фреймі поточного вікна й здійснити попередній перегляд знайденого сайту. Для кожного знайденого посилання зазначений також засіб, за допомогою якого вона знайдена. Крім того, користувач може провести додатковий пошук за вже відібраною інформацією.

Browsys (www.browsys.com)

При використанні даної системи проблему пошуку можна розв'язати простим перебором варіантів (Google, Bing, Youtube, News, Blogs, Wikipedia і т.д). Browsys пропонує 17 різних варіантів пошуку, до яких відносяться великі пошукові системи, а також кілька сервісів Google, таких як Google Новини, популярні соціальні мережі, обмін знаннями й Bookmarking сайти, і, нарешті, Ebay. Як і у звичайній системі, запит уводиться в спеціальне віконечко, а от кнопки «шукати» тут немає. Замість цього користувачеві пропонується вибрати один з розвідувачів, назви яких написані на кнопках. Після натискання однієї з них, на екрані з'являться посилання, які знайшла обрана пошукова система. Якщо щось не влаштовує, можна нажати іншу кнопку й так, поки потрібний результат не буде знайдений, або не закінчиться весь список пошукових систем. Для того, щоб спеціалізувати ваш запит, потрібно вибрати відповідне посилання у верхньому меню. Відповідно до цього міняється й список задіяних пошукових систем. Є об'єднаний пошук за Google і Bing. Шукати можна не тільки за словами, але й за зображеннями, звуку й відео. Є пошук новин за Worldnews, Topix, the Guardian, the NY Times, Google News, і ін. Іншої цікавою особливістю даного розвідувача є можливість створення власного списку сайтів з даної тематики. Цей список створюється в сервісі «віртуальний пошук» і зберігається в розвідувачі під обраним для нього іменем.

Dogpile (www.dogpile.com)

Це метапшукова система від Infospace, який поєднує результати пошуку найбільш популярних пошукових систем Google, Yahoo! Search, MSN, Ask.com, About, MIVA, Looksmart і ін. Досить цікава метапошукова система з веселим мультяшним інтерфейсом. Він почав працювати в 2006 році. Dogpile у першу чергу виводить ті посилання, які дублюються відразу в декількох пошукових машинах (поруч із кожним посиланням вказується, де вона була знайдена). Чим нижче за списком ви опускаєтеся, тим більше унікальні посилання бачите, а це значить, що за ними утримується або інформація, яка не індексується іншими розвідувачами, або матеріали, які були додані відносно недавно. Є зручна функція для контролю вмісту. Він передбачає три варіанти фільтрації: відсутність фільтрації, відкидання найбільш нескромних сторінок і, нарешті, максимальна фільтрація, після якої, по ідеї, повинні залишитися тільки бездоганно благопристойні посилання. Можна налагодити спосіб сортування результатів пошуку зображень, новин і медіафайлів. Крім того, у відповідності зі своєю назвою на сайті розвідувача організують реальні акції в допомогу тваринам, викладені різні картинки із собаками і т.д.

Інтелектуальні пошукові системи

Як відзначають дослідники Інтернету, результати пошуку у великому ступені залежать від правильно сформованого запиту. Багато з людей, намагаючись одержати яку-небудь інформацію, формулюють свої питання в досить розмовній формі у вигляді запитів типу, «яка завтра буде погода». Звичайний розвідувач видає посилання у відповідь на таке питання відповідно до принципу максимально пересічних слів у питанні й у змісті тексту на сайті. Тому, щоб одержати відповідь на своє питання, користувач повинен сам переглянути видану інформацію й знайти в ній шуканий розв'язок завдання. У створенні інтелектуальних пошукових систем реалізується ідея про комп'ютер, який зможе спілкуватися з людиною на зрозумілому йому мові, володіючи при цьому набагато більшими пізнаннями, ніж звичайна людина. Передбачається, що така система буде

відповідати на найрізноманітніші питання користувачів, задані на звичайній розмовній мові. І відповідати не посиланнями на сторінки або цитатами з них, а фактами. В останні кілька років такі пошукові системи з'явилися. Це Hakia, Powerset, True Knowledge і Wolframalpha.

True Knowledge (www.True Knowledge.com)

Нова пошукова машина True Knowledge уміє працювати зі звичайними запитами. Однак головна особливість цього розвідувача – планується, що він буде відповідати на користувацькі запити не зовсім звичайно – у пошуковій видачі будуть розміщені не тільки посилання на сторінки або цитати, а факти. У цей момент за запитами доступна бета-версія системи, яка комбінує ці дві видачі – задавши запит, можна одержати й список посилань, і, в окремій області вікна, список фактів. Приміром, запит виду – «who is George Bush» підносить у верхній частині список фактів, які являють собою своєрідні кнопки переходу на більш докладну інформацію. Користувачам сервісу надається можливість поповнення бази даних фактами, подіями, особистостями; у наявності кілька рівнів, а для досвідчених користувачів доступна можливість додавання нових класів, об'єктів і зв'язків. У деяких випадках пошукова видача являє собою досить релевантні посилання й факти, однак іноді система не справляється навіть із найпростішими запитами. А в цілому видача досить сильно залежить від заданого запиту.

Wolfram Alpha (www.wolframalpha.com)

Wolframalpha — база знань із елементами штучного інтелекту, у якій закладена величезна кількість математичних моделей і інформації. Її творець Стівен Вольфрам після навчання в Ітоні й Оксфорді одержав ступінь доктора наук в області теоретичної фізики в Каліфорнійському технологічному інституті в 20 років. В 1981 році йому був вручений "грант геніїв", стипендія фонду Макартур. Його книга "Нова наука" (A New Kind of Science), у якій він заявляє, що в основі всіх наук можуть лежати прості алгоритми, а не складні структури й правила, була зустрінута захватами з боку одних і несхваленням інших. В основі Wolfram Alpha лежить "движок" Mathematica. У нього вбудований потужний логічний механізм, який може робити виводи, маючи дані й математичну модель. Цей підхід розповсюджений на області, слабко пов'язані з математикою, зокрема, географію, бізнес і кулінарні рецепти. Wolfram Alpha може, наприклад, не тільки відповідати на запитання начебто ″Де перебуває Єгипет?″ (прості розвідувачі з таким навчилися справлятися), але й ″Де завтра опівдні буде перебувати МКС?″. Для того щоб відповістити на останнє запитання, потрібно зрозуміти, коли настане завтра, а також мати математичну модель руху МКС або розрахувати її, виходячи з наявних про станцію даних. Звичайні розвідувачі цим не займаються. Wolfram Alpha для цього створений. Розвідувачем Wolfram Alpha можна назвати з великою натяжкою. Він у вкрай рідких випадках звертається до зовнішніх джерел даних. Команда Стівена Вольфраму витратила кілька років на створення бази даних фактів, а також великої кількості математичних моделей. Розвідувач займається пошуком у бібліотеці, заснованої на програмних продуктах Стефана Вольфраму – Mathematica і A New Kind of Science. Розроблювальні автором алгоритми дозволять додати цим даним зрозумілу для користувача форму. Коли користувач ставить запитання, дані для відповіді будуть братися саме із цієї бази. Не ідеться про запити природньою мовою, хоча сама мова запитів дуже схожа на англійську. У той же час система розуміє короткі запити, схожі з тими, до яких звикли користувачі звичайних розвідувачів. Відповідь виводиться у вигляді діаграм, таблиць і графіків. Запуск першої публічної версії системи відбувся 16 травня 2009 року.

Спеціалізовані пошукові системи

Пошук зображень

Taggalaxy (www.TagGalaxy.com)

Цей пошуковий сервіс являє собою засіб для пошуку зображень на Flickr.com, з попереднім переглядом. Кількість картинок, що завантажуються на сервери цього сервісу настільки велике, що для того щоб знайти якесь конкретне зображення в цьому океані

знімків і картин, необхідна окрема пошукова система. А незвичайним його робить інтерфейс пошуку, який повністю зроблений тривимірним. Процес пошуку за ключовим словом нагадує якусь комп'ютерну гру. Taggalaxy – ця незвичайна пошукова система має тривимірний інтерфейс у вигляді планетної системи, тим самим він виглядає воістину красиво й захоплююче.

Picsearch (www.picsearch.com)

Сервіс працює дуже швидко, виводить результати пошуку в зручній формі й майже ніколи не показує непотребних посилань. Під час пошуку не забувайте користуватися додатковими налагодженнями (кнопка Advanced Search), де можна задати розмір шуканого зображення, його кольоровість і наявність на картинках анімації.

Retrievr (labs.systemone.at/retrievr)

Пошукова система шукає саме картинки (але не за всім Інтернетом, а тільки за Flickr). Однак у пошуку потрібно задавати не слово, а, як не дивно, теж картинку. У маленькім віконці малюєте що-небудь (графічний редактор самий найпростіший – 4 розміри кисті, така палітра, як в «Фотошопі»). Намалювали, відсунули курсор убік – і retrievr відразу видає безліч зображень, які хоч чимсь схожі на вашу «творчість». Збігу, щоправда, трапляються нечасто: система орієнтується тільки на основні геометричні форми, а виходить, намалювавши чорну морду кота, ви в результатах пошуку цілком можете одержати кілька портретів людей, яку-небудь чорнильну ляпку й, допустимо, камінь. Але весело. Можна приємно провести час і знайти чимало несподіваних зображень.

Пошук музики й звуків

Findsounds (www.findsounds.com)

Розвідувач створений для пошуку звуків (не плутати з музикою), різних звукових ефектів і т.д. Ресурс дозволяє шукати звукові файли різних форматів – wav, mp3, aiff, au. У базі даних ресурсу є найрізноманітніші звуки – лементи тварин, скрегіт машин, дзенькіт, стукіт, сирени, дзижчання комах, гуркіт вибухів і стрілянини, сплеск води і т.д. У результатах пошуку ресурс показує не тільки посилання на знайдені файли, але і їх основні характеристики, а також показує графік амплітуди звуку, за якою можна судити про характер звучання даного прикладу. Шукає за аудіо форматами – AIFF, AU, MP3 і WAVE, за кількостю каналів – mono і stereo, і ще за декількома параметрами, включаючи максимальний розмір файлу. Шукає швидко й багато, що у зв'язуванні зі зручним і інтуїтивно-зрозумілим інтерфейсом дозволяє використовувати його в потребах професійних і не тільки. Він схожий на Google. Даний розвідувач надає потужні можливості, але в той же час є простим, зрозумілим і зручним у користуванні. Є дуже зручна функція для батьків: у цьому розвідувачі фільтрується музика, що містить у собі ненормативну лексику. Одержавши запит у командному рядку – приміром, Rocket, – розвідувач видає кілька сотень посилань на файли, у яких хтось його виголошує, або лунає звук ракети, або звук старту космічного човника, а то й зовсім звук пострілу з ракетниці в Quake або DOOM. База звукових ефектів Findsounds може знайти застосування в самих різних областях – від розробки комп'ютерних ігор і інших додатків, до створення презентацій і всіляких кліпів.

Musicplasma (www.musicplasma.com)

Вам подобається певна музика й ви прагнете знайти що-небудь схоже? Для цього існує розвідувач Musicplasma.com. На відміну від інших розвідувачів він шукає не музику як таку, а виконавців. Якщо задати серверу будь-чиє ім'я або назва групи, то засобами флеш-графіки в браузері відобразиться мудре сузір'я імен: у центрі – шуканий виконавець, а десятки інших розмістяться ближче або далі від нього, у міру подібності їх музики. Картинка дуже наочна й дозволяє відразу побачити, хто на кого і як сильно схожий. Кулька з пошуковим запитом перебуває в самому центрі карти. Найбільш схожі на нього виконавці розташовуються поруч. Якщо вам подобається той, що в центрі, то майже напевно вам сподобаються й сусідні, хоча ви могли ніколи раніше не чути навіть їх назв. Розмір кожної

кульки відповідає популярності групи. Імена з'єднуються лініями, і, прослідковуючи ланцюжка, що відходять від знаменитих команд, робиш чимало відкриттів, натикаючись на невідомі групи, що відіграють, на думку Musicplasma, схожу музику. Наприклад, з її допомогою можна виявити неймовірні зв'язки між класичними композиторами – такими як Бетховен, Брамс, Аркуш, Вагнер – і сучасними музикантами. Деякі "карти зірок" так великі, що не вміщаються на екрані, але за ними легко переміщатися, просто кликаючи мишею. Клацання по будь-якому імені запускає новий пошук асоціативних зв'язків, і через пару секунд можна спостерігати картину, створену вже навколо іншого центру. Musicplasma – це, у першу чергу, чудовий інструмент для досліджень. Якого б найвідомішого виконавця не ввести, обов'язково поруч із ним виявиться пара-трійка «родинних», але абсолютно невідомих музикантів. Для багатьох музикантів у спеціальнім віконці ліворуч виводиться їхня повна дискографія. Кожний з альбомів можна купити (посилання ведуть в Amazon).

Новинні розвідувачі

Wikio (wikio.com)

Wikio – новини й інформація. Пошукова система є як би величезним інформаційним порталом, суть полягає в пошуку новинних сайтів і блогів зі свіжою пресою.

Addictomatic (www.addictomatic.com)

Розвідувач пропонує відмінну заміну ранковій газеті. Уводите в поле пошуку будь-яке слово, пов'язане з подіями, що відбуваються зараз, відомими людьми або подіями, і одержуєте результат – огляд найпопулярніших сервісів зі згадуванням інформації, що цікавить вас, на них. Серед сайтів, за якими проводиться пошук і збір інформації: новини live.com, повідомлення з Twitter, відео з Youtube, Google Blogs, картинки з Flickr і багато чого іншого.

Наукові пошукові системи

У даному розділі зібрані посилання на спеціалізовані наукові пошукові системи, електронні архіви, засоби пошуку статей і посилань.

Scirus (Scirus.com)

Універсальна наукова пошукова система. Багаторазово визнавалася кращою спеціалізованою пошуковою системою, що включає в себе реферати більш 28 млн. статей з більш 14,000 журналів (52% з них європейські) 4,000 видавництв, патентів, матеріалів конференцій і т.д. із усього світу, включаючи 260 російських журналів. Глибина охоплення – 40 років (з 1966 року), включені всі спеціалізовані бази Elsevier, основні бази інших видавництв (напр., Inspec, Medline і т.д.), дані із платформ усіх наукових видавництв (напр., Springer), дана інформація з індексації в інших базах за кожним записом, а також інформація із цитуємості (зокрема для російських авторів). З недавніх пір з'явилася можливість установити браузерную панель Scirus. Це дозволяє здійснювати пошук в Scirus'e прямо із браузера, швидко переміщатися між результатам пошуку за різними запитами, підсвічувати на знайдених сторінках слова з пошукових запитів, додавати цікаві наукові сайти в індекс цієї пошукової системи.

Scholargoogle (scholar.google.com)

Пошукова система з наукової літератури. Включає статті великих наукових видавництв, архіви препринтів, публікації на сайтах університетів, наукових суспільств і інших наукових організацій. Шукає статті в тому числі й російською мовою. Що не маловажно, розраховує індекс цитування публікацій і дозволяє знаходити статті, що містять посилання на ті, що вже знайдені.

Scholar (www.scholar.ru)

Розвідувач був створений для спрощення пошуку документів наукової тематики російською мовою. У першу чергу, проект розрахований на електронні публікації, виконані в Росії. Проект індексує також дисертації, монографії й інші наукові матеріали, індексуються й переведені з російського матеріали. Основна мета проекту – збір інформації

про публікації яківільно копіюються. Проект не розрахований на зберігання повних текстів публікацій у тому або іншому вигляді. Замість цього, використовується база посилань на тексти документів з інформацією про самі публікації (анотація, автори і т.д.). Проект Scholar.ru придасться насамперед студентам і тим, хто цікавиться науковими публікаціями. Як і у випадку з іншими «розвідувачами», сам сайт не містить яких-небудь публікацій, а тільки надає посилання на них. Можна додавати посилання на свої статті в базу даних. Є цікавий форум з різних наукових тематик. Також на сайті приводиться програма наукових конференцій.

Science Research Portal (www.rad.pfu.edu.ru)

Наукова російськомовна пошукова система, підтримувана компанією Deep Web Technology (DWT), що здійснює повнотекстовий пошук у журналах багатьох великих наукових видавництв, таких як Elsevier, Highwire, IEEE, Nature, Taylor & Francis і ін. Шукає статті й документи у відкритих наукових базах даних: Directory of Open Access Journals, Library of Congress Online Catalog, Science.gov і Scientific News.

Medpoisk (www.medpoisk.ru)

Розвідувач інформації винятково на медичних сайтах. Дана пошукова система використовує движок пошуку від Google. Medpoisk.ru – це універсальний розвідувач, який призначений для пошуку винятково на медичних сайтах. Цей сайт – відмінний інструмент для кожного медика й усіх, хто бажає одержати відповідь на будь-яке питання з області медицини. Як лікувати ту або іншу хворобу, які протипоказання в тих або інших ліків, до якого лікаря звернутися – усе це й багато чого іншого можна довідатися, задавши запит розвідувачеві. Розвідувач містить у собі біржу праці й може використовуватися для пошуку роботи серед медичних працівників. Ресурс також містить каталог медичних установ, розсортованих за регіонами. Серед цих установ адреси клінік, медичних центрів різної спрямованості, родильні будинки, діагностичні центри, косметологічні салони та ін.

Pubmed (pubmed.com)

Це пошукова система розроблена в Національному Центрі Біотехнологічної Інформації (National Center for Biotechnology Information – NCBI), який є підрозділом Національної Медичної Бибилиотеки США (National Library of Medicine – NLM), що є частиною Національного Інституту Здоров'я США (National Institutes of Health – NIH). MEDLINE – база даних медичної інформації, що включає бібліографічні описи з більш ніж 4800 медичних періодичних видань із усього світу, починаючи з 1949 р. У цей час MEDLINE доступна безкоштовно для пошуку через Інтернет як для фахівців, так і для широкої публіки. Плюси цієї системи очевидні: величезна база даних і велика кількість функцій для керування пошуком. Зараз це універсальний розвідувач літератури з медичної тематики. Справа не тільки в тому, що бази даних охоплюють велику кількість публікацій, але й у зручності пошуку й обробки отриманих результатів.

СПИСОК ВИКОРИСТОВАННОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

ОСНОВНА ЛІТЕРАТУРА

1. Ахрамович В.М. Комп'ютерні мережі: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2010. – 352 с.
2. Буров Є.В. Комп'ютерні мережі: підручник. – Львів: «Магнолія 2006», 2010. – 262 с.
3. Компьютерные сети. 4-е изд. / Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.: ил. – (Серия «Классика Computer Science»).
4. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. [4-е изд.] / В. Г. Олифер, Н. А. Олифер – СПб.: Питер, 2010. – 944 с.
5. TCP/IP. Для професионалов. 3-е изд. / Т. Паркер, К. Сиян. – СПб.: Питер, 2004. – 959 с.

ДОДАТКОВА ЛІТЕРАТУРА

6. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с.
7. Ахрамович В.М., Чегренець В.М. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець. – К.: ДУТ, 2017. – 396с.
8. Mandriva Linux. Полное руководство пользователя. – СПб.:БХВ-Петербург, 2006. – 544 с.: ил.
9. Microsoft Windows XP. Руководство администратора / под общ. ред. А.Н.Чекмарева. – СПб.: БХВ-Петербург, 2006. – 848 с.: ил.
10. UNIX: руководство системного администратора. Для профессионалов. 3-е изд. / Э.Немеет, Г.Снайдер, С.Сибасс, Т.Хейн – СПб.: Питер; К.: Издательская группа BHV, 2006. – 925 с.: ил.
11. Администрирование сети на примерах. Поляк-Брагинский А. В. – СПб.: БХВ-Петербург, 2005. – 320 с.: ил.
12. Аппаратные средства локальных сетей. Энциклопедия / М. Гук, – СПб.: Питер, 2004. – 573 с.: ил.
13. Архитектура компьютерных систем и сетей: Учеб. пособие / Т.П. Барановская, В.И. Лойко и др.; под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 256 с.: ил.
14. Болілий В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник. – Кіровоград: ЦОП Авангард, 2008. – 146с.
15. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. – СПб.: Питер, 2006. – 703 с.
16. Виртуальные машины: несколько компьютеров в одном (+CD). / А.К. Гультяев – СПб.: Питер. 2006. – 224 с.: ил.
17. Вычислительные системы, сети и телекоммуникации: Учебник. – 2-е изд., перераб. и доп. / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко; Под ред. А. П. Пятибратова – М.: Финансы и статистика, 2004. – 512с.: ил.
18. Знакомство с Microsoft Windows Server 2003 / Пер. с англ. / Дж. Ханикат – М.: ИЗдательско-торговый дом "Русская редакция", 2003. – 464 с.: ил.
19. Кириленко А. Самоучитель HTML. – СПб.: БХВ-Петербург, 2005. – 272 с.
20. Клейменов С.А. Администрирование в информационных системах: учеб. Пособие для студ. Высш. Учеб. Заведений / С.А. Клейменов, В.П. Мельников, А.М. Петраков; под ред. В.П. Мельникова – М.: Издательский центр «Академия», 2008. – 272 с.
21. Компьютерные коммуникации. Учебный курс. Иванов В. – СПб.: Питер 2002. – 224 с.: ил.
22. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд. / М. В. Кульгин. СПб.: Питер, 2003. 462 с.: ил.
23. Кулаков Ю.О. Комп'ютерні мережі: навч. посіб. / Ю.О. Кулаков, І.А. Жуков. – К.: вид-во Нац.авіц.ун-ту «НАУ-друк», 2009. – 392 с.

24. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. – К.: Видавництво „Юніор”, 2005. – 400с.
25. Макин Дж. К., Десаи Анил. Развертывание и настройка Windows Server 2008. Учебный курс Microsoft / Пер. с англ. – М.: Издательство «Русская Редакция», 2008. – 640 стр. :ил.
26. Основы локальных сетей: курс лекций: учеб. пособие: для студентов вузов, обучающихся по специальностям в обл. информ. технологий. / Ю.В.Новиков, С.В.Кондратенко – М.: Интернет – Ун-т Информ. Технологий, 2005. – 360 с. – (Серия «Основы информационных технологий» / Интернет Ун-т информ. технологий).
27. Поляк – Брагинский А.В. Администрирование сетей на примерах. 2-е изд., перераб. И доп. – СПб.: БХВ- Петербург, 2008 – 432с.:ил.
28. Рональд Бодчер. Программа сетевой академии Cisco CCNA [3-е изд.]: [пер. с англ.] / Рональд Бодчер, К. Р. Киркендаль. – М.: изд. Дом “Вильямс”, 2005. – 1186 с.
29. Рональд Бодчер. Программа сетевой академии Cisco CCNA 3 и 4. [3-е изд.]: [пер. с англ.] / Рональд Бодчер, К. Р. Киркендаль. – М.: изд. Дом “Вильямс”, 2007. – 944 с.
30. Системное администрирование на 100% (+CD). Бормотов С.В. – СПб.: Питер, 2006. – 256 с.: ил.
31. Тонкая настройка Windows XP. Холмогоров В. – СПб.: Питер , 2006. – 288 с.: ил.
32. Управление и поддержка Microsoft Windows Server 2003. MCSA/MCSE / Пер. с англ. / Холме Дэн, Томас Орин – М.: Издательско-торговый дом "Русская редакция", 2004. – 448 стр.: ил.
33. Якобсен Й. Концепция разработки Web-сайтов. Как успешно разработать Web-сайт с применением мультимедиа-технологий / Йенс Якобсен; пер. с нем. И.А. Марков. – М.: НТ Пресс, 2006. – 512 с.

Надруковано у РВЦ Державного університету телекомунікацій
Формат 60х90/8. Папір друкарський.
Наклад 100 прим. Зам. 794.

Свідоцтво суб’єкта видавничої справи ДК №6185 від 17.05.2018 р.

03110, м. Київ, вул. Солом’янська, 7.
Тел. (044) 249-25-76