МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

Методичні вказівки
до виконання лабораторних робіт
для студентів за спеціальністю 125 "Кібербезпека"

Київ 2023

УДК 681.32(075)
І74

Укладачі: О.А. Курченко, канд. техн. наук, доцент;
Ю.І. Хлапонін, д-р техн. наук, професор

Рецензент О.В. Сєлюков, д-р техн. наук, професор

Відповідальний за випуск Ю.І. Хлапонін, д-р техн. наук, професор

Затверджено на засіданні кафедри кафедри кібербезпеки та комп'ютерної інженерії, протокол № 8 від 12 квітня 2023 р.

В авторській редакції.

Інформаційно-комунікаційні системи: методичні вказівки / І74 уклад.: Курченко О.А., Хлапонін Ю.І. – Київ: КНУБА, 2023. – 84 с.

Містять зміст, порядок оформлення і вказівки до виконання лабораторних робіт.

Призначені для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека».

ЗМІСТ

ВСТУП

Мета викладання дисципліни полягає в формуванні у студентів теоретичних знань в області організації і застосування сучасних технологій і засобів інформаційно-комунікаційних систем і мереж, практичних навичок використання програмних і технічних засобів інформаційних мереж і комунікаційних технологій.

Основні завдання курсу:

- вивчення базових теоретичних принципів побудови інфокомунікаційних мереж;
- формування систематичних знань в області мереж і систем телекомунікацій;
- вивчення основних технологій мереж;
- вироблення навичок і умінь проектування і експлуатації інформаційно-комунікаційних мереж.

Результати навчання:

- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

Лабораторна робота 1. Мережеві утиліти і їх використання. Утиліти ipconfig, ping, tracert, сервіс Whois

Мета роботи: визначення налаштувань для підключення до локальної мережі і до мережі Internet з використанням утиліти ipconfig. Дослідження ймовірносно-часових характеристик фрагментів мережі Internet з використанням утиліти ping. Дослідження топології фрагментів мережі Internet з використанням утиліти tracert.

Теоретичні відомості

Адресація в IP-мережах, типи адрес

Кожен комп'ютер в мережі TCP / IP має адреси трьох рівнів:

1. Локальна адреса сайту, яка визначається технологією, за допомогою якої побудована окрема мережа, в яку входить даний вузол. Для вузлів, що входять в локальні мережі, це MAC-адреса мережного адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними.

2. IP-адреса, що складається з 4 байт, наприклад, 109.26.17.100. Ця адреса використовується на мережному рівні. Він призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі і номера вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Network Information Center, NIC), якщо мережа повинна працювати як складова частина Internet.

Зазвичай провайдери послуг Internet отримують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами.

3. Символьний ідентифікатор (так званий також DNS-ім'ям) - ім'я, наприклад, SERV1.IBM.COM. Ця електронна адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домену, використовується на прикладному рівні, наприклад, в протоколах FTP або telnet.

Три основних класи IP-адрес

IP-адреса має довжину 4 байти і записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі, і між якими ставлять крапку - 128.10.2.30 - традиційна десяткова форма представлення адреси, 10000000 00001010 00000010 00011110 - двійкова форма представлення адреси.

Адреса складається з двох логічних частин - номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших бітів адреси:

якщо адреса починається з 0, то мережу відносять до класу A, і номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла в мережі (мережі класу A мають номери в діапазоні від 1 до 126. У мережах класу A кількість вузлів повинно бути більше 216, але не перевищувати 224);

якщо перші два біти адреси рівні 10, то мережа відноситься до класу B і є мережею середніх розмірів з числом вузлів 28 - 216 (в мережах класу B під адресу мережі і під адресу вузла відводиться по 16 біт - 2 байта);

якщо адреса починається з послідовності 110 - мережа класу C з числом вузлів не більше 28 (адреса мережі - 24 біта, а під адресу вузла - 8 біт);

якщо адреса починається з послідовності 1110, то він є адресою класу D і позначає особливий, груповий адрес - multicast (якщо в пакеті як адреса призначення вказана адреса класу D, то такий пакет повинні отримати всі вузли, яким визначено цю адресу);

якщо адреса починається з послідовності 11110, то це адреса класу E, вона зарезервована для майбутніх застосувань.

Відображення символьних адрес на IP-адресі: служба DNS

DNS (Domain Name System) - це розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Internet. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним іменем вузла.

Протокол DNS є службовим протоколом прикладного рівня. Цей протокол несиметричний - в ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери зберігають частину розподіленої бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративним доменам мережі Internet. Клієнти сервера DNS знають IP-адресу сервера DNS свого адміністративного домену і за протоколом IP передають запит, в якому повідомляють відоме символьне ім'я і просять повернути відповідний йому IP-адрес.

Якщо дані про запрошення відповідно зберігаються в базі даного DNS-сервера, то він посилає відповідь клієнту, якщо немає - то він надсилає запит DNS-сервера іншого домену, який може сам обробити запит,

або передати його іншому DNS-серверу. Всі DNS-сервери з'єднані ієрархічно, відповідно до ієрархії доменів мережі Internet. Клієнт опитує ці сервери імен, поки не знайде потрібні відображення. Цей процес прискорюється через те, що сервери імен постійно кешують (записують у внутрішню пам'ять) інформацію, надану за запитами.

База даних DNS має структуру дерева, званого доменним простором імен, в якому кожен домен (вузол дерева) має ім'я і може містити піддомени. Корінь бази даних DNS управляється центром Internet Network Information Center.

Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі:

- .com - комерційні організації (наприклад, microsoft.com);
- .edu - освітні (наприклад, mit.edu);
- .gov - урядові організації (наприклад, nsf.gov);
- .org - некомерційні організації (наприклад, fidonet.org);
- .net - організації, що підтримують мережі (наприклад, nsf.net).

Кожен домен DNS адмініструється окремою організацією, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Кожен домен має унікальне ім'я, а кожен з піддоменів має унікальне ім'я усередині свого домену. Ім'я домена може містити до 63 символів. Кожен вузол в мережі Internet однозначно визначається своїм повним доменним ім'ям (fully qualified domain name, FQDN), яке включає імена всіх доменів у напрямку від цього вузла до кореня. Наприклад - server.aics.acs.cctpu.edu.ru.

Далі в описі команд використовується:

- <текст> - текст в кутових дужках - обов'язковий параметр;
- [текст] - текст в квадратних дужках - необов'язковий параметр;
- (текст) - текст у круглих дужках - вибрати один з параметрів;
- вертикальна риса «|» - роздільник для взаємовиключних параметрів - потрібно вибрати один з них;
- три крапки «...» - можливе повторення зазначених параметрів.

Утиліта ipconfig

Утиліта ipconfig (IP configuration) призначена для настройки протоколу IP для операційної системи Windows (рис. 1). Для отримання цієї інформації запустіть інтерпретатор команд cmd.exe «Пуск» → «Знайти програми та файли» → cmd і в командному рядку введіть: ipconfig (ви-

користовуючи команди cd / і cls можна перейти в кореневий каталог і очистити екран, відповідно, для зручності роботи).

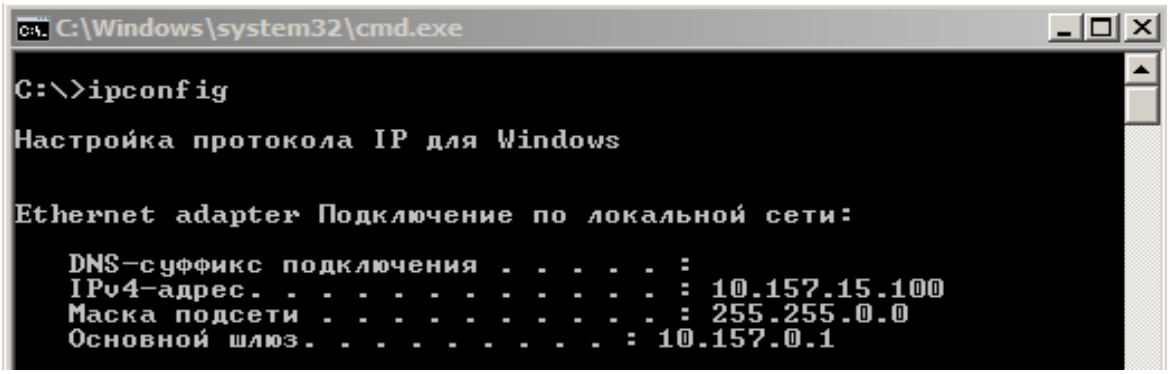


Рис. 1. Налаштування протоколу IP для операційної системи Windows

Утиліта ping

Утиліта ping (Packet Internet Groper) є одним з головних засобів, що використовуються для налагодження мереж, і служить для примусового виклику відповіді конкретного вузла (відправляє пакети на вказану адресу і аналізує параметри пакетів, які повернулися). Вона дозволяє перевіряти роботу програм TCP / IP на віддалених машинах, адреси пристроїв в локальній мережі, адреса і маршрут для віддаленого мережевого пристрою. У виконанні команди ping беруть участь система маршрутизації, схеми дозволу адрес і мережеві шлюзи. У Windows утиліта ping є в комплекті поставки і являє собою програму, що запускається з командного рядка (рис. 2).

Зверніть увагу: деякі сервери з метою безпеки можуть не посилати ехо-відповіді (наприклад, www.microsoft.com).

Формат команди: ping [-t] [- a] [- n] [- l] [- f] [- i TTL] [- v TOS]
[-R] [] [ім'я машини] [[- j список вузлів] | [-k список вузлів]] [- w]

Параметри утиліти ping

Ключі	Функції
-t	Відправка пакетів на вказаний вузол до команди переривання
-a	Визначення імені вузла за IP-адресою
-n	Кількість відправлених запитів

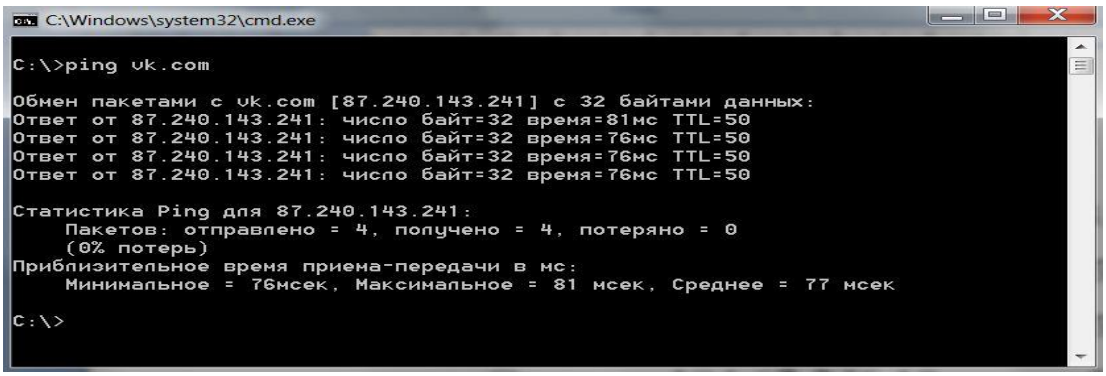


Рис. 2. Утиліта ping - програма, яка запускається з командного рядка

На практиці більшість опцій в форматі команди можна опустити, тоді в командному рядку може бути: ping ім'я вузла (для зациклення виведення інформації про з'єднання використовується опція -t; для виведення інформації n-раз використовується опція -n кількість разів). За замовчуванням передається чотири запити по 32 байта в кожному, після чого виводяться статистичні дані за отриманими пакетам.

Утиліта tracert

Утиліта tracert дозволяє виявляти послідовність маршрутизаторів, через які проходить IP-пакет на шляху до пункту свого призначення і час затримки на кожному з них.

Формат команди: tracert ім’я_машини (ім’я_машини - може бути ім'ям вузла, DNS або IP-адресою комп'ютера). Вихідна інформація являє собою список машин, починаючи з першого шлюзу і закінчуючи пунктом призначення. Пакети надсилаються по три на кожен вузол (рис. 3).

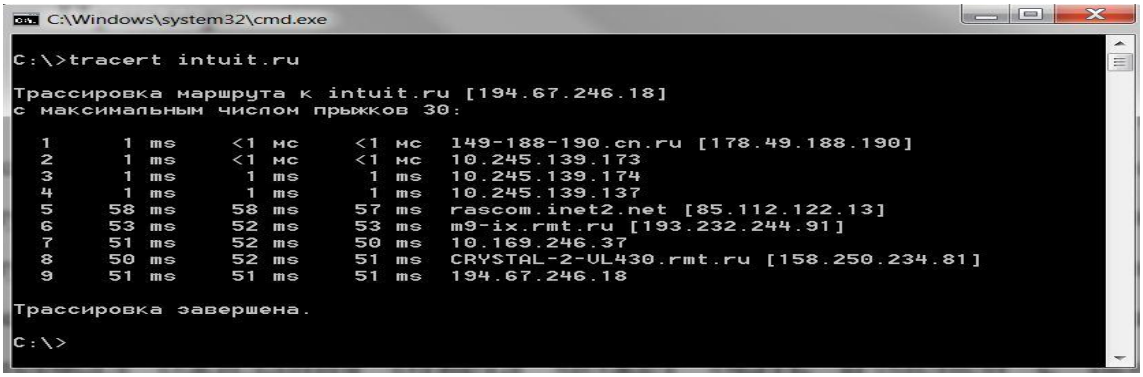


Рис. 3. Утиліта tracert

Для кожного пакету на екрані відображається величина інтервалу часу між відправленням пакета і отриманням відповіді. Символ «*» означає, що відповідь на даний пакет не була отримана. Якщо вузол не відповідає, то при перевищенні інтервалу очікування відповіді видається

повідомлення «Перевищено інтервал очікування для запиту». Інтервал очікування відповіді може бути змінений за допомогою опції «-w» команди tracert.

Сервіс Whois

При реєстрації доменних імен другого рівня обов'язковою умовою є надання вірних відомостей про власника цього домену: для юридичних осіб - назва організації, для фізичних осіб - ПІБ і паспортні дані. Також обов'язковим є надання контактної інформації. Частина цієї інформації стає вільно доступною для будь-якого користувача мережі Інтернет через сервіс Whois (англ. Who is - «хто такий?»). Основне його призначення - отримання реєстраційних даних про власників доменних імен і IP-адрес. Отримати необхідну інформацію про власника домену можна через Whois-клієнт ОС Windows, але найпростіше відправити запит можна через веб-форму on-line сервісу Whois, наприклад - gov.ua/whois.

Завдання на лабораторну роботу

Оформіть звіт по роботі, опишіть виконання вправ.

Вправа 1. За допомогою утиліти ipconfig визначити IP адрес ПК.

Вправа 2. За допомогою утиліти ping перевірити стан зв'язку з двома будь-якими працездатними вузлами.

Результат відобразити для кожного з досліджуваних вузлів у вигляді таблиці:

а. IP адреса вузла;

в. відсоток втрачених пакетів;

с. середній час прийому-передачі.

Вправа 3. Провести трасування двох працездатних вузлів. Результати відобразити в таблиці.

№ вузла	Час проходження пакету №1	Час проходження пакету №2	Час проходження пакету №3	Середній час проходження	IP-адрес маршрутизатору

Визначити ділянку мережі, яка характеризується найбільшою затримкою при пересиланні пакетів. Для знайдених маршрутизаторів за допомогою сервісу Whois визначити назву організації, контактні дані (тел., E-mail) і ін. (Виконати на різних сервісах Whois). Отриману інформацію вказати в звіті.

Лабораторна робота 2. Мережеві утиліти і їх використання. Утиліти arp, netstat, hostname, nbtstat, nslookup

Мета роботи: Практично освоїти роботу з утилітами TCP / IP - arp, netstat, hostname, nbtstat, nslookup.

Теоретичні відомості

До складу TCP / IP входять діагностичні утиліти, призначені для перевірки конфігурації стека і тестування мережевого з'єднання.

Утиліта	Застосування
arp	Виводить для перегляду і зміни таблицю трансляції адрес, використовувану протоколом дозволу адрес ARP (Address Resolution Protocol - визначає локальну адресу за IP-адресою).
netstat	Виводить статистику і поточну інформацію по з’єднанню TCP/IP.
hostname	Виводить ім’я локального хоста. Використовується без параметрів.
nbtstat	Виводить статистику і поточну інформацію по NetBIOS. Використовується для перевірки стану поточних з'єднань.
nslookup	Здійснює перевірку записів та доменних псевдонімів хостів, доменних сервісів хостів, а також інформації операційної системи, шляхом запитів до серверів DNS.

Утиліта ARP

Основне завдання протоколу ARP - трансляція IP-адрес у відповідні локальні адреси (рис. 4). Для цього ARP-протокол використовує інформацію з ARP-таблиці (ARP-кешу).

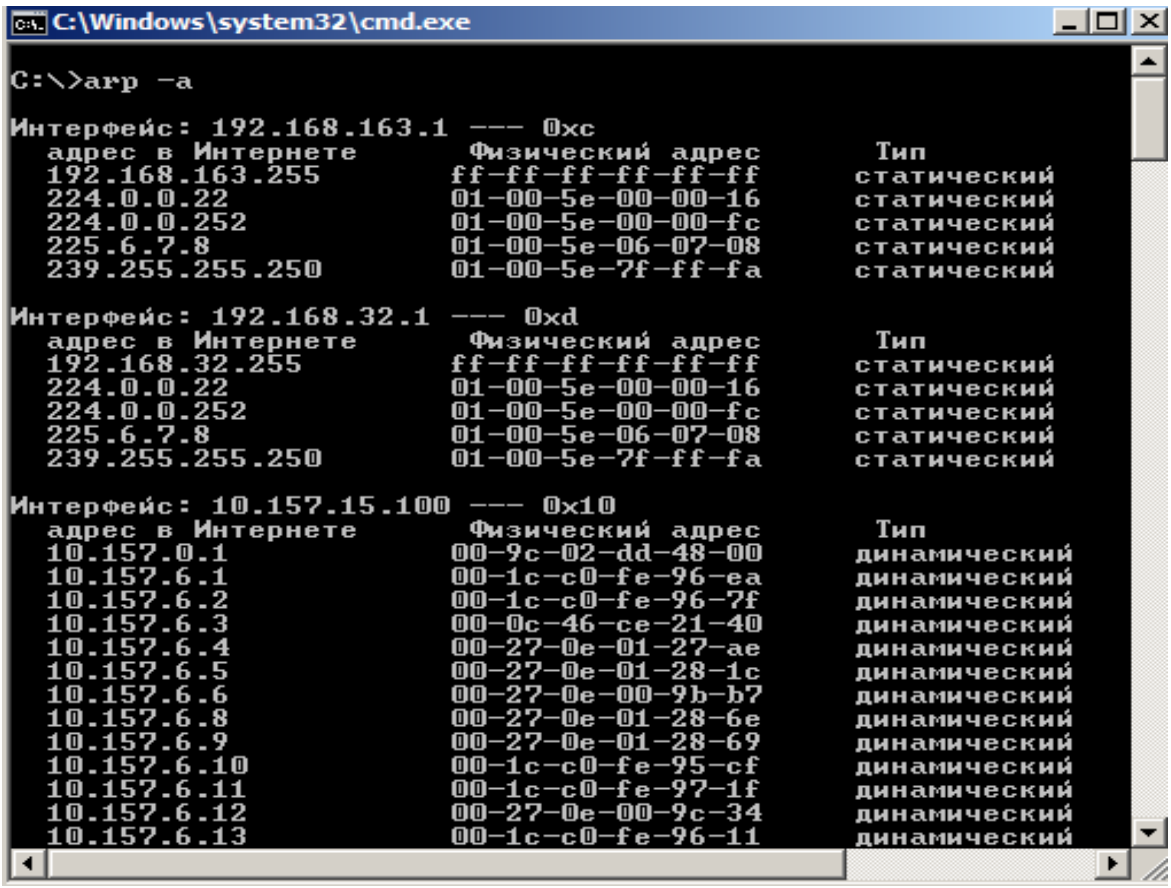


Рис. 4. Утиліта arp

Якщо необхідний запис в таблиці не знайдено, то протокол ARP відправляє широкомовний запит до всіх комп'ютерів локальної підмережі, намагаючись знайти власника даної IP-адреси.

Синтаксис: arp [-s inet_addr eth_addr] | [-D inet_addr] | [-A].

Параметри: -s занесення в кеш статичних записів;

-d видалення з кешу запису для певної IP-адреси;

-a перегляд вмісту кеша для всіх мережевих адаптерів локального комп'ютера.

Утиліта netstat

Утиліта netstat дозволяє отримати статичну інформацію по деяким з протоколів стека (TCP, UDP, IP, ICMP), а також інформує про поточні мережеві з'єднання (рис. 5). Вона корисна на брандмауерах, з її допомогою можна виявити порушення безпеки мережі.

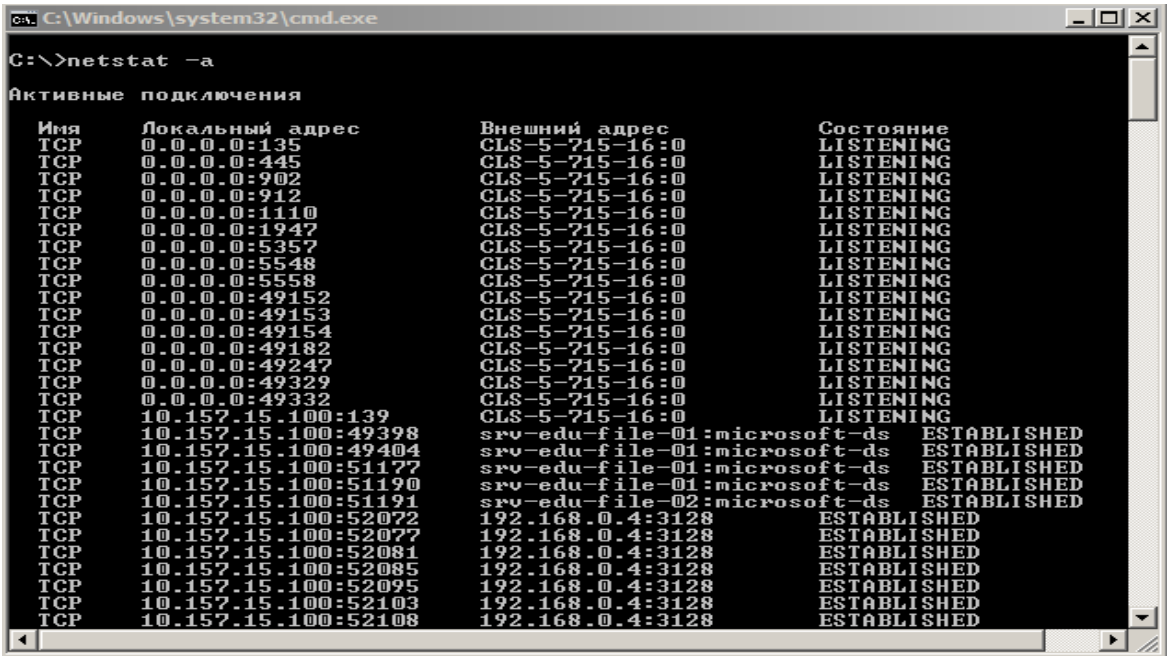


Рис. 5. Утиліта netstat

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r].

Параметри: -a виводить перелік всіх мережевих з'єднань і прослуховування портів локального комп'ютера;

-e виводить статистику для Ethernet-інтерфейсів (наприклад, кількість отриманих і відправлених байт);

-n виводить інформацію по всіх поточних з'єднаннях (наприклад, TCP) для всіх мережевих інтерфейсів локального комп'ютера;

-s виводить статистичну інформацію для протоколів UDP, TCP, ICMP, IP. Ключ «/ more» дозволяє переглянути інформацію посторінково;

-r виводить вміст таблиці маршрутизації.

Утиліта hostname

Виведіть на екран ім'я локального хоста за допомогою команди hostname. Команда hostname надає швидкий спосіб отримати ім'я вузла в конкретній локальній мережі (рис. 6).

Рис. 6. Утиліта hostname

Команда має простий синтаксис: hostname. Відразу ж після виконання команди, ім'я комп'ютера буде відображено на екрані.

Утиліта nbtstat

Утиліта nbtstat використовується для відображення інформації протоколу NetBIOS over TCP / IP (NetBT) і в основному застосовується при вирішенні проблем, що виникають при наявності в мережі ПК на основі Windows 2003 і більш старих систем (рис. 7).

Синтаксис команди nbtstat:

nbtstat [-a <ім'я комп'ютера>] [-A <адрес_IP>] [-c] [-n] [-r] [-R] [-RR] [-s] [-S].

Параметри команди nbtstat

Параметр	Застосування
-a <ім’я_комп'ютера>	Використовується для відображення таблиці імен NetBIOS зазначеного віддаленого комп'ютера.
-c	Показує таблицю кешу NetBIOS.
-n	Показує таблицю імен NetBIOS локального комп'ютера.
-s	Використовується для відображення таблиці сеансів NetBIOS.

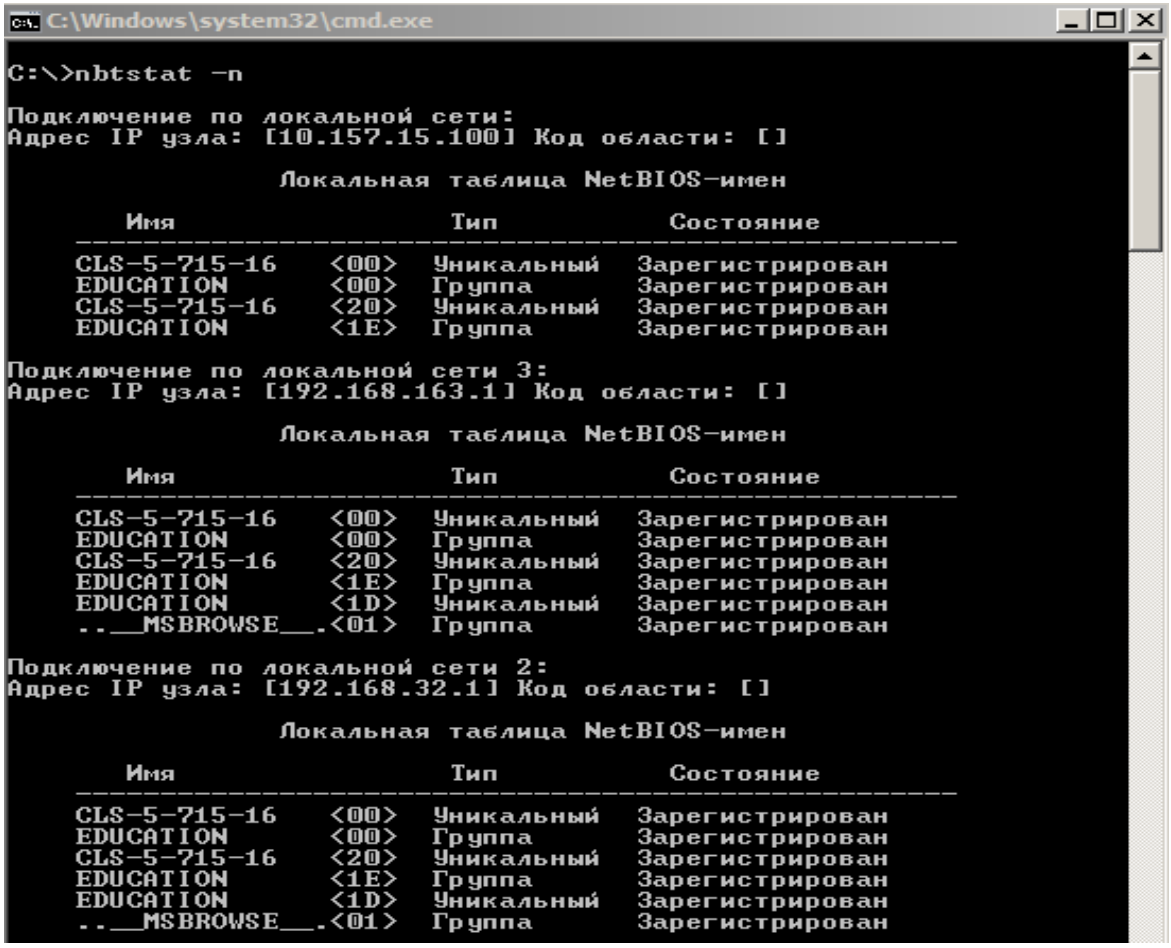


Рис. 7. Утиліта nbtstat

Утиліта nslookup

Утиліта nslookup є найефективнішою з доступних утиліт діагностики служби DNS. Утиліта nslookup дозволяє виконувати запити до серверів DNS, імітуючи послідовність дій, яка виконується клієнтським комп'ютером.

Для опитування серверів DNS цю команду можна запустити окремо. Додавши одну з підкоманд (рис. 8), можна розширити функціональність утиліти. Основна команда nslookup має наступний синтаксис:
nslookup [- <підкоманда>] [вузол] [- <сервер імен>].

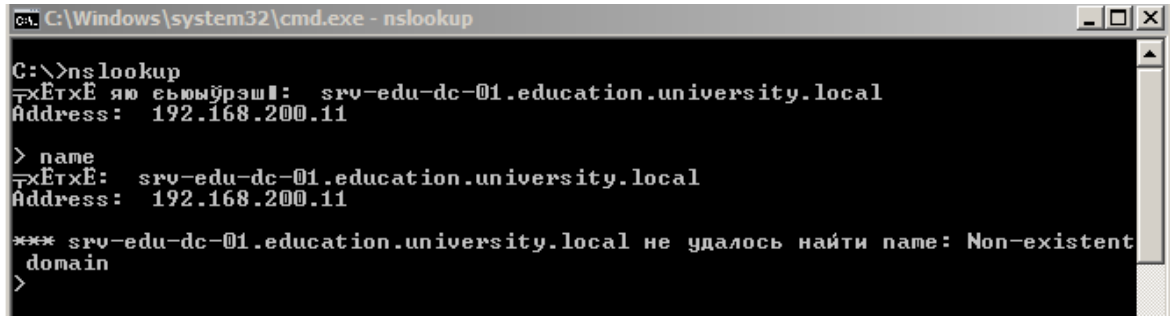


Рис. 8. Утиліта nslookup

Надавши утиліті як параметр ім'я вузла, повністю певне доменне ім'я або IP-адресу, можна перевірити здатність системи виконувати перетворення імен. Якщо служба DNS налаштована неправильно, то це можна з'ясувати за допомогою команди nslookup.

Велика частина функціональності утиліти nslookup доступна через відповідні підкоманди. Найпростішим способом отримати доступ до меню підкоманди є введення команди nslookup і натискання клавіші <Enter>. Це призведе до запуску інтерактивного режиму команди nslookup.

Завдання на лабораторну роботу

Оформіть звіт по лабораторній роботі, опишіть виконання вправ.

Вправа 1. Виведіть на екран довідкову інформацію по утилітам. Для цього в командному рядку введіть ім'я утиліти без параметрів або з /?. Вивчіть ключі, які використовуються при запуску утиліт.

Вправа 2. Виведіть на екран ім'я локального хоста за допомогою команди hostname.

Вправа 3. За допомогою утиліти arp з аргументом «a» перегляньте ARP-таблицю локального комп'ютера.

Вправа 4. За допомогою утиліти netstat виведіть перелік мережевих з'єднань і статистичну інформацію для протоколу TCP.

Приклади DNC адрес для виконання завдання: mail.ua, web.ua, auto.ria.com, gov.ua, uz.gov.ua, olx.ua, osvita.ua, otpusk.ua, prom.ua, parfums.ua,
pandora.ua, parter.ua, parimatch.ua, mazda.ua, ttt.ua, taxer.ua, taburetka.ua.

Лабораторна робота 3. Мережеві утиліти і їх використання. Утиліти getmac, netsh, net, pathping

Мета роботи: Отримати практичні навички роботи з утилітами - getmac, netsh, net, pathping.

Теоретичні відомості

Утиліта getmac

Утиліта командного рядка GETMAC присутня в версіях Windows XP і новіше (рис. 9). Використовується для отримання адрес мережевих адаптерів (MAC-адрес) як на локальному, так і на віддаленому комп'ютері.

Синтаксис: GETMAC [/ S <система> [/ U <користувач> [/ P <пароль>]]] [/ FO <формат>] [/ NH] [/ V].

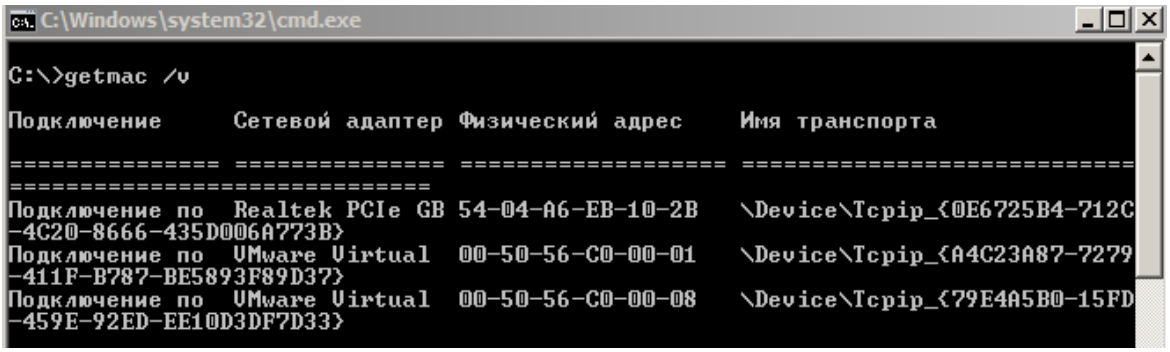


Рис. 9. Утиліта getmac

Параметри:

/ S <система> - ім'я або IP-адреса віддаленого комп'ютера;

/ U [<домен> \] <користувач> ім'я користувача;

/ FO <формат> - формат, в якому слід відображати результати запиту. Допустимі формати: "TABLE" (таблиця), "LIST" (список), "CSV" (колективний запит поля).

/ V - відображення детальної інформації. В інформації, що відображається присутнє ім'я мережевого підключення і назва мережевого адаптера;

/? - висновок довідки щодо використання команди.

Утиліта netsh

Утиліта мережевої оболонки NETSH (NETwork SHell) - найбільш повна і функціонально стандартна програма управління мережею з використанням командного рядка в Windows. При запуску netsh без параметрів на екран виводиться запрошення до введення внутрішніх команд оболонки (рис. 10).

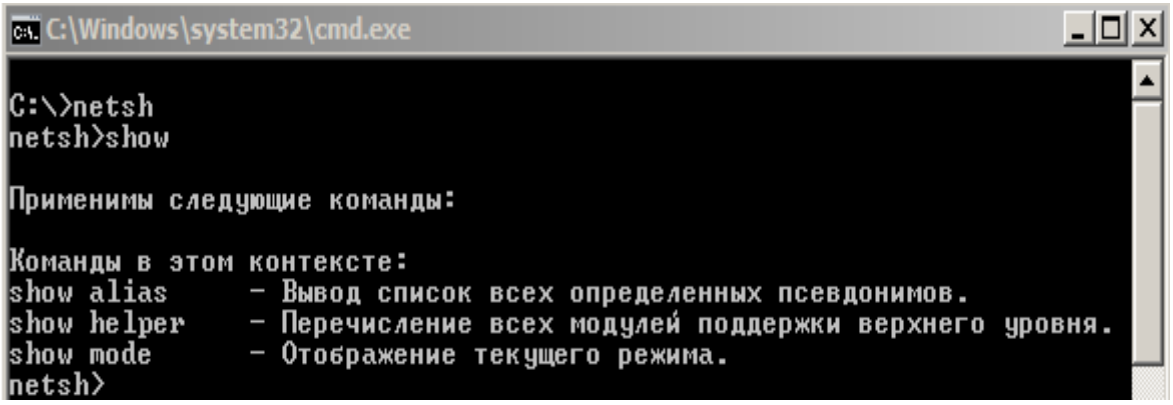


Рис. 10. Утиліта netsh

Набір команд представляє собою багаторівневу структуру, що дозволяє виконувати необхідні дії в обраному контексті. При введенні питання «/?» можна отримати довідку щодо доступного переліку команд.

Утиліта net

Утиліта NET.EXE існує у всіх версіях Windows і є однією з найбільш використовуваних в практичній роботі з мережевими ресурсами. Дозволяє підключати і відключати мережеві диски, запускати і зупиняти системні служби, додавати і видаляти користувачів, керувати ресурсами, які спільно використовуються, встановлювати системний час, відображати статистичні та довідкові дані про використання ресурсів і багато іншого.

Робота з системними службами

Згідно довідкової інформації, список служб, якими можна керувати за допомогою net.exe можна отримати, використовуючи наступну команду: net help services.

За допомогою net.exe можна запустити або зупинити системну службу, в тому числі, що не представлену в списку, який відображається при виконанні даної команди. Для зупинки використовується параметр stop, а для запуску - параметр start:

net stop dnscache - зупинити службу dnscache;

net start dnscache - запустити службу dnscache.

Повне ім'я служби можна скопіювати з «Панелі управління» - «Адміністрування» - «Служби» - «Ім'я служби» - «Властивості» - «Ім'я».

Робота з мережевими дисками

Net use - відображає список мережевих дисків, підключених на комп'ютері (рис. 11). У колонці «Локальний» відображається буква мережевого диска, а в колонці «Віддалений» - ім'я віддаленого мережевого ресурсу в форматі UNC.

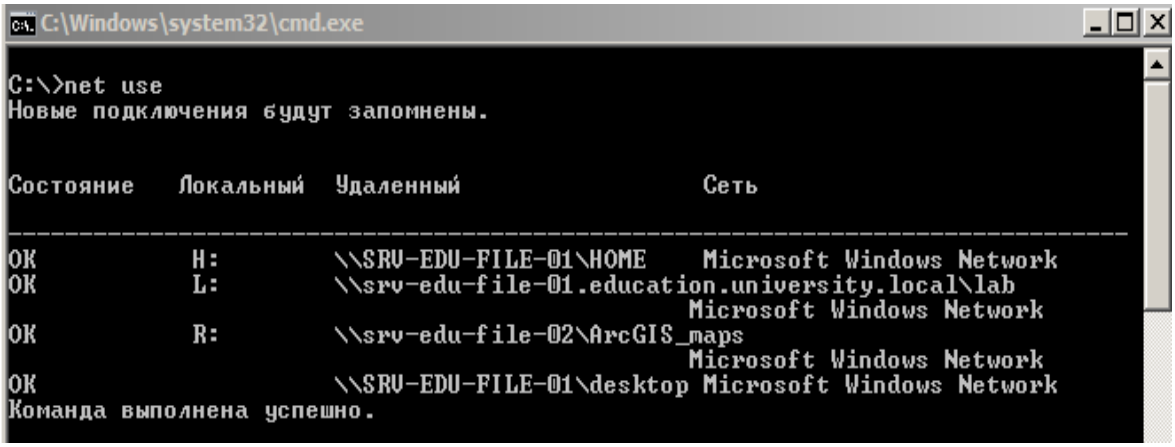


Рис. 11. Утиліта net

Для відключення мережного диска або пристрою використовується команда net use з ключем / DELETE:

net use X: / delete - відключити мережевий диск X:

Регістр букв в цьому ключі не має значення, крім того можна використовувати скорочення: net use Y: / del.

Робота з файлами і каталогами

NET SHARE - ця команда дозволяє виділити ресурси системи для мережевого доступу. При запуску без інших параметрів, виводить інформацію про всі ресурси даного комп'ютера, які можуть бути спільно використані. Для кожного ресурсу виводиться ім'я пристрою або шлях і відповідний коментар net share - отримати список поділюваних в локальній мережі ресурсів даного комп'ютера (рис. 12).

Для видалення існуючого ресурсу, використовується параметр / DELETE: net share TEMP / DELETE - видалити розділяється ресурс під ім'ям TEMP.

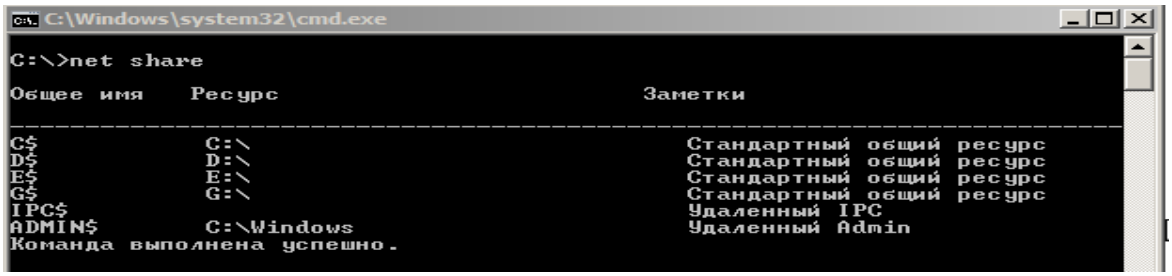


Рис. 12. Утиліта net с параметром share

Робота з користувачами і комп'ютерами

Утиліта NET дозволяє відобразити дані про облікові записи користувачів і груп, додавати нові записи, видаляти існуючі, відображати параметри безпеки, пов'язані з авторизацією користувачів і деякі інші операції по адмініструванню на локальному комп'ютері або контролері домену.

Net user - відобразити список користувачів net user / DOMAIN - відобразити список користувачів поточного домену.

Статистика та синхронізація годин

Утиліта NET.EXE дозволяє отримати статистичні дані по використанню служб сервера і робочої станції:

net statistics server - відобразити статистичні дані для сервера;

net statistics workstation - відобразити статистичні дані для робочої станції. Для зміни системного часу комп'ютера використовується команда NET TIME (рис. 13).

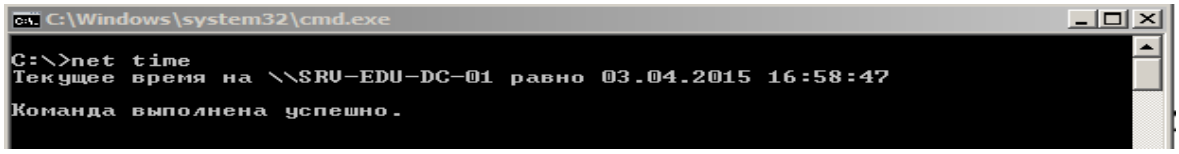


Рис. 13. Утиліта net с параметром time

Вона синхронізує годинник комп'ютера з іншим комп'ютером або доменом. Якщо використовується без параметрів в домені, то виводить поточну дату і час встановлені на сервері для даного домена.

Утиліта pathping

Команда PATHPING виконує трасування маршруту до кінцевого вузла аналогічно команді TRACERT, але додатково, виконує відправку запитів на проміжні вузли маршруту для збору інформації про затримки і втрати пакетів на кожному з них (рис. 14).

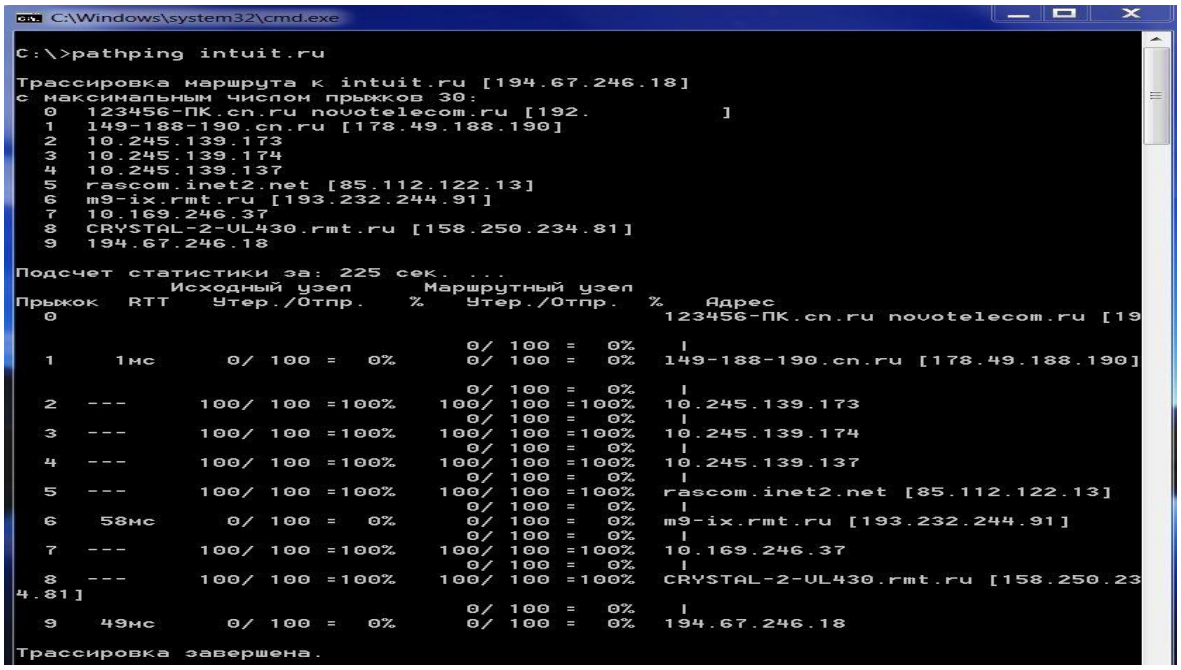


Рис. 14. Утиліта pathping

Практично, PATHPING, запущена на виконання з параметрами за замовчуванням, виконує ті ж дії, що і команда TRACERT плюс команди

PING для кожного проміжного вузла із зазначенням числа луна-запитів, рівним 100 (ping -n 100...).

При інтерпретації результатів виконання pathping потрібно враховувати, що деякі маршрутизатори можуть бути налаштовані на блокування icmp-трафіку, що не дозволяє правильно відпрацювати трасування, і отримати статистичні дані.

Завдання на лабораторну роботу

Оформіть звіт по лабораторній роботі, опишіть виконання вправ.

Вправа 1. Виведіть на екран довідкову інформацію по утилітам. У командному рядку введіть ім'я утиліти без параметрів або з / ?.

Вправа 2. Використовуючи утиліту Getmac з аргументом «v» визначте детальну інформацію про підключення, мережеві адаптери, фізичні адреси і імена транспорту.

Вправа 3. Використовуючи утиліту Netsh з аргументом «dump» перегляньте сценарії конфігурації ipV4.

Вправа 4. Використовуючи утиліту Net з аргументом «use» можна звернутися до списку підключених до ПК дисків, список користувачів ПК. Використовуючи утиліту Net з аргументом «share» перегляньте інформацію про ресурси даного ПК, які спільно використовуються.

Вправа 5. Використовуючи утиліту Pathping виконати трасування 2 сайтів і вказати затримки і втрати на всіх вузлах.

Приклади DNC адрес для виконання завдання: mail.ua, web.ua, auto.ria.com, gov.ua, uz.gov.ua, olx.ua, osvita.ua, otpusk.ua, prom.ua, parfums.ua,
pandora.ua, parter.ua, parimatch.ua, mazda.ua, ttt.ua, taxer.ua, taburetka.ua.

Лабораторна робота 4. Призначення пакетів і їх структура, адресація пакетів.

Теоретичні відомості

Інформація в локальних мережах пересилається короткими частинами, які називають пакетами (packets), кадрами (frames) або блоками, причому максимальний розмір цих пакетів обмежений.

Призначення локальної мережі - це забезпечення якісного зв'язку всім абонентам мережі. Одним з основних параметрів взаємодії комп'ютерів є час доступу до мережі (access time). Воно визначається як часовий інтервал між моментом готовності абонента до передачі даних і моментом початку цієї передачі, тобто цей час очікування абонентом початку своєї передачі. Час доступу не повинен бути великим, інакше величина інтегральної швидкості передачі даних значно зменшиться навіть при високошвидкісному зв'язку.

Очікування початку передачі пов'язано з тим, що в мережі не може здійснюватись кілька передач одночасно (при топологиях шина і кільце). В іншому випадку інформація від різних передавачів змішується і спотворюється. У зв'язку з цим абоненти передають свою інформацію по черзі. Кожному абоненту, перш ніж почати передачу, треба дочекатися своєї черги, час очікування і є час доступу.

Якби вся інформація передавалася будь-яким абонентом відразу вся, безперервно, без поділу на пакети, то це призвело б до захоплення мережі цим абонентом на тривалий час. Всі інші абоненти змушені були б очікувати завершення передачі всієї інформації, на що могло б знадобитися десятки секунд і хвилин. Для того щоб зрівняти в правах всіх абонентів, а також зробити приблизно однаковими для всіх величину часу доступу до мережі використовують пакети (кадри) обмеженої довжини.

Крім того, при передачі великих масивів інформації досить висока ймовірність помилки через завади і збої. Наприклад, при характерною для локальних мереж величиною ймовірності одиночної помилки в 10-8 пакет довжиною 10 Кбіт буде спотворений з ймовірністю 10-4, а масив довжиною 10 Мбіт - вже з ймовірністю 10-1. При виявленні помилки доведеться повторити передачу всього цього масиву. Однак, при повторній передачі великого масиву ймовірність помилки також висока, і процес

цей при занадто великому масиві може повторюватися до нескінченності.

З іншого боку, порівняно великі пакети мають переваги перед занадто маленькими пакетами, наприклад, перед побайтовій (8 біт) або послівній (16 біт або 32 біт) передачею даних.

Це пов'язано з тим, що кожен пакет крім даних, які потрібно передати, містить певну кількість службової інформації. Якщо порція переданих даних буде дуже маленькою (кілька байт), то частка службової інформації стане високою, що знизить загальну швидкість обміну інформацією по мережі.

Існує оптимальна довжина пакету, при якій середня швидкість обміну інформацією по мережі буде максимальна. Вона не є постійною величиною - залежить від рівня завад, методу управління обміном, кількості абонентів, характеру переданої інформації, і від інших особливостей мережі.

Процес інформаційного обміну в мережі є низкою пакетів, кожен з яких містить інформацію, яка передається від абонента до абонента.

Розміри пакета і його структура в кожному конкретному випадку визначаються стандартом на дану мережу і пов'язані з апаратними особливостями даної мережі, обраної топологією і типом середовища передачі інформації. Існують загальні принципи формування структури пакета (рис. 15).

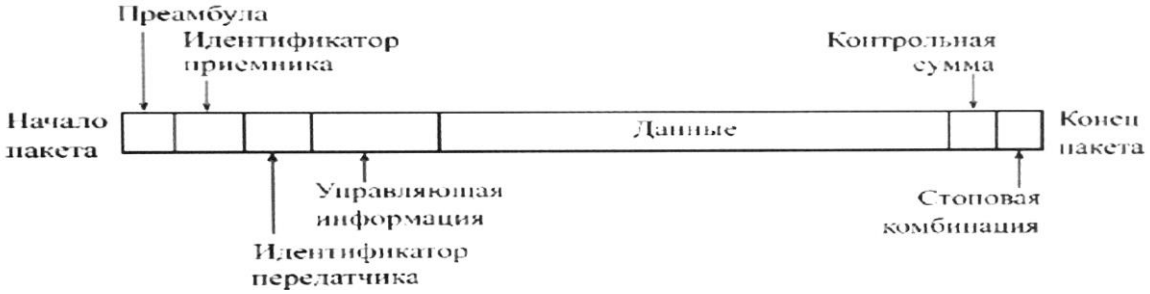


Рис. 15. Структура пакету

Стартова комбінація бітів (преамбула) яка забезпечує початкову настройку апаратури адаптера на прийом і обробку пакета.

Мережевий адрес (ідентифікатор) абонента, який приймає, індивідуальний номер, присвоєний кожному приймаючому абоненту в мережі. Ця електронна адреса дозволяє приймачу розпізнати адресований йому пакет.

Мережевий адрес (ідентифікатор) абонента, який передає, індивідуальний номер, присвоєний кожному абоненту, який передає.

Службова інформація, яка вказує на тип пакета, його номер, розмір, формат, маршрут доставки і т.д.

Дані (поле даних) - це та інформація, для передачі якої використовується пакет. На відміну від всіх інших полів пакету це поле має змінну довжину, яка визначає повну довжину пакета. Існують спеціальні керуючі пакети, які не мають поля даних.

Контрольна сума пакета - це числовий код, що формується передавачем за певними правилами. Приймач, повторюючи обчислення, зроблені передавачем, з прийнятим пакетом, порівнює їх результат з контрольною сумою і робить висновок про безпомилковість передачі пакета. Якщо пакет помилковий, то приймач запитує його повторну передачу.

Стопова комбінація служить для інформування обладнання абонента, який приймає, про закінчення пакета.

У процесі сеансу обміну інформацією по мережі між передавачем і абонентами, які приймають, відбувається обмін пакетами по встановленим правилам - протоколом обміну. Приклад протоколу показаний на рис. 16.

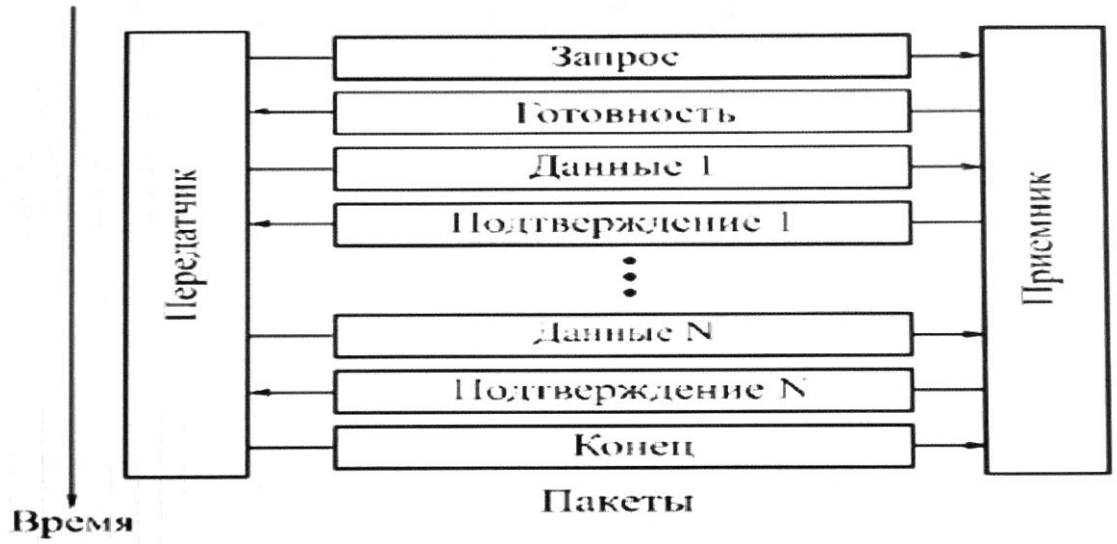


Рис. 16. Приклад обміну пакетами при сеансі зв'язку

Сеанс обміну даними починається з запиту передавачем готовності приймача прийняти дані. Для цього використовується керуючий пакет «Запит». Якщо приймач не готовий, він відмовляється від сеансу спеціальним керуючим пакетом. У разі, коли приймач готовий до мережної взаємодії, він посилає у відповідь керуючий пакет «Готовність». Потім починається обмін даними. При цьому на кожен отриманий пакет з даними приймач відповідає керуючим пакетом - «Підтвердження». Якщо пакет даних переданий з помилками, у відповідь на нього приймач запи-

тує повторну передачу. Закінчується сеанс керуючим пакетом «Кінець», яким передавач повідомляє про розрив зв'язку. Існує безліч стандартних протоколів, які використовують як передачу з підтвердженням (з гарантованою доставкою пакета), так і передачу без підтвердження (без гарантії доставки пакета). При реальному обміні по мережі застосовуються багаторівневі протоколи, кожен з рівнів яких передбачає свою структуру пакета (адресацію, керуючу інформацію, формат даних і т.д.). Протоколи високих рівнів мають справу з такими поняттями, як файл-сервер або додаток, що запитує дані у іншої програми, і цілком можуть не «знати» ні про тип апаратури мережі, ні про метод управління обміном в ній. Пакети більш високих рівнів послідовно вкладаються в переданий пакет (рис. 17). Такий процес послідовної упаковки даних для передачі називається інкапсуляцією пакетів.

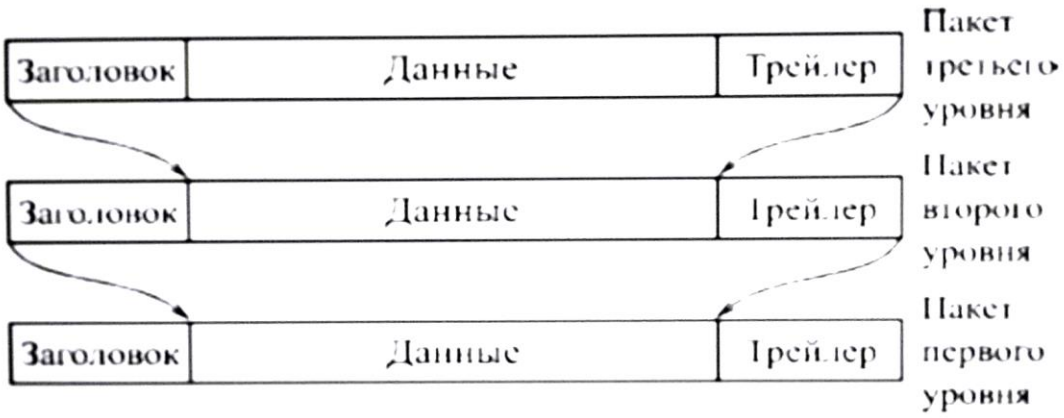


Рис. 17. Багаторівнева система вкладення пакетів

Частка допоміжної інформації в пакетах при цьому зростає з кожним наступним рівнем, що знижує ефективну швидкість передачі даних. Для збільшення цієї швидкості бажано, щоб протоколи обміну були простіше, а кількість рівнів цих протоколів було б мінімальним. Процес зворотного послідовного розпакування даних приймачем називається декапсуляцією пакетів.

Адресація пакетів

Кожному абоненту (вузлу) локальної мережі необхідно мати свою унікальну адресу (ідентифікатор або MAC-адресу), для того щоб йому можна було відправляти пакети. Існують дві основні системи присвоєння адрес абонентам мережі (мережевих адаптерів цих абонентів).

Одна з них зводиться до того, що при установці мережі кожному абоненту користувач надає індивідуальний адрес в інтервалі від 0 до 254. Присвоєння адрес проводиться програмно або за допомогою пере-

микачів на платі мережевих адаптерів. Контроль унікальності мережевих адрес всіх абонентів в цьому випадку покладається на адміністратора.

Інший підхід до адресації був розроблений міжнародною організацією IEEE, що займається питаннями стандартизацією мереж. Ідея полягає в тому, щоб привласнювати унікальну мережеву адресу кожному адаптеру мережі ще на етапі його виготовлення. Був обраний 48-бітний формат адреси, що відповідає приблизно 280 трильйонів різних адрес. Ймовірно, така кількість мережевих адаптерів ніколи не буде випущено. Запропоновано наступна структура MAC-адреси, представлена на рис. 18:

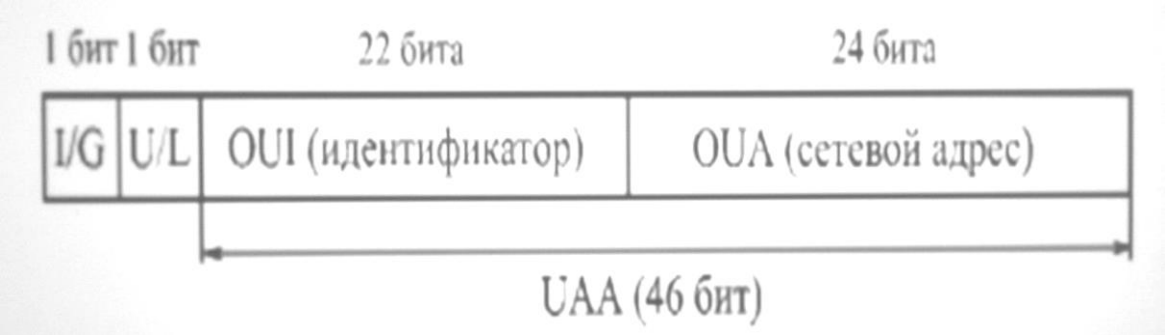


Рис. 18. Структура 48-бітного стандартного MAC-адресу

Молодші 24 розряди коду адреси - OUA (Organizationally Unique Address) - організаційно унікальна адреса. Їх привласнює кожен із зареєстрованих виробників мережевих адаптерів. Всього можливо близько 16 мільйонів комбінацій, тобто кожен виробник може випустити 16 мільйонів мережевих адаптерів.

Наступні 22 розряди коду - OUI (Organizationally Unique Identifier) - організаційно унікальний ідентифікатор. IEEE привласнює один або кілька OUI кожному виробнику мережевих адаптерів. Такий підхід дозволяє виключити збіг адрес адаптерів від різних виробників. Всього можливо понад 4 мільйонів різних OUI, тобто теоретично може бути зареєстровано 4 мільйони виробників. Разом OUA і OUI називаються UAA (Universally Administered Address) - універсально керований адрес або IEEE-адрес.

Два старших розряди адреси - керуючі, вони визначають тип адреси і спосіб інтерпретації інших 46 розрядів. Старший біт I / G (Individual / Group) вказує на тип адреси. Якщо він встановлений в 0, то індивідуальний, якщо в 1, то груповий (багатопунктовий або функціональний). Пакети з груповою адресою отримають всі, хто має цей груповий адрес,

мережеві адаптери. Інший керівник біт U / L (Universal / Local) іменується прапорцем універсального / місцевого управління. Він визначає, як було присвоєно адресу даного адаптера змінного струму. Найчастіше він встановлений в 0. Установка біта U / L в 1 означає, що ця адреса задається не виробником мережевого адаптера, а організацією, яка використовує дану мережу.

Щоб дозволити усім абонентам мережі одночасно (широкомовна передача) використовувати спеціально виділену мережеву адресу, всі 48 бітів встановлені в одиницю. Його приймають всі абоненти мережі незалежно від значень їх індивідуальних і групових адрес.

Завдання на лабораторну роботу

Повторити теоретичний матеріал за темою лабораторного заняття.

Підготувати короткі доповіді на тему:

1. Завдання аналізу мережевого трафіку.
2. Програмні засоби для аналізу мережевого трафіку.
3. Налаштування аналізатора пакетів.
4. Збір інформації про мережну активність.
5. Аналіз заголовків захоплених пакетів.

Надати відповіді на тестові завдання.

1. Розташуйте основні поля пакета в порядку їх прямування при передачі даних.

• керуюча інформація
• преамбула
• трейлер
• контрольна сума
• адреса відправника та одержувача
• дані

2. У локальних мережах використовується...

• комутація пакетів
• комутація каналів
• комутація повідомлень

3. Контрольна сума пакета використовується для…

• позначення кінця пакета
• позначення наступного в черзі пакету
• оцінки правильності передачі пакета
• фіксування факту передачі

4. Інкапсуляція пакетів - це…

• розпакування пакетів високих рівнів у пакети низьких рівнів

• упаковка пакетів низьких рівнів у пакети високих рівнів

• упаковка високих рівнів у пакети низьких рівнів

• розпакування пакетів низьких рівнів у пакети високих рівнів

5. Тип комутації, що передбачає попередню процедуру встановлення з'єднання між абонентами з ініціативи одного з них

• динамічна комутація

• постійна комутація

• статична комутація

• стохастична комутація

Підготувати відповіді на контрольні питання:

1. Навіщо потрібний аналіз мережних пакетів?

2. Якими засобами можна проаналізувати мережний трафік?

3. Як працює сніфер пакетів?

4. З яких частин складається пакет TCP/IP?

5. Яка інформація міститься в заголовку пакета TCP/IP?

Лабораторна робота 5. Мережеві сервіси.

Теоретичні відомості

Мета роботи: набуття навичок безпечного використання мережевих сервісів.

Розглянемо кілька корисних програм, які дозволять вам використовувати вашу локальну мережу з більшою ефективністю.

Звертаємо вашу увагу на те, що всі описані тут програми представлені лише в навчальних цілях. Ми вважаємо за потрібне попередити про те, що використовуючи описане програмне забезпечення для отримання несанкціонованого доступу до комп'ютерів інших користувачів вони чинять протиправні дії.

TheDude

Якщо у вашій локальній мережі досить багато комп'ютерів, цілком можливо, що вам захочеться поліпшити управління мережею за допомогою спеціального програмного забезпечення. Зокрема, існують програми, які вміють відстежувати стан комп'ютерів мережі і повідомляти про нього адміністратору. Наприклад, програма TheDude, яку ми зараз розглянемо, служить для моніторингу локальної мережі. Основна її особливість - автоматичне складання карти мережі і відстеження стану пристроїв, що входять в мережу. Програму можна завантажити на URL http://www.mikrotik.com, дистрибутив займає близько 1,4 Мб.

Вікно TheDude складається з декількох робочих областей (рис. 19).

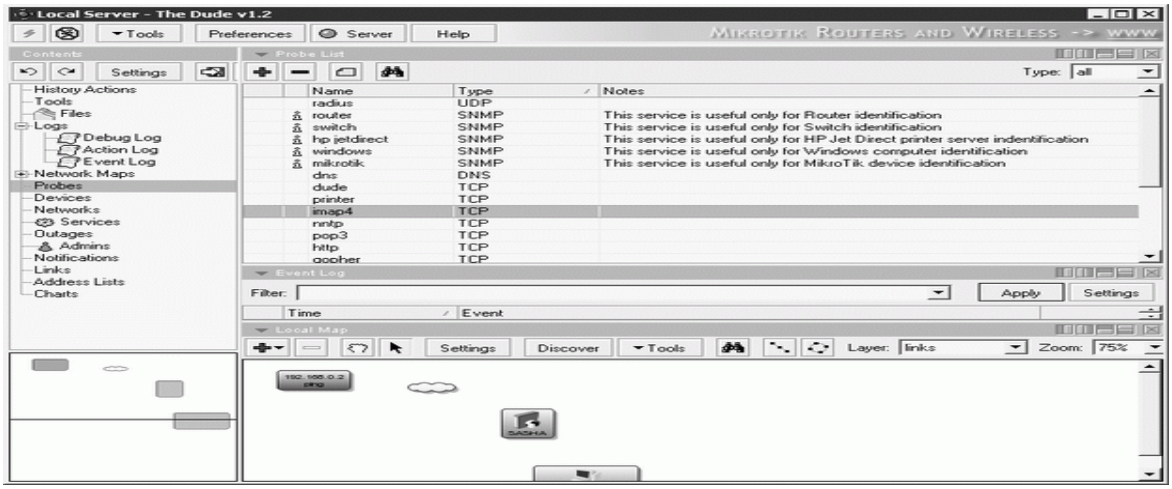


Рис. 19. Головне вікно TheDude

У верхній лівій частині вікна знаходиться вікно для переміщення по розділах програми, трохи нижче - міні-карта мережі. У правій же частині відображаються обрані розділи програми.

Наприклад, розділ NetworkMaps LocalMap виводить карту мережі. Карта будується автоматично на основі сканування діапазону адрес вашої мережі, який задається при першому запуску програми. Знайдені пристрої відображаються у вигляді квадратиків з інформацією про імена пристроїв. Програма періодично пінгує включені в карту пристрії, з'ясовуючи їх доступність. Якщо пристрій доступно - воно виділено на карті зеленим кольором, якщо немає - червоним. Користувач має можливість додавати елементи на карту вручну, експортувати карту в різні графічні формати.

Для того, щоб TheDude просканував певний діапазон IP-адрес в пошуках комп'ютерів і інших пристроїв - натисніть кнопку Discover, яку можна знайти в віконці LocalMap.

Введіть діапазон адрес, який цікавить вас і запустіть сканування (рис. 20). Так само ви можете відразу ж встановити галочки AddNetworkToAuto Scan для того, щоб програма надалі автоматично сканувала обраний діапазон адрес поряд з іншими і LayoutMapAfter Discovery Complete - для оновлення карти після завершення пошуку пристроїв.

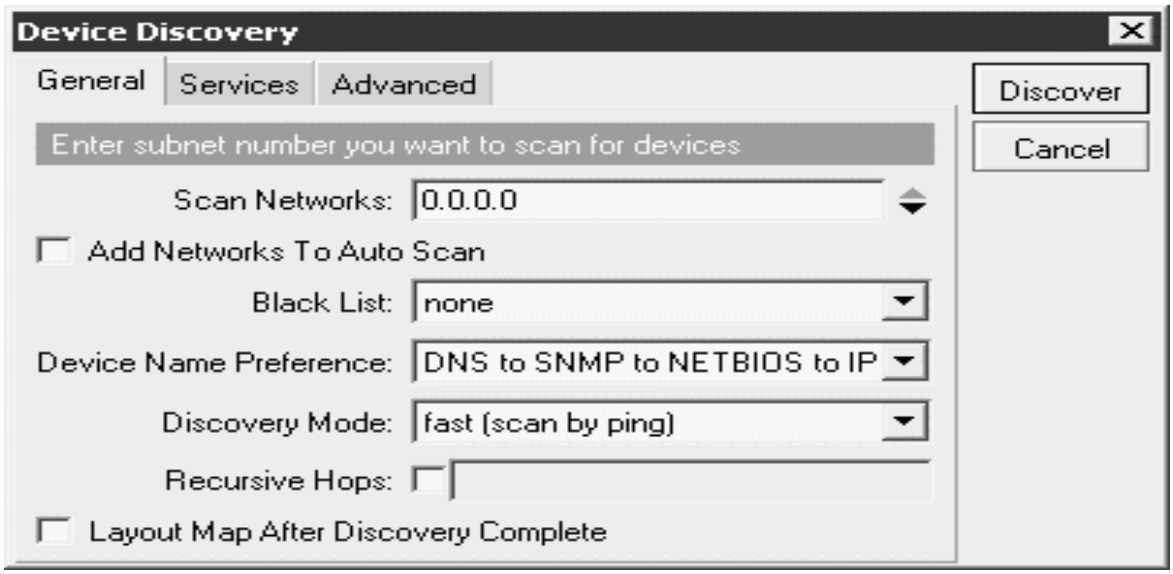


Рис. 20. Настройка пошуку нових пристоїв

Вкладка цього вікна Services служить для настройки мережевих сервісів, на які повинна реагувати програма, а Advanced містить деякі додаткові параметри сканування.

Мабуть, карта мережі - це основна і найбільш цікава можливість програми. Решта її інструментів мають меншу цінність, хоча, все одно, цікаві так як надають додаткову інформацію про мережеві пристрої, процес сканування і так далі.

Наступна програма, яку ми розглянемо, призначена для перехоплення і аналізу пакетів, які подорожують по мережі.

Packetyzer

Packetyzer - це потужна безкоштовна програма для перехоплення і аналізу мережевих пакетів. Вона підтримує більш ніж 483 протоколи, вміє працювати з провідними і бездротовими мережами, легко налаштовується.

Packetyzer можна скачати на http://www.networkchemistry.com/products/packetyzer.php

Розмір дистрибутива складає близько 11,5 Мб.

При запуску програма попросить вас вказати мережевий адаптер, який буде використовуватися для захоплення пакетів (рис. 21), тут же можна обмежити загальний розмір захоплених пакетів (LimitTotalCaptureto) і максимальну довжину одного пакета (LimiteachPacketto). Так само тут можна включити автоматичний скролінг вікна захоплення пакетів протягом роботи програми (Automaticscrollingduringcapture).

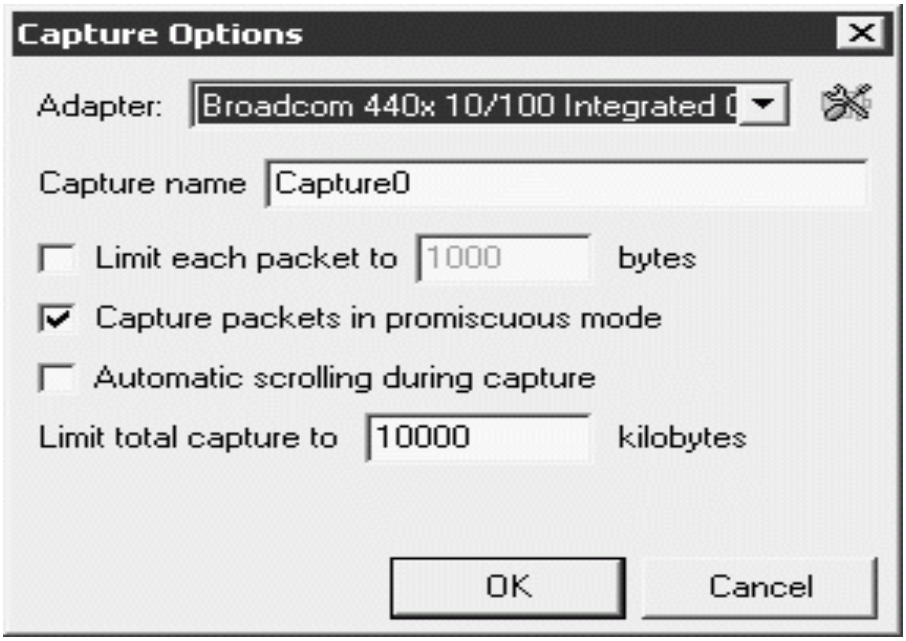


Рис. 21. Початкова настройка Packetyzer

Після цього Packetyzer може починати роботу. Для включення захоплення пакетів треба натиснути F5 або вибрати меню Session StartCapture. Відповідно, для зупинки захоплення треба також натиснути F5, або скористатися командою меню Session StopCapture.

В ході роботи програми здійснюється перехоплення пакетів, що проходять через обраний мережевий адаптер (рис. 22).

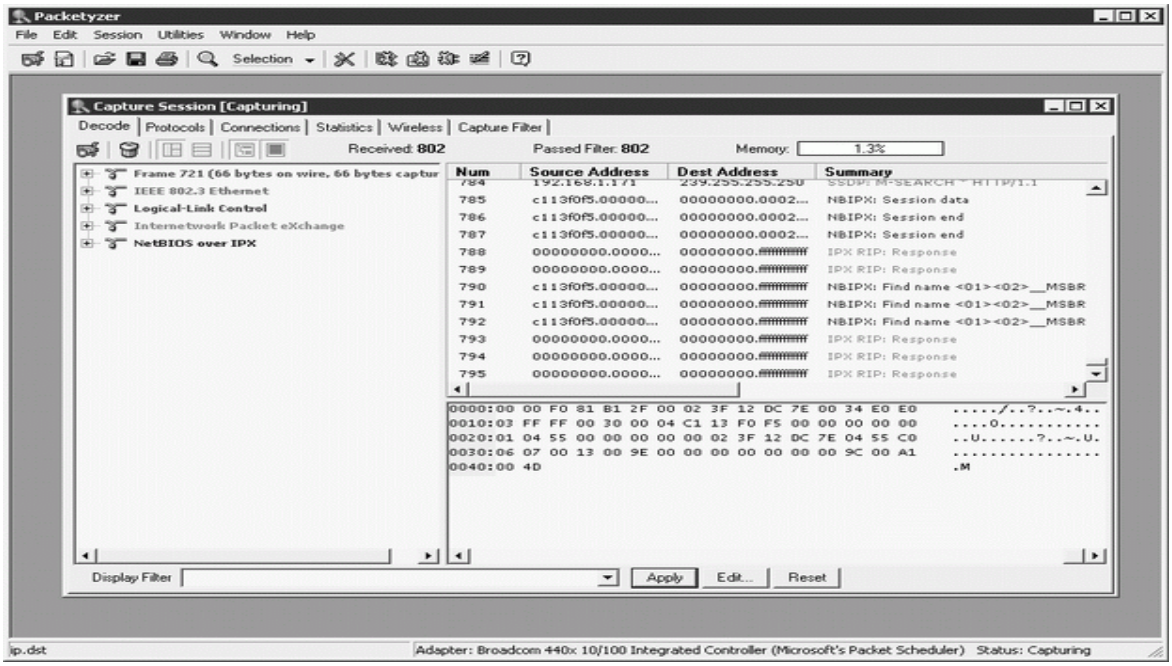


Рис. 22. Packetyzer в роботі

На вкладці Deem, у верхній правій частині вікна програми розташована область, що містить інформацію про захоплені пакети. Якщо клацнути мишею по одній з рядків цієї області, в лівій частині вікна відобразиться детальна інформація про пакет, в правій нижній частині можна бачити цей же пакет в шістнадцятковому представленні.

Ви можете редагувати пакети, використовуючи пункт меню Session PacketEditing, можете відправляти пакети, використовуючи засіб, який ховається за пунктом меню Session SendPacket (рис. 23).

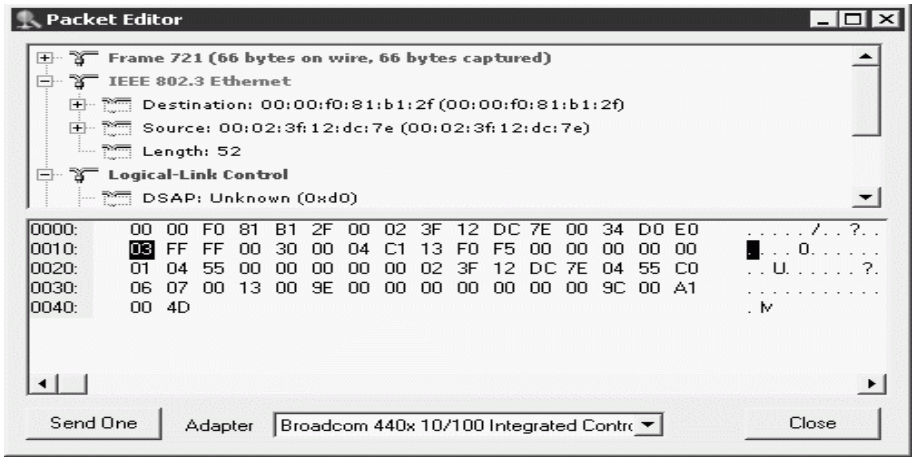


Рис. 23. Правка та відсилання пакета

Новий пакет можна створити на основі виділеного пакету. Відредагувавши виділений пакет (правка здійснюється в шістнадцятковому вигляді), ви можете натиснути на кнопку SendOne для його відправки.

Результати сканування можна зберегти в файл (File Save). Так само програма вміє працювати з файлами-результатами сканування в різних форматах.

Тепер давайте розглянемо вкладки вікна сканування.

Так, вкладка Protocols містить інформацію про тип і кількість пакетів, що відповідають тому чи іншому протоколу. Інформація виводиться в графічному вигляді з розбивкою протоколів на групи.

• Вкладка Connections містить інформацію про мережеві з'єднання.

• Вкладка Statistics - статистику роботи програми.

• Вкладка Wireless - інформацію про роботу програми з бездротовими мережами.

• Вкладка CaptureFilter містить інформацію про фільтри пакетів, відповідно до яких здійснюється захоплення.

Тепер давайте розглянемо досить просту, але ефективну програму для сканування ресурсів мережі.

LanSpy

Автори програми стверджують, що LanSpy здатний розповісти все або майже все про віддалений комп'ютер. Якщо ви спробуєте цю програму - ви зрозумієте, що це твердження дуже близько до істини. Програму можна завантажити на http://lantricks.com/lanspy/, розмір дистрибутива складає близько 1,1 Мб.

Отже, перед нами програма для сканування діапазонів IP-адрес і отримання інформації про комп'ютери, яким відповідають ті чи інші адреси. Якщо ви - адміністратор досить великої локальної мережі - ця програма допоможе вам дізнатися подробиці про комп'ютери, які підключені до вашої мережі.

Програма проста у використанні - ви запускаєте її, задаєте діапазон IP-адрес (рис. 24) в полі, розташованому у верхній частині вікна програми і натискаєте Enter або кнопку із зеленою стрілкою.

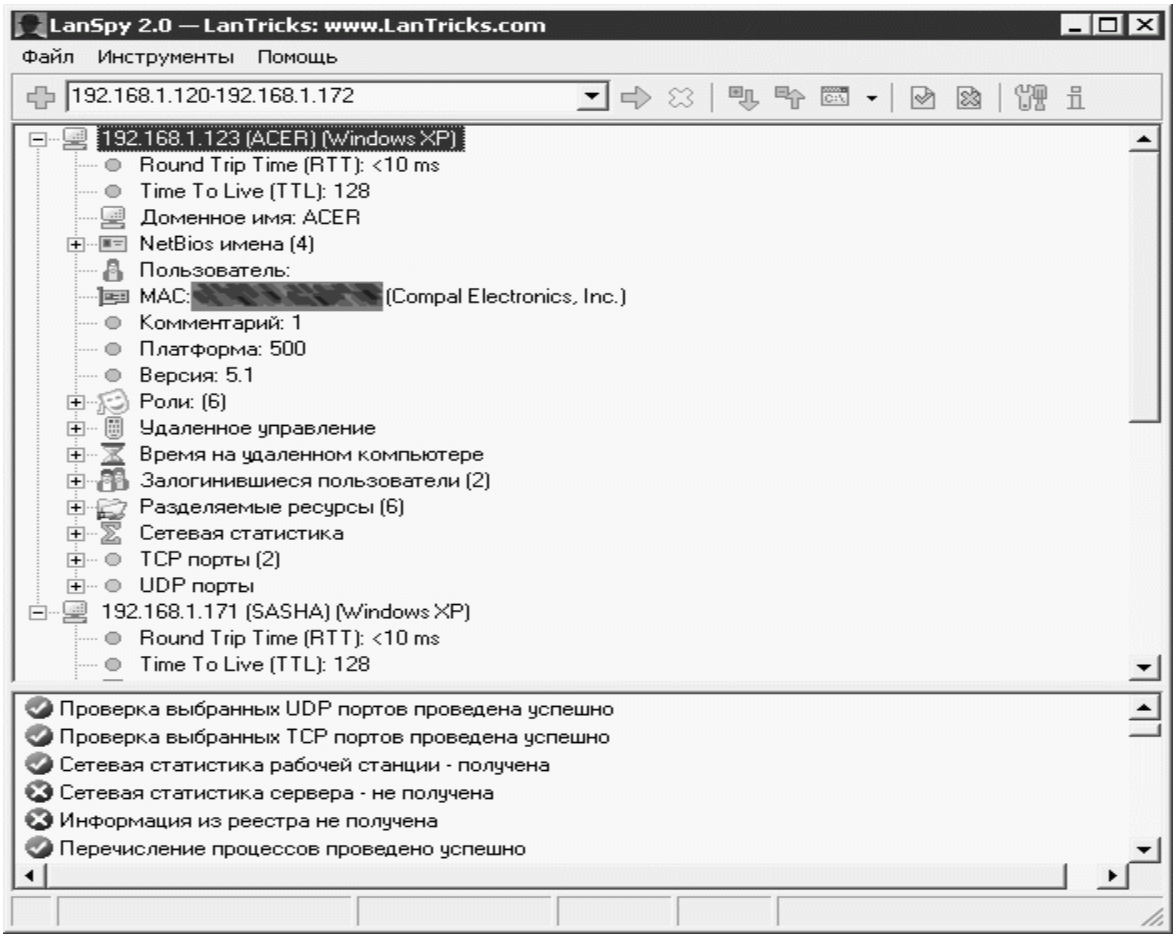


Рис. 24. Сканування мережі за допомогою LanSpy

Після цього починається сканування, хід якого відображається у віконці, розташованому в нижній частині вікна програми. А в верхній частині ви можете бачити інформацію про активні комп'ютери. Ця інформація досить обширна. Крім різних статистичних даних про роботу мережі, ми отримуємо відомості про IP-адресу, мережеве ім’я і MAC-адресу комп'ютера, далі, програма виводить список загальних ресурсів, відкритих TCP і UDP-портів і так далі.

LanSpy має настройки (Файл Налаштування), найбільш корисні з яких ми зараз розглянемо.

Так, в розділі опція Сканувати (рис. 25). ви можете зменшити таймаут при пінг для збільшення швидкості сканування, однак, пам'ятайте, що при дуже малому таймауті (це залежить від швидкості з'єднання і завантаженості мережі) система може просто не встигнути відповісти.

Встановивши галочку Ігнорувати результати пінгу ви можете підвищити ймовірність знаходження робочої системи у вашій мережі навіть в тому випадку, якщо вона не відповідає на ping-запит.

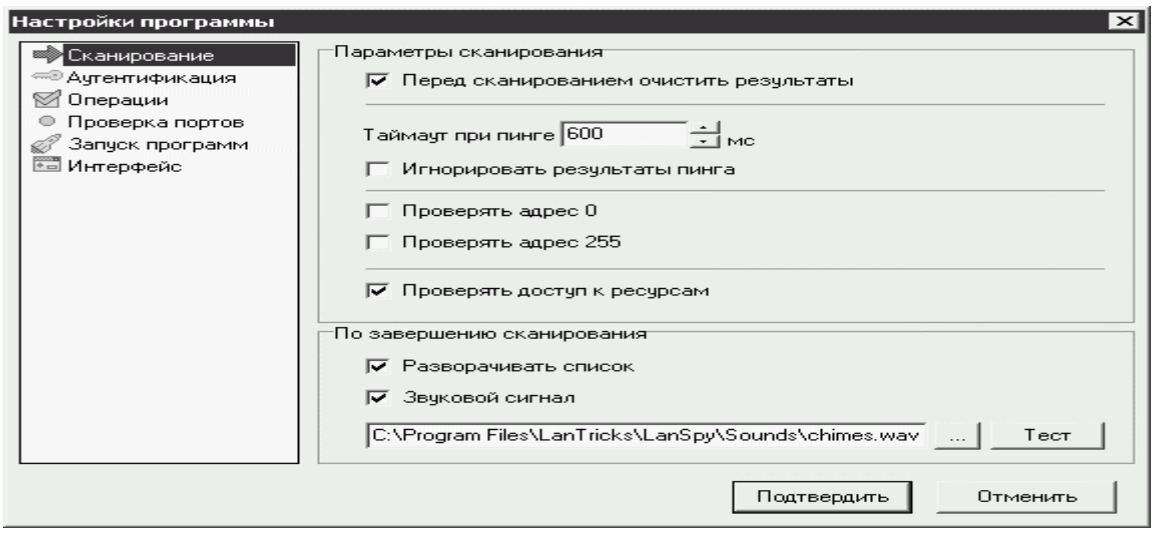


Рис. 25. Настройка параметрів сканування

На рис. 26 ви можете бачити вікно настройки параметрів сканування TCP-портів.

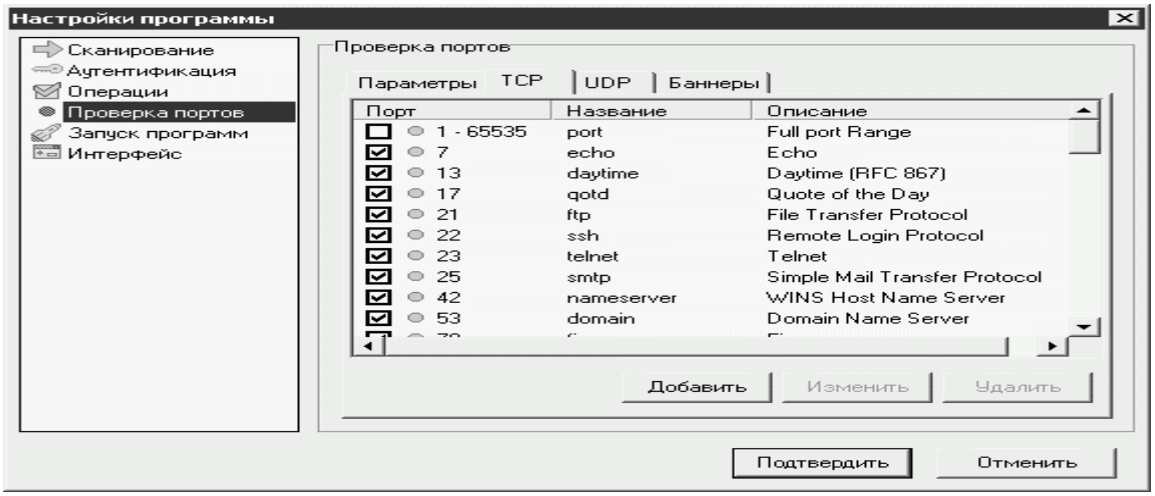


Рис. 26. Настройка параметрів сканування TCP-портів

За замовчуванням програма сканує зазвичай порти, які застосовуються, зі списку. При бажанні ви можете просканувати весь діапазон TCP-портів, встановивши галочку в поле 1-65535, або - додати порт, який вам хотілося б просканувати, вручну, натиснувши на кнопку Додати і заповнивши поля вікна, що з'явилося.

Цю можливість зручно використовувати для перевірки вашої мережі на предмет наявності троянських програм на її комп'ютерах. Для швидкої перевірки можна задати відомі порти троянців (їх можна знайти в Інтернеті за ключовими словами "порти троянських програм") і періодично сканувати машини вашої мережі на предмет наявності на них відкритих портів, які з високою часткою ймовірності належать до "троянських коней".

Аналогічні настройки є і для UDP-портів, для них також справедливо все вищесказане про шкідливі програми.

Тепер давайте розглянемо програму для роботи з ресурсами мережі.

NetShareWatcher

Колективні ресурси - наприклад - папки - це один з обов'язкових атрибутів будь-якої локальної мережі. Але крім очевидної користі загальна папка може послужити засобом для поширення в мережі шкідливих програм або, наприклад, папка з файлами тільки для читання може бути несанкціоновано перетворена в папку, файли якої можуть бути змінені, що, в результаті, може призвести до поганих наслідків для локальної мережі.

Програма, яку ми зараз розглянемо, називається NetShareWatcher. Призначена вона для моніторингу загальних ресурсів комп'ютерів, підключених до локальної мережі. Дистрибутив програми займає близько 1,5 Мб, скачати її можна з http://netsharewatcher.nsauditor.com/

На рис. 27 ви можете бачити робоче вікно програми. У лівій частині вікна програми можна побачити дві вкладки - Targets і Network. За допомогою вкладки Network ви можете переглядати вашу локальну мережу і додавати її комп'ютери і робочі групи в список "цілей" для стеження за загальними ресурсів, тобто - на вкладку Target.

Зробивши клацання правою кнопкою миші по імені комп'ютера або робочої групи у вікні Network, ви можете вибрати пункт Addtotargets (для комп'ютера) або AddDomaintotargets (для робочої групи), після чого обраний ресурс буде додано на вкладку Targets. Так само додати комп'ютер на цю вкладку можна, клацнувши значок "+", розташований над вкладками і у вікні заповнити властивості "цілі".

На цьому етапі роботи з програмою ми зупинимося докладно - саме він є ключовим у використанні програми так як вікно, аналогічне додаванню "цілі", служить для настройки стеження за загальними ресурсами комп'ютерів, вже доданих до списку Targets.

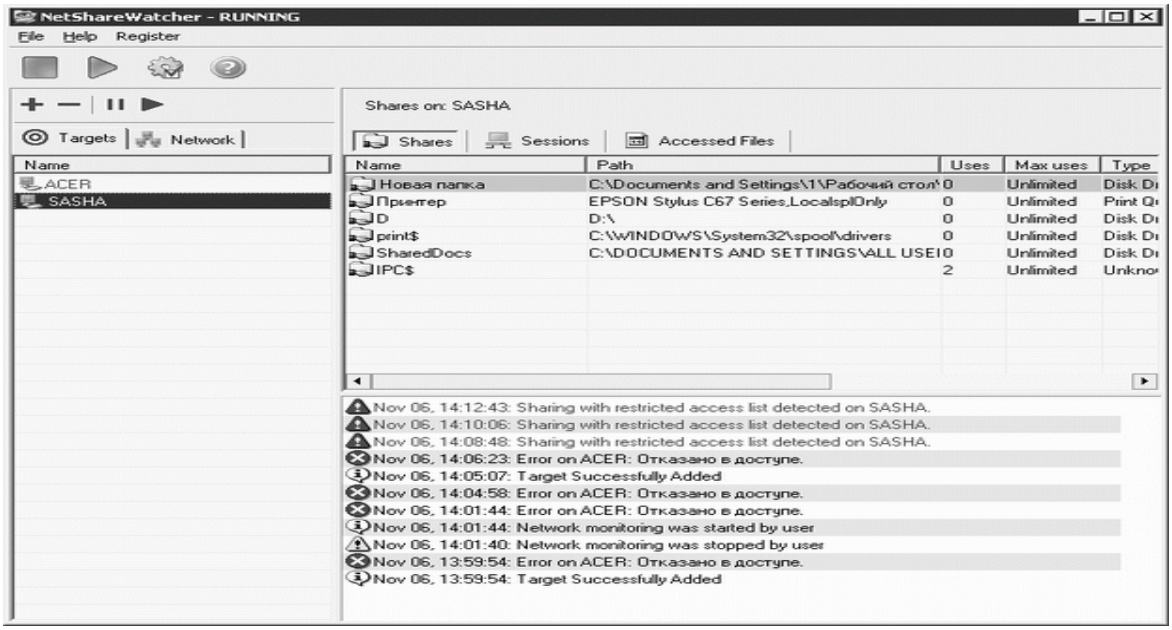


Рис. 27. Робоче вікно NetShareWatcher

Отже, перша вкладка вікна настройки параметрів "цілі" називається General (рис. 28). Вона має два ключових поля - Name - тобто ім'я комп'ютера, і IP - тобто його IP-адресу. Ввівши ім'я або адресу комп'ютера, ви можете заповнити другу автоматично, натиснувши відповідну кнопку - Getfrom IP або GetFromName - для отримання імені по IP-адресі або IP-адресі по імені комп'ютера.

При необхідності встановіть перемикач NetworkLoginInformation в позицію Custom і введіть в поле Username ім'я користувача для входу в мережу і в поле Password мережевий пароль.

Далі, на вкладці Restrictions, вам знадобиться задати групи користувачів (рис. 29), для яких потрібно призначити права доступу до загальних ресурсів. Треба відзначити, що призначати права доступу ви можете (навіть швидше повинні так як зазвичай різні загальні ресурси несуть різні функції) для кожного окремого загального ресурсу.

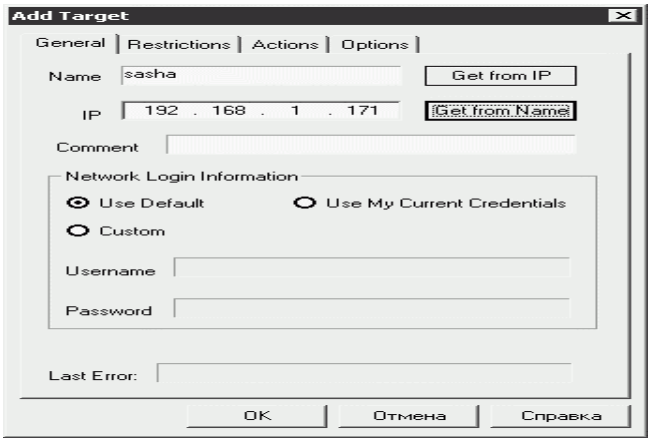


Рис. 28. Настройка загальних параметрів пристрою

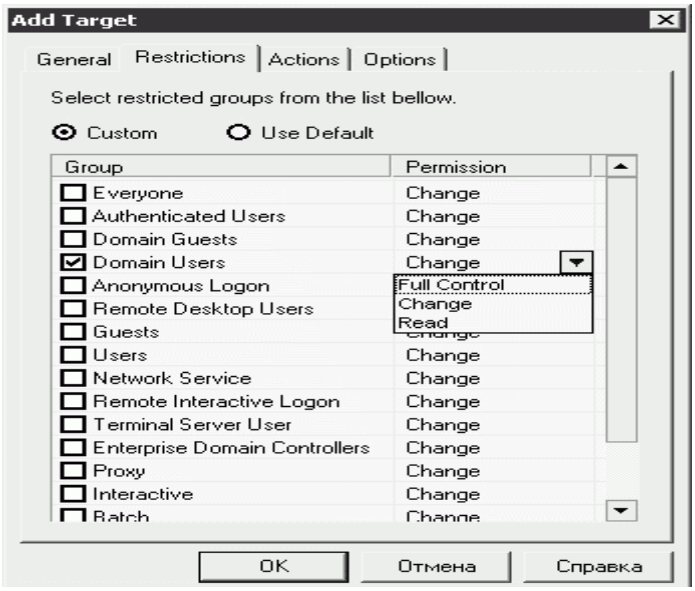


Рис. 29. Призначення дозволів групам користувачів

Далі, зверніть увагу на вкладку Actions (рис. 30).

У разі, якщо станеться якась подія, що стосується порушення прав доступу до загального ресурсу, програма може відправити повідомлення (SendMessage), заданий полем Text, на E-Mail, показати попередження в треї (ShowBaloonTip), заборонити доступ до загального ресурсу (DisableSharing). Що треба зробити (може не виконуватися для особливих адміністративних поділюваних ресурсів (їх можна задати на вкладці Options) і для черг друку) - включити або відключити цю можливість можна галочками AdministrativeShares і PrintQueue.

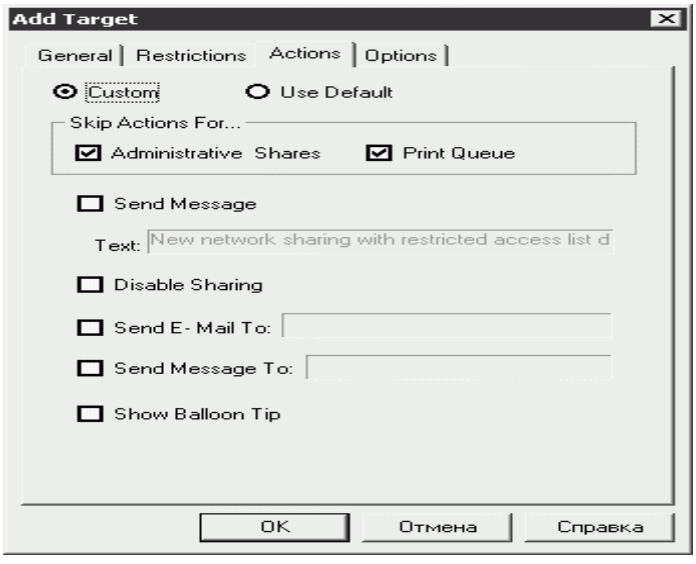


Рис. 30. Настройка реакції програми на події

Коли опції поділюваних ресурсів налаштовані, програма працює у фоновому режимі, відстежуючи події, які пов'язані з цими ресурсами. Вмикати і вимикати моніторинг ресурсів можна кнопками

StartMonitoring і StopMonitoring, розташованими у верхній частині вікна програми.

Крім усього іншого NetShareWatcher може показувати інформацію про те, хто в даний момент використовує загальні ресурси комп'ютера - для цього вам потрібно виділити Ваш комп'ютер у вікні Targets і вибрати в правій частині вікна програми вкладку AccessedFiles.

Поговоривши про моніторинг загальних ресурсів, перейдемо до ще однієї цікавої теми, а саме - для дистанційного управління комп'ютером.

AccessRemote PC

Існує чимало програм, які організовують віддалений доступ до комп'ютера. Як правило, схема такого доступу виглядає так: на керованому комп'ютері запускається серверна частина програми, на керуючому - клієнтська, після чого користувач, який сидить за комп'ютером-клієнтом може управляти машиною, де працює серверна частина. AccessRemote PC побудований саме за таким принципом. Програма дозволяє отримувати повний доступ до віддаленого комп'ютера, причому не тільки через локальну мережу, а й через Інтернет. Крім доступу у неї є деякі корисні можливості, які роблять її цікавою для цілей навчання (зокрема - в комп'ютерних класах навчальних закладів).

Отже, AccessRemote PC можна завантажити на http://www.access-remote-pc.com Розмір дистрибутива складає близько 1,8 Мб. Програма ця платна, причому, існує вона в різних версіях, з особливостями яких можна ознайомитися на її сайті. Пробна версія розрахована на 30 запусків, причому в ході випробування програми вона функціонує без будь-яких обмежень, тобто ви зможете в повній мірі випробувати її можливості.

Давайте розглянемо особливості установки і використання AccessRemote PC.

Програму треба встановити на всіх комп'ютерах, якими ви хочете керувати, так само як і на тому комп'ютері (або комп'ютерах), з якого ви хочете займатися управлінням інших машин.

В ході установки вам буде запропоновано або встановити на комп'ютері повну конфігурацію програми, або - лише клієнтську частину (рис. 31).

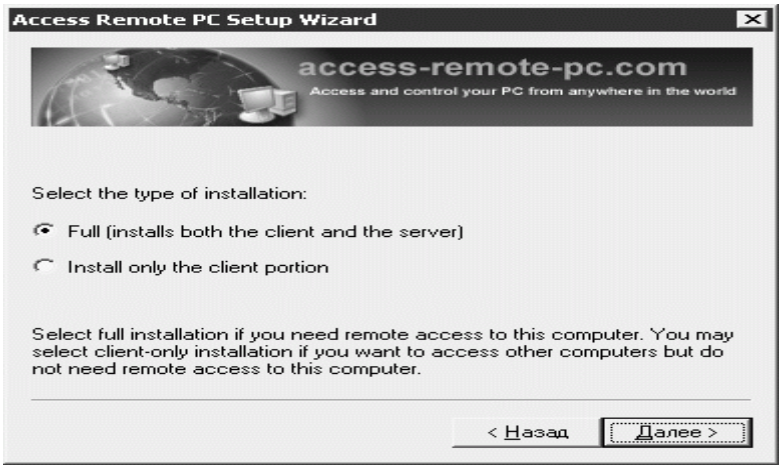


Рис. 31. Вибір обсягу програми, що встановлюється

Якщо ви хочете, щоб комп'ютером, на який встановлюється програма, можна було керувати на інших машинах - вибирайте повну версію (Full), якщо ж ви не хочете цього, тобто збираєтеся лише керувати з цього комп'ютера іншими - можете вибрати Installonlytheclientportion.

В одному з наступних вікон вам зададуть питання - чи хочете ви отримувати доступ до вашого ПК лише використовуючи його IP-адресу або ім'я мережі (I will be accessing this computer only by name or IP-address), або ж ви бажаєте скористатися сервісом RPC (I have an RPC account ...) (рис. 32).

Рис. 32. Вибір способу підключення до ПК

Якщо ви збираєтеся користуватися програмою серйозно і довго, отримувати доступ до вашого ПК через Інтернет - вам є сенс зареєструватися на сервері компанії, отримати номер RPC і користуватися ними. Ну а якщо ваші потреби обмежені локальною мережею - нічого не міняйте в цьому вікні, просто натиснувши кнопку Далі.

Тепер - ще один ключовий момент установки. Вам запропонують поставити ім'я користувача і пароль, які згодом будуть використовуватися для управління комп'ютером з інших машин (рис. 33).

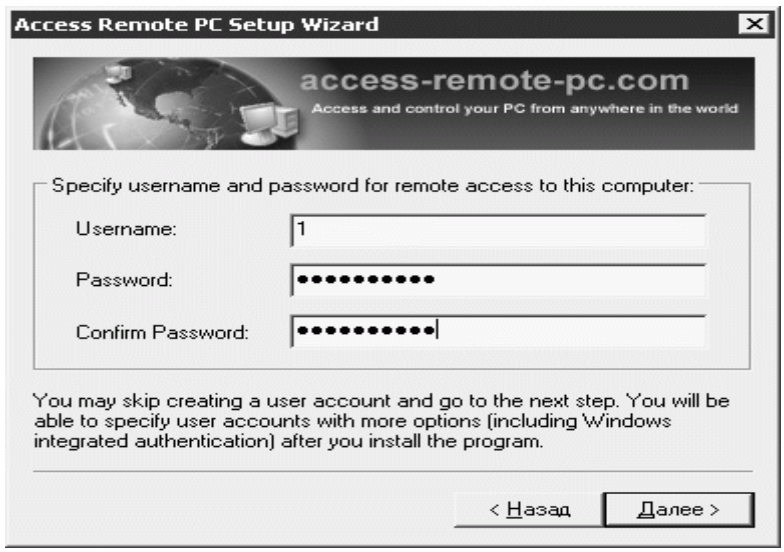


Рис. 33. Задаємо ім'я користувача і пароль для доступу до ПК

Ці параметри можна задати і пізніше, після установки програми, але ми поставимо їх відразу. Тепер установка програми на одному з комп'ютерів завершена. Точно так само встановимо її на інші машини (в цілях безпеки ви можете задавати різні паролі на різних комп'ютерах, хоча якщо ви не хочете возитися з різними іменами і паролями - можете задати один і той же для всіх комп'ютерів мережі).

Після установки значок програми з'являється в трее Windows. За замовчуванням AccessRemote PC запускається разом з системою.

Після того, як програма встановлена на всіх машинах, можна спробувати встановити з'єднання. Для цього треба запустити Remote PC Client за допомогою значка на робочому столі (рис. 34)

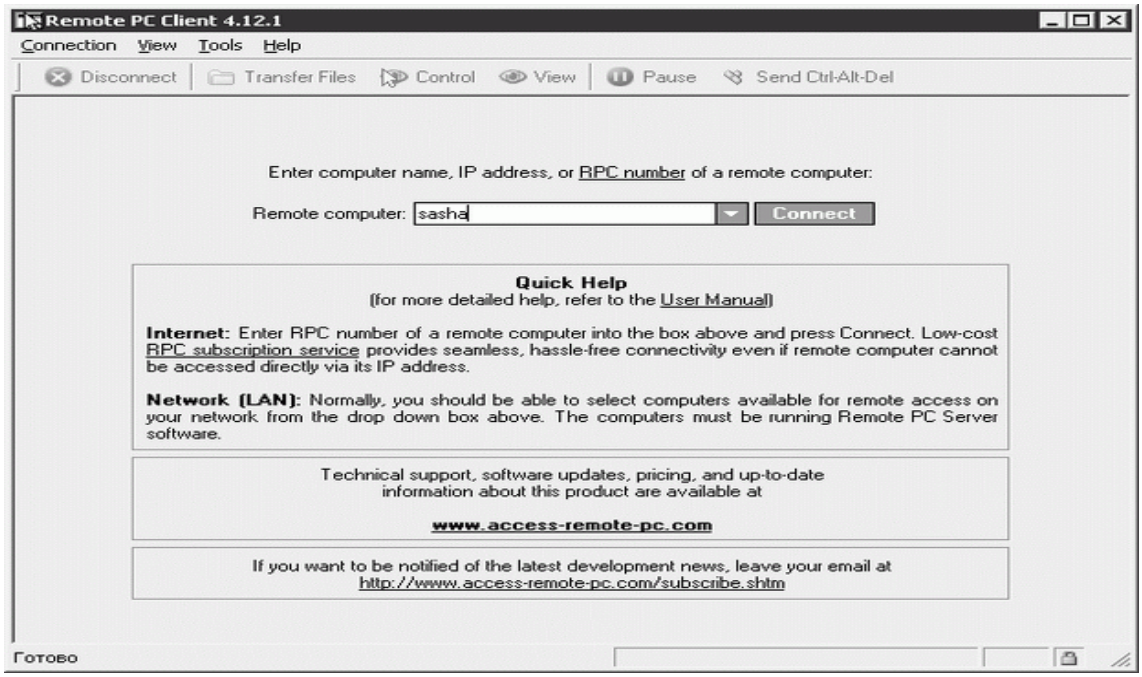


Рис. 34. Початок підключення до віддаленого комп’ютеру

У першому вікні Remote PC Client попросить вас ввести ім'я, IP-адреса або RPC-номер комп'ютера, до якого ви хочете підключитися. Ми ввели ім'я комп'ютера (Sasha), після чого система запросила введення імені користувача і пароля. Ми ввели ім'я користувача і пароль (ті, які вказували при установці програми на комп'ютер, видимий в мережі під ім'ям Sasha) і Remote PC Client запропонував вибрати один з варіантів дій (рис. 35).

А саме, натиснувши кнопку ViewScreen (перегляд екрану) ми побачимо екран керованого комп'ютера в віконці клієнта, натиснувши Transferfiles (передача файлів) побачимо щось на зразок двох Провідників - один - в правій частині вікна - для віддаленої системи, другий - в лівій - для тієї, за якою ми працюємо. Ці ж кнопки продубльовані у верхній частині вікна.

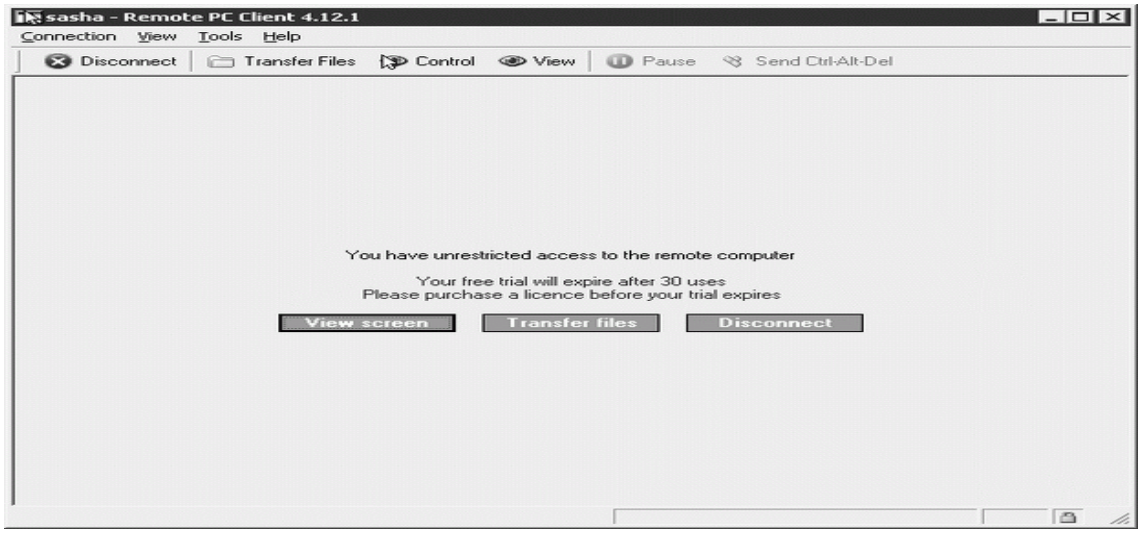


Рис. 35. Вибір дії

Тепер натискаємо кнопку ViewScreen і тут же можемо працювати з віддаленим комп'ютером так, як ніби сидимо за ним (рис. 36).

1

Рис. 36. Робота з віддаленим комп’ютером

В ході роботи ви можете перемикатися між режимами взаємодії з комп'ютером за допомогою кнопок у верхній частині вікна програми і управляти деякими параметрами.

Зокрема, командою Tools EnableSound можна передавати звуки з віддаленого комп'ютера і, при бажанні, налаштувати якість звуку командою Tools SoundOptions.

Дуже зручно використовувати віддалений робочий стіл у повноекранному режимі - так різниця між роботою безпосередньо за комп'юте-

ром і управлінням ним практично непомітна. Для того, щоб включити повноекранний режим - виберіть пункт меню View FullScreen. Для повернення у віконний режим натисніть Ctrl + Escape.

Переключивши програму в режим View і підключивши кілька комп'ютерів до одного, ви передаєте зображення з одного ПК на інші, що зручно, наприклад, при поясненні нової теми в комп'ютерному класі.

Для завершення сеансу зв'язку натисніть кнопку Disconnect.

Тепер давайте розглянемо настройки серверної частини програми. Відкрити їх вікно можна, зробивши подвійне клацання по піктограмі AccessRemote PC в треї (рис. 37).

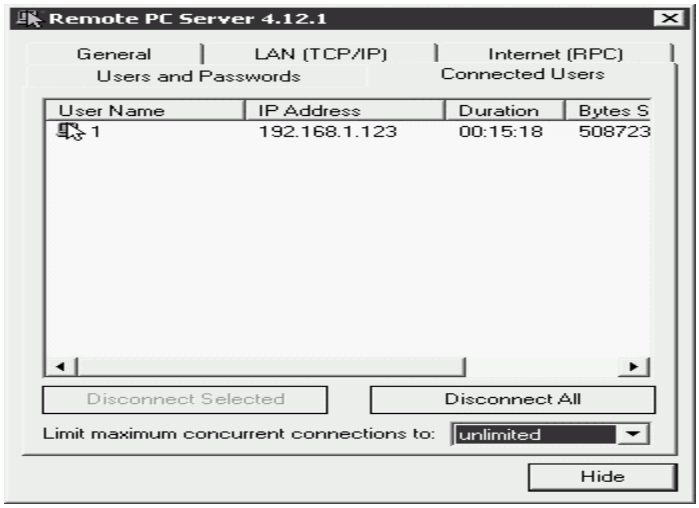


Рис. 37. Настройка серверної частини програми

Вкладка ConnectedUsers дозволяє переглядати інформацію про підключених користувачів, відключати їх усіх (DisconnectAll), або - тільки виділеного (DisconnectSelected), а також керувати кількістю підключень.

Вкладка UsersandPasswords дозволяє додавати в систему нових користувачів (New), редагувати існуючих (Edit) і видаляти їх (Delete).

Вкладка General крім цілком стандартних установок Automatically start when Windows Starts (Запускатися разом з Windows) і Show Icon in Tascbar (показувати іконку на панелі завдань) містить дуже важливу групу налаштувань, до якої веде посилання Advanced Settings (рис. 38).

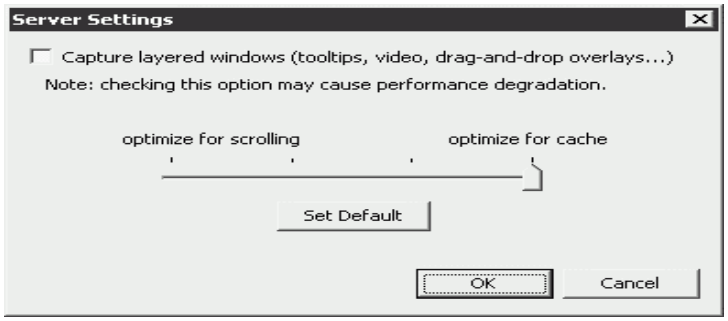


Рис. 38. Додаткові опції сервера

Встановивши галочку в поле Capture layered Windows ... ви зможете переглядати відео, що відтворюється на віддаленому комп'ютері, у вікні клієнта. Однак, це сильно збільшить навантаження на систему, що може привести до уповільнення її роботи.

Вкладка LAN (TCP / IP) містить настройки порту, на якому "сидить" сервер і параметрів підключення (їх цілком можна залишити за замовчуванням), а вкладка Internet (RPC) дозволяє налаштовувати доступ до ПК через Інтернет, зокрема, дозволяє ввести його RPC - номер якщо ви зареєструвалися в системі.

В ході роботи програми не було помічено серйозних збоїв. Як бачите, AccessRemote PC - це відмінне рішення для тих, хто хоче керувати комп'ютером дистанційно.

Завдання на лабораторну роботу

Оформіть звіт по лабораторній роботі. Виконати роботу з 5 і більше працездатними сервісами, опишіть послідовність дій.

Лабораторна робота 6. Принципи передачі інформації в мережі і стандартна модель взаємодії

Теоретичні відомості

Методи управління обміном

Мережа об'єднує кілька абонентів, кожен з яких має право передавати свої пакети. Однак одночасно по одному кабелю передавати кілька пакетів не можна, інакше може виникнути колізія (конфлікт), який призведе до спотворення або втрати цих пакетів. Необхідно встановити черговість доступу до мережі (захоплення мережі) усіма абонентами, які бажають передавати свої дані. Це відноситься, головним чином, до мереж з топологіями кільце і шина.

У будь-якій мережі обов'язково застосовується той чи інший метод управління обміном (метод доступу, метод арбітражу), що запобігає або дозволяє конфлікти між абонентами. Від ефективності роботи обраного методу управління обміном залежать основні характеристики мережі: швидкість обміну інформацією між комп'ютерами, здатність навантаження (здатність працювати з різними інтенсивностями обміну), час реакції мережі на зовнішні події і т.д. Метод управління - це один з найважливіших параметрів мережі. Тип методу управління обміном багато в чому визначається особливостями мережевої топології.

Методи управління обміном в локальних мережах діляться на дві групи:

Централізовані методи, в яких все управління обміном зосереджено в одному місці. Недоліки таких методів: нестійкість до відмов центру, мала гнучкість управління (центр не може оперативно реагувати на всі події в мережі). Перевага централізованих методів - відсутність конфліктів.

Децентралізовані методи, в яких відсутній центр управління. Всіма питаннями управління, в тому числі запобіганням, виявленням і розв'язанням конфліктів, займаються всі абоненти мережі. Головні переваги децентралізованих методів: висока стійкість до відмов і велика гнучкість, проте можливі конфлікти, які треба вирішувати.

Децентралізовані методи управління мережевим обміном, в свою чергу, ділять:

Детерміновані методи, які визначають чіткі правила і порядок використання мережі абонентами. Абоненти мають певну систему пріоритетів, причому ці пріоритети різні для всіх учасників мережевого обміну. При цьому конфлікти повністю виключені (або малоймовірні), проте деякі абоненти можуть чекати своєї черги на передачу досить тривалий час. До детермінованих методів належить, наприклад, маркерний доступ (мережі Token-Ring, FDDI), при якому право передачі передається по естафеті від попереднього абонента до наступного.

Випадкові методи, які мають на увазі випадкове (псевдовипадкове) чергування абонентів, що використовують мережу для передачі своїх даних. При цьому існує можливість конфліктів (колізій), але пропонуються способи їх вирішення. Випадкові методи значно гірше (в порівнянні з детермінованими) працюють при великих інформаційних навантаженнях в мережі (при великому мережевому трафіку) і не гарантують абоненту величину часу доступу. У той же час вони, як правило, стійкіше до відмов мережевого обладнання і більш ефективно використовують мережу при невисокій інтенсивності обміну. Характерним прикладом випадкового методу служить - CSMA / CD.

Для трьох основних топологій характерні три найбільш типових методів управління мережевим обміном.

Управління обміном в мережі з топологією зірка

У топології зірка найчастіше використовують централізований метод управління обміном. Це пов'язано з тим, що всі інформаційні потоки проходять через центр, і саме цьому центру логічно виконувати управління обміном в мережі. Периферійні абоненти, які бажають передати свій пакет (мають заявки на передачу), посилають центру свої запити (керуючі пакети або спеціальні сигнали). Центр надає їм право передачі пакету в порядку, визначеному алгоритмом. Наприклад, по їх фізичному розташуванню в зірці в напрямку за годинниковою стрілкою. У цьому випадку говорять, що абоненти мають географічні пріоритети (по їх фізичному розташування). У кожен момент часу найвищим пріоритетом має наступний за своєю чергою абонент, але в межах повного циклу опитування жоден з абонентів не має ніяких переваг перед іншими. Такий метод управління називають методом з пасивним центром, так як центр пасивно прослуховує периферійні абоненти.

Використовують і інший принцип реалізації централізованого управління (з активним центром). У цьому випадку центр посилає запити

про готовність передавати (керуючі пакети або спеціальні сигнали) по черзі всім периферійним абонентам. Той периферійний абонент, який має дані для передачі (перший з опитаних) посилає відповідь і відразу починає свою передачу. Надалі центр проводить сеанс обміну саме з ним. Після закінчення цього сеансу центральний абонент продовжує опитування периферійних абонентів. Якщо бажає передавати центральний абонент, він передає свої дані позачергово.

Обидва варіанти припускають, що ніяких конфліктів бути не може. Якщо всі абоненти активні, і заявки на передачу надходять інтенсивно, то всі вони будуть передавати строго по черзі, але центр повинен бути винятково надійний, інакше буде заблокований весь процес обміну. Механізм управління в даному випадку не дуже гнучкий, так як центр працює за заданим алгоритмом. До того ж швидкість управління обміном невисока. Адже навіть у разі, коли передає тільки один абонент, йому все одно доводиться чекати після кожного переданого пакета, поки центр опитає всі інші периферійні абоненти.

Як правило, централізовані методи управління застосовуються в невеликих мережах (з обмеженим числом абонентів). У разі великих мереж навантаження по управлінню обміном на центр істотно зростає.

Управління обміном в мережі з топологією шина

При топології шина також можливо централізоване управління. При цьому один з абонентів («центральний») посилає по шині всім іншим («периферійним») запити (керуючі пакети), з'ясовуючи, хто з них має дані для передачі, потім дозволяє передачу одному з абонентів. Абонент, який отримав право на використання мережі, по тій же шині передає свій інформаційний пакет іншому абоненту. Після закінчення передачі абонент, який передавав, все по тій же шині повідомляє «центру», що він закінчив передачу (керуючим пакетом), і «центр» знову починає опитування абонентів. Переваги та недоліки такого управління - ті ж самі, що і в разі централізовано керованої зірки. Відмінність полягає в тому, що центр тільки управляє обміном, а не пересилає інформацію від одного абонента до іншого, як в топології активна зірка.

Значно частіше в шині використовується децентралізоване випадкове управління, так як мережеві адаптери всіх абонентів однакові, і саме цей метод найбільш органічно підходить до шиної топології. При децентралізованому управлінні всі абоненти мають рівні права доступу до мережі, а значить особливості топології в великій мірі збігаються з особ-

ливостями методу управління. Рішення про можливість передавати свій пакет, приймається кожним абонентом, виходячи з аналізу стану мережі. В даному випадку виникає конкуренція між абонентами за захоплення мережі, що призводить до можливості конфліктів між ними і спотворення інформації, що передається через колізії.

Існує велика кількість алгоритмів доступу (сценаріїв доступу), іноді досить складних. Їх вибір залежить від різних характеристик мережі: швидкості передачі, довжини шини, її завантаженості (інтенсивності обміну і пропускної здатності мережі), використовуваного коду для передачі даних.

Суть всіх випадкових методів управління обміном досить проста і полягає в наступному. Якщо мережа вільна (ніхто не передає пакетів), то абонент, який має дані для обміну, починає свою передачу. Час доступу до мережі в цьому випадку дорівнює нулю. Якщо ж в момент виникнення у абонента заявки на передачу мережа зайнята, то абонент, який претендує на її використання, чекає звільнення мережі. У разі одночасної передачі спотворяться і пропадуть обидва пакети. Після звільнення мережі абонент, що бажає передавати, починає свою передачу. Виникнення конфліктних ситуацій (зіткнень пакетів, колізій), в результаті яких передається інформація спотворюється, можливо в наступних випадках:

При одночасному початку передачі двома або кількома абонентами, коли мережа вільна. Ситуація досить рідкісна, але все-таки цілком можлива.

При одночасному початку передачі двома або кількома абонентами відразу після звільнення мережі. Ця ситуація найбільш типова, так як за час передачі пакета одним абонентом може виникнути кілька нових заявок на передачу у інших абонентів.

Використовувані випадкові методи управління обміном (арбітражу) розрізняються тим, як вони запобігають можливим конфліктам або дозволяють їм виникати.

Недоліком всіх випадкових методів є те, що вони не гарантують абонентам величину часу доступу до мережі, яка залежить не тільки від затримки між спробами передачі, але і від загальної завантаженості мережі. Тому в мережах, що виконують завдання управління обладнанням (на виробництві, в наукових лабораторіях), де потрібна швидка реакція на зовнішні події, мережі з випадковими методами управління практично не використовуються.

Управління обміном в мережі з топологією кільце

Кільцева топологія має свої особливості при виборі методу управління обміном. Тут немає одночасного розповсюдження сигналу в дві сторони характерного для топології шина. У мережі з топологією кільце можна використовувати різні централізовані методи управління (як в зірці), а також методи випадкового доступу (як у шині), але частіше вибирають специфічні методи управління, які в найбільшій мірі відповідають особливостям кільця.

Найпопулярнішими методами управління в кільцевих мережах є маркерні (естафетні) які використовують невеликий керуючий пакет спеціального виду. Естафетна передача маркера по кільцю дозволяє передавати право на використання мережі від одного абонента до іншого. Маркерні методи відносяться до децентралізованих і детермінованих методів управління мережевим обміном. У них відсутній явно виражений центр, але існує чітка система пріоритетів, яка дозволяє повністю уникнути конфліктів.

По кільцю безперервно переміщується спеціальний керуючий пакет мінімальної довжини (маркер), який надає абонентам право передавати свій пакет. Основна перевага маркерного методу полягає в гарантованій величині часу доступу до мережі.

Завдання на лабораторну роботу

Оформіть звіт по лабораторній роботі, опишіть основні принципи передачі інформації в мережі. Розробити таблицю, яка ілюструє методи управління обміном в різних топологіях.

Лабораторна робота 7. Бездротові технології Bluetooth

Мета роботи: вивчити концепції бездротових мережевих технологій, класифікацію бездротових мереж. Дослідити характеристики бездротової персональної мережі стандарту IEEE 802.15.1.

Теоретичні відомості

З'єднання телефону і комп'ютера

З'єднання і синхронізація здійснюються за допомогою програми, другим необхідним елементом є наявність Bluetooth-адаптера. У телефоні він є вбудованим, а установка адаптера на комп'ютер не викликає проблем, так як здійснюється за допомогою Майстра установки нового обладнання Windows (рис. 39).

Рис 39. Настройка адаптера Bluetooth

Далі необхідно розкрити вікно «Bluetooth-оточення» і вибрати у верхньому меню розділ Bluetooth, клацнути пункт «Додаткові настройки» і у вікні, натиснути на «Локальні служби». Далі потрібно вказати і запам'ятати COM-порт для організації з'єднання (рис. 40).

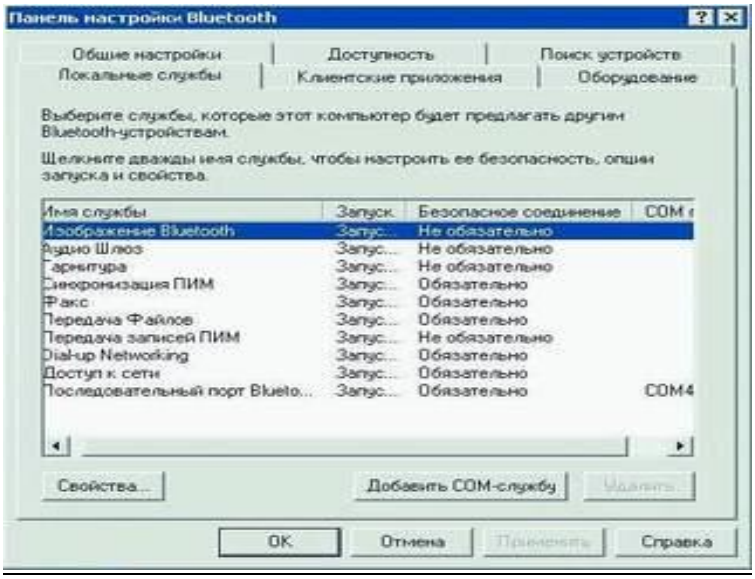


Рис. 40. Панель настройки Bluetooth

В меню Bluetooth телефону активуємо однойменну функцію. Будуть знайдені всі Bluetooth-пристрої (рис. 41), що знаходяться в радіусі дії. Нам залишається тільки вибрати ім'я нашого комп'ютера і натиснути Next. Після - на екрані виникне вимога ввести код; вводимо «0000». Переходимо до екрану комп'ютера і також вказуємо «0000». Необхідно, щоб пароль по обидва боки підключення збігався.

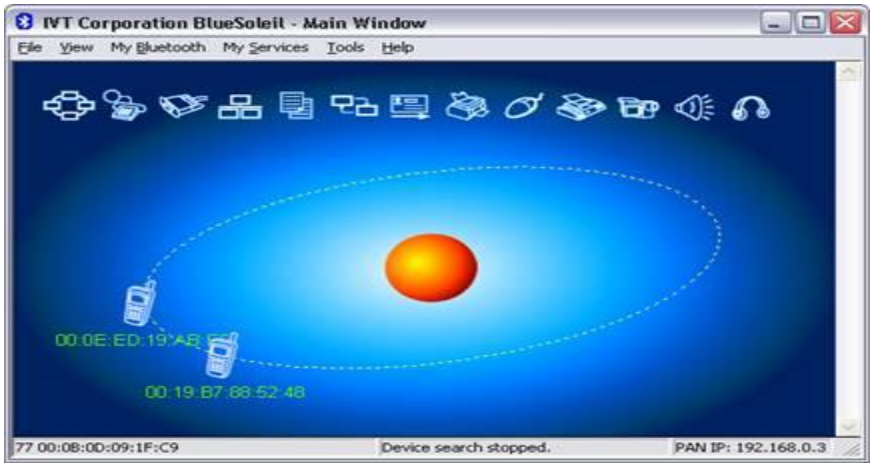


Рис. 41. Вікно діалогу, в якому відображаються телефон з активним BT

Після закінчення синхронізації в провіднику стає можливим доступ до вмісту пам'яті пристрою. Ця функція дуже зручна для установки нових програм і копіювання важливої інформації (рис. 42).

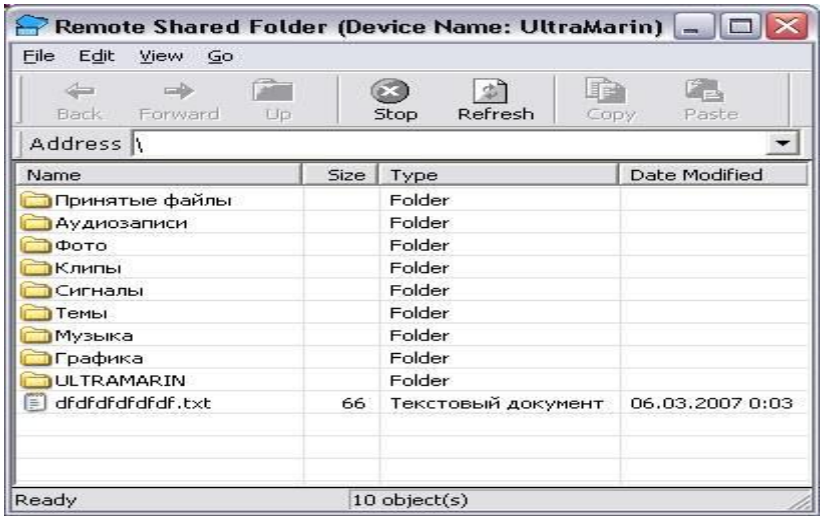


Рис. 42. Відображення вмісту телефона на ПК

У підсумку вийшло з'єднання телефону і комп'ютера (рис. 43).

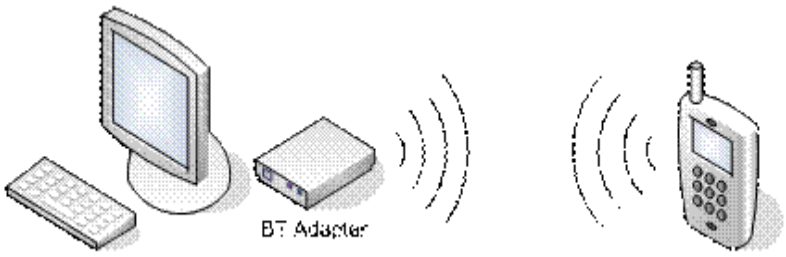


Рис. 43. Схема з’єднання комп’ютера з телефоном по каналу Bluetooth

З'єднання двох комп'ютерів

Якщо потрібно з'єднати два комп'ютери між собою за допомогою технології Bluetooth, потрібно використовувати Bluetooth-адаптер. Після об'єднання двох комп'ютерів за допомогою Bluetooth на екрані з'явиться відповідне діалогове вікно (рис. 44).

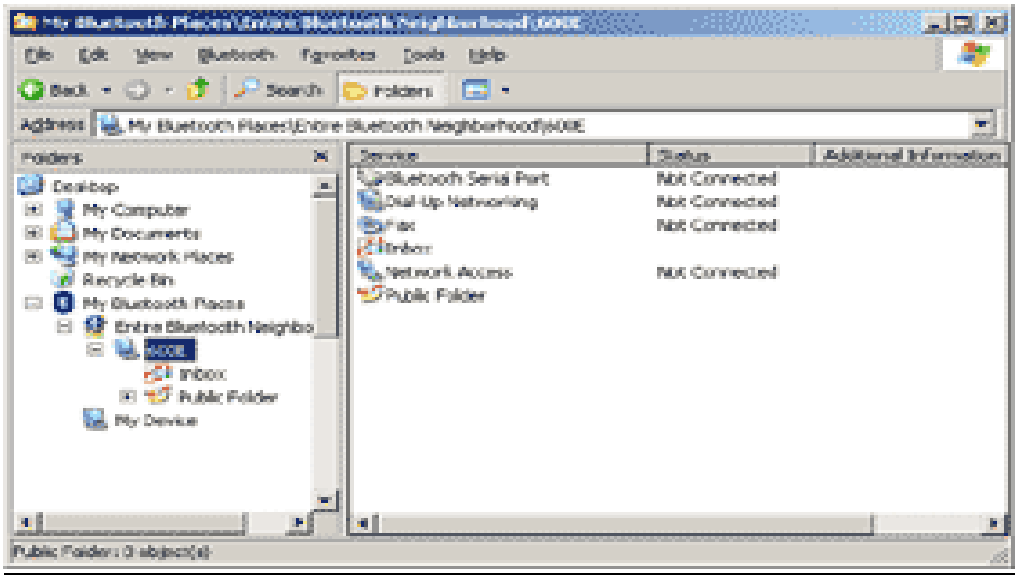


Рис. 44. Поєднання комп’ютерів за допомогою Bluetooth

Операційна система бачить з'єднання Bluetooth, як досить швидкий послідовний порт (він приблизно в п'ять разів швидше, ніж звичайний COM або IrDA). Далі слід налаштувати підключення Bluetooth в папці «Мережні підключення» (рис. 45).

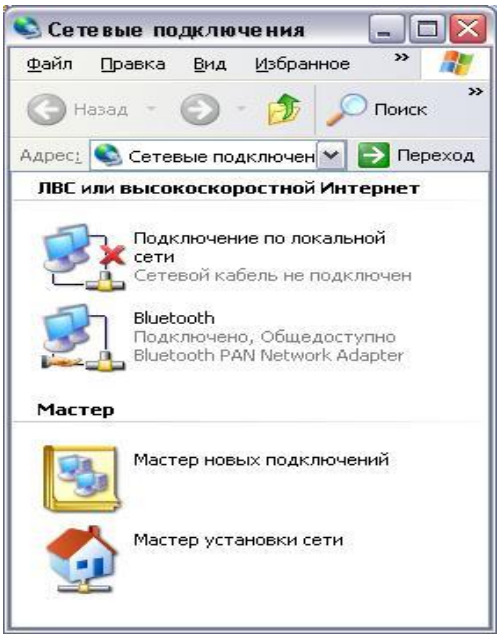


Рис. 45. Настройка підключення Bluetooth

Необхідно обрати доступні компоненти (рис. 46).

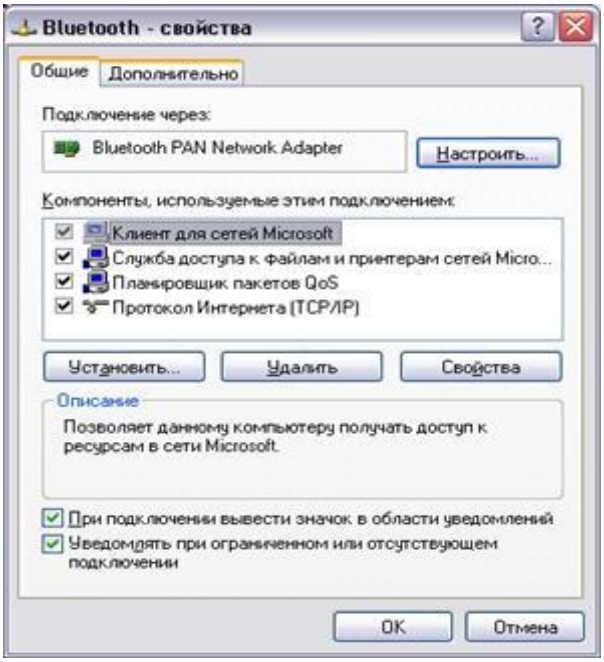


Рис. 46. Настройка компонентів Bluetooth

Після виконання всіх дій вийшло мережеве підключення з наступними параметрами (рис. 47):

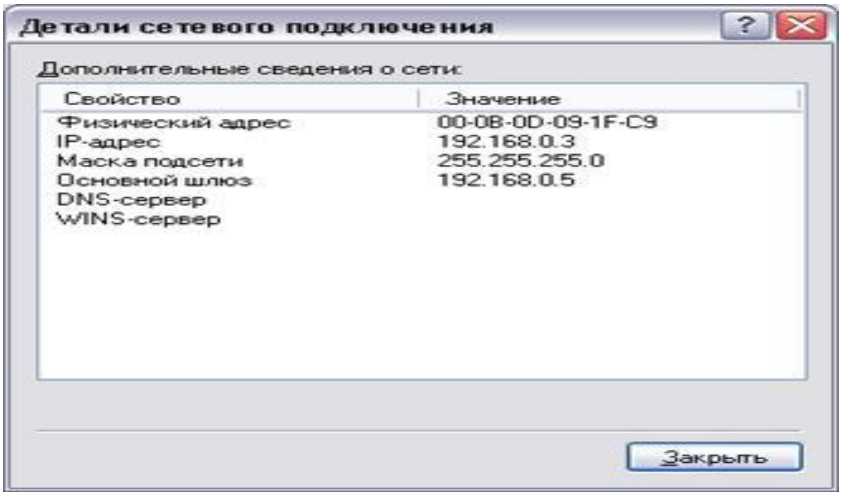


Рис. 47. Параметри мережевого підключення Bluetooth

Завдання на лабораторну роботу

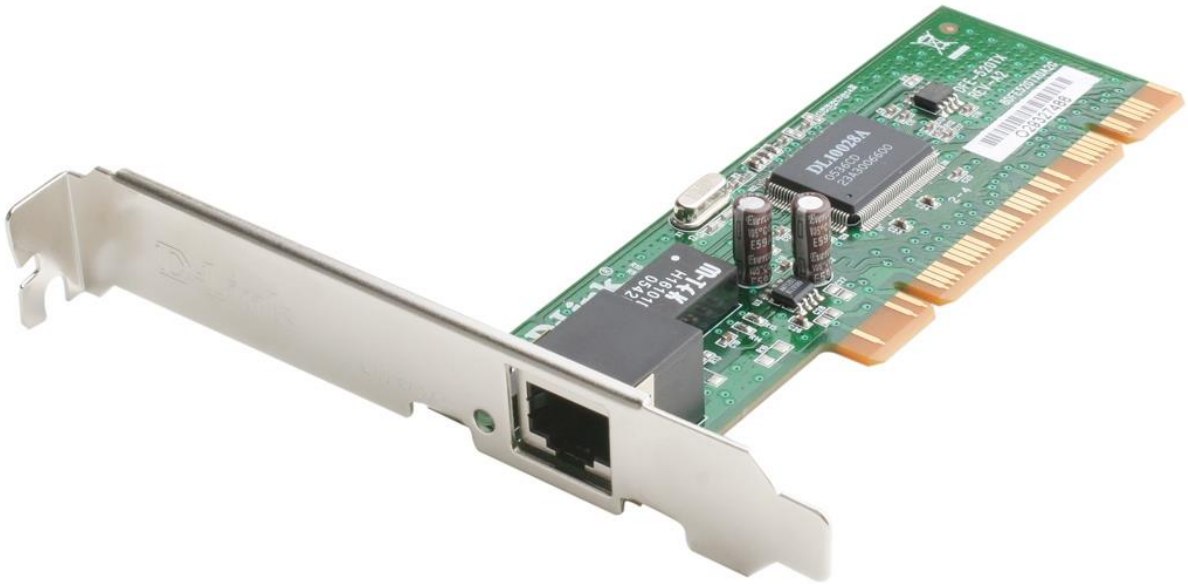
Оформіть звіт по лабораторній роботі, опишіть та покажіть скріншотами виконання вправ. Виконати таблиці, які ілюструють швидкості передачі даних.

Лабораторна робота 8. Устаткування Ethernet і Fast Ethernet

Мета роботи: Ознайомитися з обладнанням для мереж Ethernet і Fast Ethernet - на сьогоднішній день мережа Ethernet / Fast Ethernet є найперспективнішою, вона поширена найбільш широко, і апаратура для неї випускається найбільшим числом виробників.

Теоретичні відомості

Адаптери Ethernet і Fast Ethernet



Мережеві адаптери (NIC, Network Interface Card) Ethernet і Fast Ethernet можуть з'єднуватись з абонентом (комп'ютером) через один зі стандартних інтерфейсів:

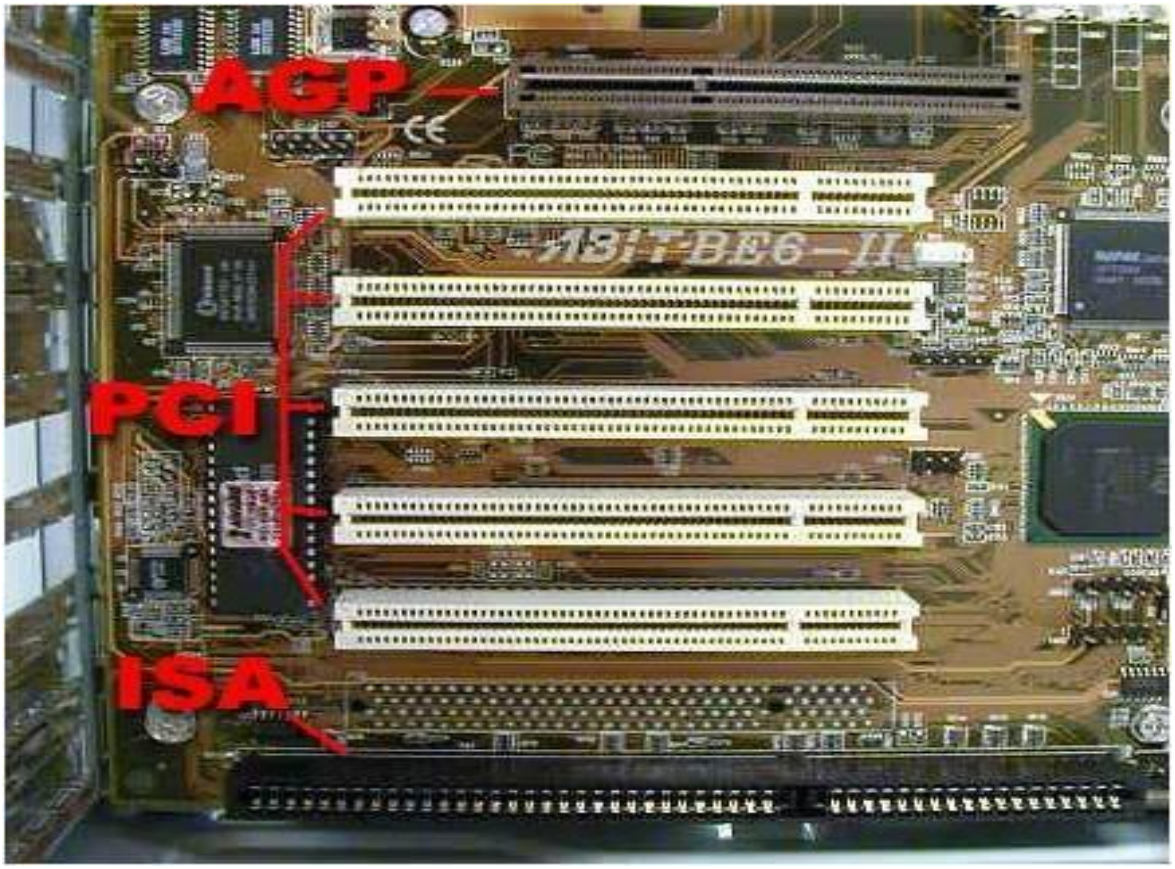
шина PCI (Peripheral Component Interconnect);

шина ISA (Industry Standard Architecture);

шина PC Card (PCMCIA).

Адаптери, розраховані на системну шину ISA вважаються застарілими. Вони випускалися 8- і 16-розрядних (8-розрядні адаптери дешевше, 16-розрядні - швидше).

Зараз шина PCI практично витіснила шину ISA, вона стала основною шиною розширення для персональних комп'ютерів.



Вона забезпечує обмін 32- і 64-розрядними даними і володіє високою пропускною здатністю (до 264 Мбайт / с), що цілком достатньо не тільки для Fast Ethernet, а й більш швидкої Gigabit Ethernet. Для забезпечення сумісності важливо ще й те, що шина PCI використовується не тільки в комп'ютерах IBM PC, але і в комп'ютерах фірми Apple. Крім того, ця шина підтримує режим автоматичного конфігурування обладнання (Plug-and-Play).

Шина PC Card (раніше використовувалась назва PCMCIA) застосовується в комп'ютерах Notebook. У цих комп'ютерах шина PCI зазвичай не має зовнішніх підключень. Інтерфейс PC Card передбачає просте приєднання до комп'ютера мініатюрних плат розширення, при цьому швидкість обміну даними з цими платами досить висока.

Однак зараз все більше портативних комп'ютерів (як і ПК) оснащується вбудованими мережевими адаптерами, так як можливість доступу до мережі стає стандартом «де-факто».

Найважливішими характеристиками мережевих адаптерів є:

спосіб конфігурації адаптера;

обсяг буферної пам'яті і режими обміну з нею;

можливість установки ПЗУ для віддаленого завантаження (BootROM);

можливість підключення адаптера до різних типів середовища передачі;

можливість застосування адаптером повнодуплексного режиму обміну;

сумісність адаптера (драйвера) з мережними програмними засобами.

Первісна настройка адаптера виконується і автоматично в режимі Plug-and-Play при включенні персонального комп'ютера. Від розміру буферної пам'яті мережного адаптера залежить швидкість роботи адаптера і його здатність підтримати великі обсяги переданих даних. Розмір пам'яті зазвичай становить кілька десятків мегабайт. Чим більше пам'ять, тим більше надісланих та отриманих пакетів може в ній зберігатися.

Деякі адаптери підтримують функцію віддаленого завантаження по мережі. Для цього на платі мережевого адаптера встановлюється мікросхема постійної пам'яті (Boot ROM), в якій записана програма початкового завантаження персонального комп'ютера. Такий підхід дозволяє використовувати комп'ютери без жорстких дисків.

Адаптер може бути розрахований тільки на один тип кабелю, але може підтримувати можливість підключення декількох різних середо-

вищ передачі даних (кручену пару, тонкий і товстий коаксіальні кабелі). Для цього на платі встановлюються відповідні роз'єми.

Найбільшу свободу підключення забезпечували універсальні, так звані адаптери «Combo», на яких встановлено повний набір роз'ємів (BNC, RJ-45 і AUI для Ethernet).

Всі мережеві адаптери підлягають сертифікації. Сертифікат FCC А-класу дозволяє використовувати адаптер в бізнесі, сертифікат FCC В-класу - будинки. Стандарт регламентує безпечні рівні електромагнітного випромінювання мережевих адаптерів.

Сумісність драйвера адаптера з мережевим програмним забезпеченням є важливою характеристикою, на яку необхідно звертати увагу при його виборі. Усі постачальники мережевого програмного забезпечення (Novell, Microsoft і ін.) сертифікують свої драйвери. Якщо такий сертифікат є, то можна бути впевненим, що проблем з сумісності з мережевим апаратним забезпеченням не буде. Виробники мережевих адаптерів регулярно поширюють поліпшені, більш швидкі і універсальні версії драйверів для своїх плат.

Репітери і концентратори Ethernet і Fast Ethernet

Використання репітерів і концентраторів (хабів) в мережі Ethernet є не обов'язковим.

Невеликі мережі на основі сегментів 10BASE2 або 10BASE5 можуть функціонувати без них. Для мереж з декількох сегментів необхідно застосування найпростіших репітерів.

Функції репітерів і концентраторів

Репітери (повторювачі) ретранслюють сигнали, які приходять на них (на їх порти), відновлюють їх амплітуду і форму, що дозволяє збільшувати протяжність мережі. Цю функцію реалізують і репітерні концентратори. Крім цієї основної функції концентратори Ethernet і Fast Ethernet можуть виконувати ще ряд функцій з виявлення та виправлення деяких найпростіших мережевих помилок.

Найпростіший концентратор являє собою досить складний пристрій, який автоматично усуває деякі несправності і збої. Концентратор не тільки об'єднує точки включення кабелів абонентів, але і покращує умови обміну мережі, підвищує її продуктивність, відключаючи несправні або некоректно працюючі сегменти.

Основна характеристика концентратора - він не робить ніякої обробки інформації, сприймаючи пакети як єдине ціле, не аналізуючи їх внутрішнього вмісту.

Комутатори Ethernet і Fast Ethernet

Комутуючі концентратори (Switched Hubs) або, як їх ще називають, комутатори (Switches), перемикачі та свічі дозволяють розділити єдину мережу на кілька сегментів для збільшення допустимого розміру мережі або з метою зниження інформаційного навантаження (трафіка) в окремих її частинах. Комутуючі концентратори переправляють з однієї частини мережі в іншу ті пакети, які цього потребують. Вони в реальному часі визначають адресу приймача пакета і приймають рішення про те, чи потрібно цей пакет переправляти, і кому. Комутатори не проводять жодної обробки пакетів, а тільки контролюють їх заголовок, вони практично не сповільнюють мережевого обміну. Оскільки комутатори працюють з інформацією, що знаходиться всередині кадру, вважається, що вони ретранслюють кадри, а не пакети, як репітерні концентратори.

Комутатор ретранслює колізії, що вигідно відрізняє їх від більш простих репітерних концентраторів. Комутатори проводять більш глибокий поділ мережі, ніж концентратори. Вони поділяють на сегменти зони колізій (Collision Domain) мережі - області мережі, на які поширюються колізії. У пакеті, що прийшов комутатор читає фізичні адреси відправника і одержувача і передає його в той сегмент, в який він адресований. Якщо пакет адресований абоненту з того ж сегмента, до якого належить відправник, то він не ретранслюється. Комутатори випускаються з 8, 12, 16 і 24 портами.

Вони характеризуються двома показниками продуктивності:

сукупна швидкість ретрансляції пакетів, яка вимірюється при активній роботі всіх наявних портів;

максимальна швидкість ретрансляції пакетів, яка вимірюється при передачі пакетів з одного порту в інший, коли всі інші порти даного комутатора відключені.

Основне правило, якого дотримуються при розбитті мережі на частини (сегменти) за допомогою комутатора, називається «правило 80/20». Відповідно до нього, необхідно, щоб понад 80 відсотків усіх передач відбувалося в межах однієї частини (одного сегмента) мережі. І тільки 20 відсотків всіх передач повинно відбуватися між різними частинами (сегментами) мережі, тобто проходити через комутатор. Тільки при виконанні цього правила комутатор, і мережа працюють ефективно. На практиці необхідно прагнути до того, щоб сервер і активно працюючі з ним абоненти (комп'ютери) розташовувалися в одному сегменті.

Мости і маршрутизатори Ethernet і Fast Ethernet

Мости і маршрутизатори спочатку представляли собою універсальні комп'ютери, що працюють в мережі і виконують специфічну функцію з'єднання двох або більше її частин.

До недавнього часу мости були основними пристроями, які застосовувались для поділу мережі на частини (сегментування). Їх вартість менше, ніж маршрутизаторів, а швидкодія вище, до того ж вони, як і комутатори, прозорі для протоколів другого рівня моделі OSI - абоненти мережі можуть не знати про наявність у мережі мостів, а всі їхні пакети доходять до потрібного адресата.

За своїми функціональними можливостями міст дуже близький до комутатору, але повільніше останнього. Він зазвичай має від двох до чотирьох портів, кожен з яких з'єднаний з одним з мережевих сегментів. У разі, коли міст виконується на базі універсального комп'ютера, в нього встановлюється потрібне число мережних адаптерів, до кожного з яких підключається свій мережевий сегмент.

Традиційно розрізняють внутрішні і зовнішні мости. Перші виконуються на основі комп'ютера-сервера, в який встановлюють кілька мережевих адаптерів (до чотирьох), підключені до різних мережевих сегментів - саме ці мережеві адаптери і відповідні програмні засоби називаються внутрішнім мостом.

Зовнішній міст - це комп'ютер, в який встановлено кілька мережних адаптерів. На відміну від внутрішнього моста, в цьому випадку сегменти мережі можуть бути тільки однотипними (наприклад, Ethernet-Ethernet).

Мости, як і комутатори, поділяють зону конфлікту (область колізії, Collision Domain). В результаті поділу зони конфлікту навантаження на кожен сегмент зменшується і долається обмеження на розмір мережі. На відміну від комутатора міст може обробляти (ретранслювати) тільки один пакет. Це пов'язано з тим, що всі функції моста виконуються послідовно одним центральним процесором комп'ютера, тому міст працює значно повільніше, ніж комутатор. Мости і комутатори дуже близькі за своїми характеристиками. Однак мости мають велику перевагу, вони можуть поєднувати не тільки однойменні сегменти, але також сполучати мережі Ethernet і Fast Ethernet з мережами будь-яких інших типів, такими як, FDDI або Token-Ring.

Функції маршрутизаторів

Маршрутизатор працює на більш високому, третьому рівні моделі OSI (комутатори і мости - на другому), вони взаємодіють з протоколами більш високих рівнів. Маршрутизатор, як комутатори або мости передає пакети з однієї частини мережі в іншу (між сегментами).

Між маршрутизаторами і мостами існують принципові відмінності:

маршрутизатори працюють не з фізичними адресами пакетів (MAC-адресами), а з логічними мережними адресами (IP-адресами або IPX-адресами);

маршрутизатори ретранслюють не всі дані, які приходять, а тільки ті, які адресовані їм, розділяючи тим самим широкомовну область мережі (Broadcast Domain);

всі абоненти обов'язково повинні знати про присутність в мережі маршрутизатора, вони не прозорі для абонентів на відміну від мостів і комутаторів;

маршрутизатори підтримують мережі з великою кількістю можливих маршрутів, шляхів передачі даних.

Маршрутизатор складніше і дорожче мостів і комутаторів (вартість маршрутизації в Ethernet приблизно в 10 разів перевищує номінальну вартість комутації). Вони складніше в управлінні і значно повільніше комутаторів, проте маршрутизатори забезпечують найглибший поділ мережі на частини. Якщо репітерні концентратори повторюють всі пакети, які надійшли на них (1-й рівень моделі OSI), а мости і комутатори ретранслюють тільки міжсегментні пакети (2-й рівень моделі OSI), то маршрутизатори об'єднують незалежні, практично не впливаючі один на одного мережі, зберігаючи при цьому можливість передачі інформації між ними (3-й рівень моделі OSI).

Для вибору маршруту кожен маршрутизатор формує в своїй пам'яті спеціальні таблиці даних, які містять:

номери мереж, підключених до даного маршрутизатора;

список всіх сусідніх маршрутизаторів;

список MAC-адрес і IP (IPX) адрес всіх абонентів мереж, підключених до маршрутизатора, який автоматично оновлюється.

Список всіх доступних маршрутизаторів повинен бути і у кожного мережевого абонента. Саме маршрутизатори використовуються для зв'язку локальних мереж з глобальними.

Маршрутизатор часто застосовується для об'єднання опорної (стрижневою) мережі типу FDDI і безлічі локальних мереж або для зв'язку локальних мереж різних типів, вони здійснюють перетворення формату пакетів, необхідну в даній ситуації. Маршрутизатор також легко перетворює швидкості передачі, пов'язуючи, наприклад, між собою мережі Ethernet, Fast Ethernet і Gigabit Ethernet. Маршрутизатори можна з'єднувати між собою. Безліч пов'язаних один з одним маршрутизаторів

утворюють так звану хмару (Cloud), що представляє собою один великий маршрутизатор. Таке з'єднання забезпечує дуже надійний і гнучкий зв'язок між усіма підключеними до нього локальними мережами.

Маршрутизатори дорогі і складні в налаштуванні і експлуатації. Тому їх використовують тільки в тих випадках, коли це дійсно необхідно, якщо застосування комутаторів і мостів не дозволяє подолати перевантаження мережі.

Завдання на лабораторну роботу

Повторити теоретичний матеріал за темою лабораторного заняття.

Підготувати короткі доповіді на тему:

1. Принципи роботи мережевих адаптерів.
2. Налаштування параметрів мережного адаптера.
3. Поняття та види комутаторів.
4. Принципи з'єднання комутаторів.
5. Управління комутатором через веб-інтерфейс.
6. Управління комутатором через командний рядок.
7. Виконання консольних команд.

Надати відповіді на тестові завдання.

1. Драйвер в операційній системі потрібний для ...

• маршрутизатора
• трансівера
• мережного адаптера
• концентратор
• комутатора

2. Пристрій, що транслює сигнали, що прийшли на один з декількох портів, тільки на порт адресата –

• концентратор
• репітер
• комутатор

3. Застосування якого пристрою дозволяє зменшити кількість конфліктів, що виникають у мережі?

• концентратор
• комутатор
• репітер

4. Для збільшення протяжності мережі із топологією «зірка» використовується ...

• комутатор

• термінатор

• маршрутизатор

• репітер

• мережевий адаптер

5. Маршрутизатор…

• підключається до відкритого кінця лінії передачі для придушення відбитих сигналів

• передає пакети між різними мережами

• передає пакети лише в межах однієї мережі

• транслює всі сигнали, що прийшли на один із портів, на всі інші порти

Підготувати відповіді на контрольні питання.

1. Для чого використовується мережевий адаптер?

2. Які види комутаторів існують?

3. Опишіть алгоритм роботи комутаційної матриці.

4. Опишіть принцип роботи VLAN.

5. Як підвищити стійкість до відмови мережі, побудованої з використанням комутаторів?

Лабораторна робота 9. З'єднання двох комп'ютерів по Wi-Fi

Мета роботи: Вивчити концепції бездротових мережевих технологій, класифікацію бездротових мереж. Дослідити характеристики бездротової персональної мережі стандарту Wi-Fi.

Теоретичні відомості

Увімкніть Wi-Fi адаптер. Клацніть «Пуск» - далі правою кнопкою миші по значку «Комп'ютер». Виберіть пункт меню «Властивостей» та клацніть по посиланню «Додаткові параметри системи» (рис. 48).

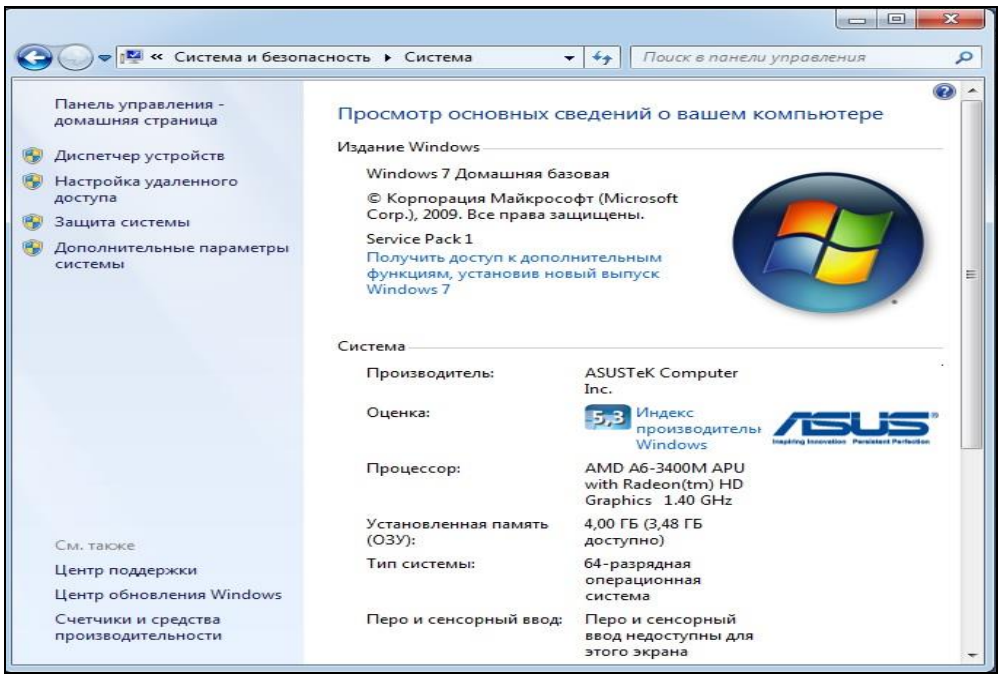


Рис. 48. Підключення Wi-Fi адаптера до ПК

Перейдіть на вкладку «Ім'я комп'ютера». В поле «Опис»: вкажіть опис комп'ютера. Натисніть кнопку «Змінити» (рис. 49).

В полі «Ім'я комп'ютера»: задайте ім'я комп'ютера. Ім'я комп'ютера повинно бути унікальним. Не можна ставити ім'я комп'ютера, яке вже використовується в мережі. В полі «робочої групи»: вкажіть ім'я робочої групи. Ім'я робочої групи має бути однаковим на всіх комп'ютерах мережі. Натисніть «ОК» (рис. 50).

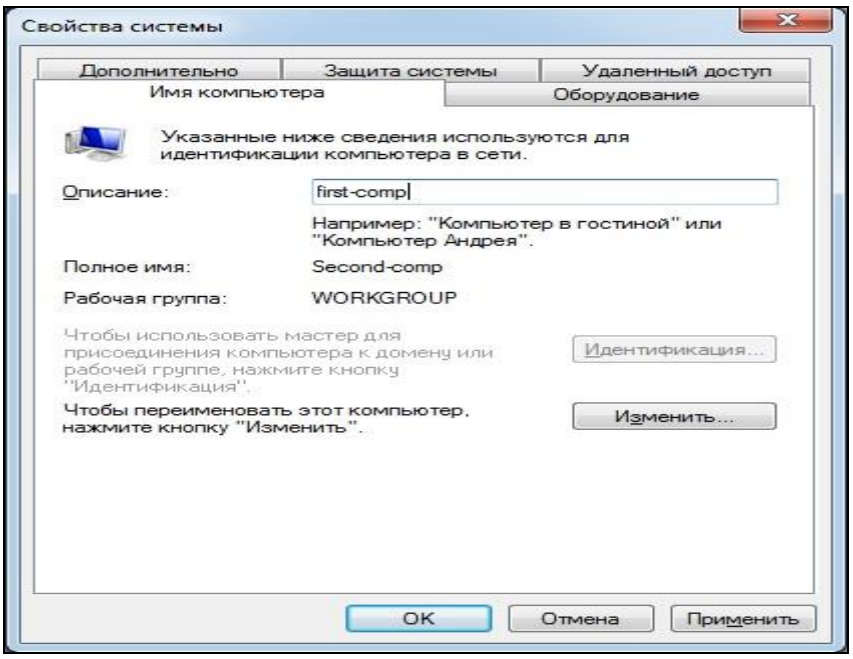


Рис. 49. Створення опису ПК

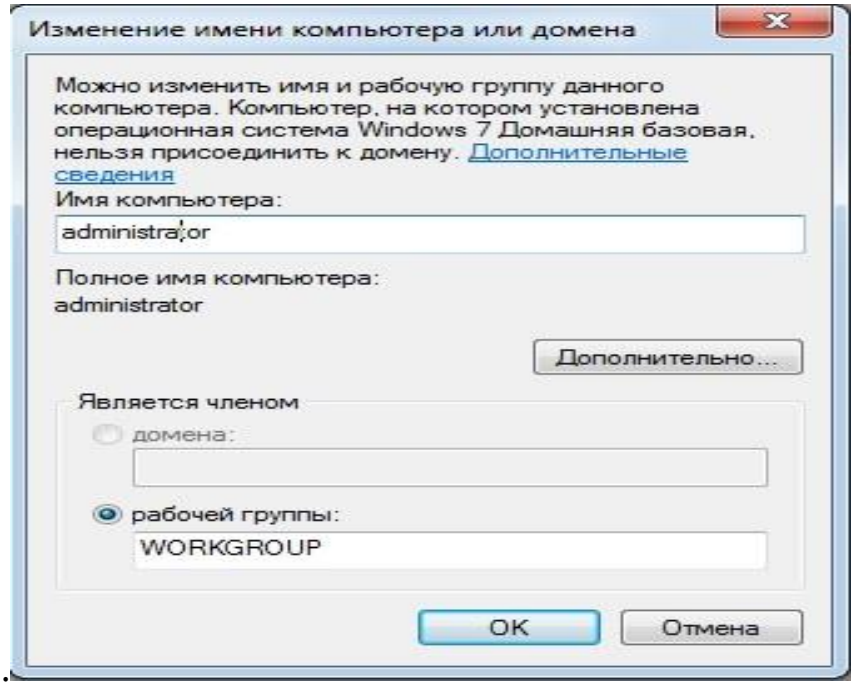


Рис. 50. Створення імені та визначення робочої групи

Зайдіть в «Центр управління мережами і загальним доступом». Натисніть посилання «Управління бездротовими мережами» (рис. 51).

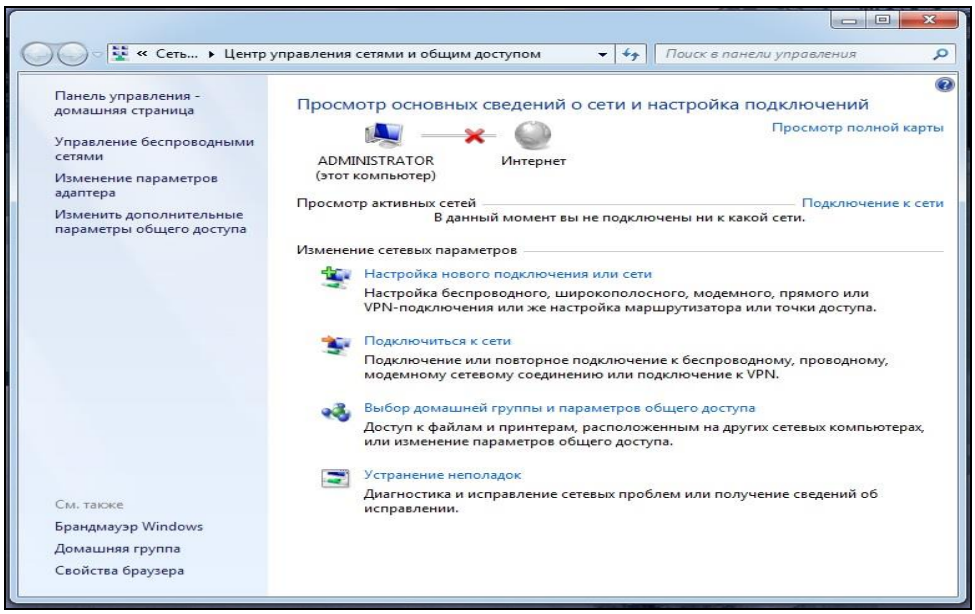


Рис. 51. Центр управління мережами та загальним доступом

Натисніть кнопку «Додати» (рис. 52).

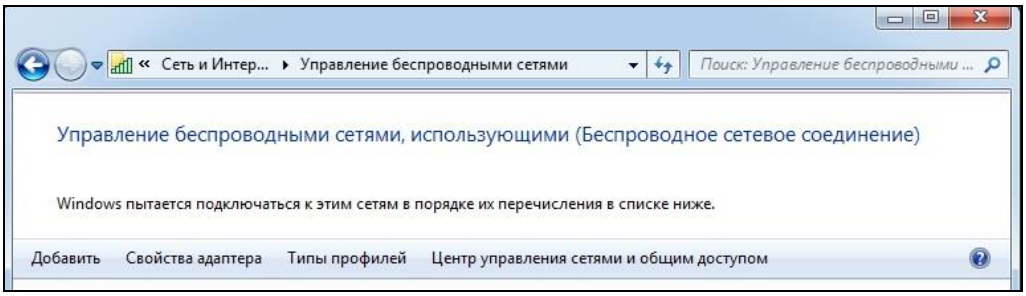


Рис. 52. Підключення до бездротової мережі

Натисніть «Створити мережу комп'ютер-комп'ютер» (рис. 53).

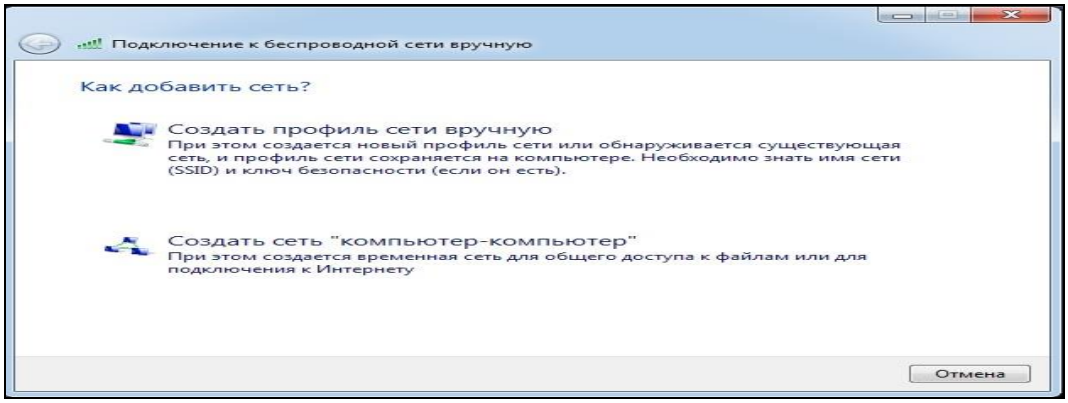


Рис. 53. Визначення способу створення мережі

Натисніть кнопку "Далі". В полі «Ім'я мережі»: задайте довільне ім'я мережі. В полі «Тип безпеки»: виберіть «WPA2-Personal».

В полі «Ключ безпеки»: введіть пароль. Він має містити від 8 до 63 знаків. Якщо вибрано шифрування WEP, то пароль повинен складатися з 5 або 13 знаків. Для створення пароля краще використовувати генератор паролів. Натисніть кнопку «Далі» (рис. 54). Натисніть кнопку «Закрити».

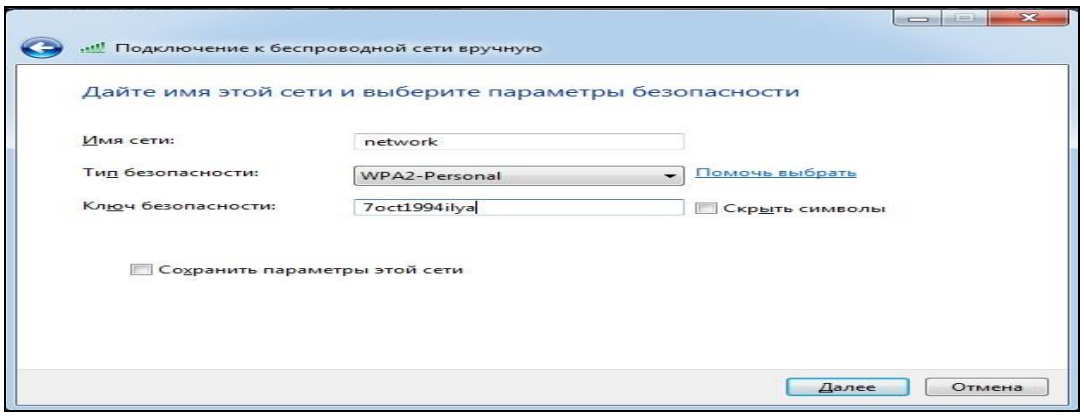


Рис. 54. Настройка параметрів безпеки мережі

Налаштування інших комп'ютерів мережі

Увімкніть Wi-Fi адаптер. Клацніть «Пуск» - далі правою кнопкою миші по значку «Комп'ютер». Виберіть пункт меню «Властивості». Клацніть по посиланню «Додаткові параметри системи» (рис. 55).

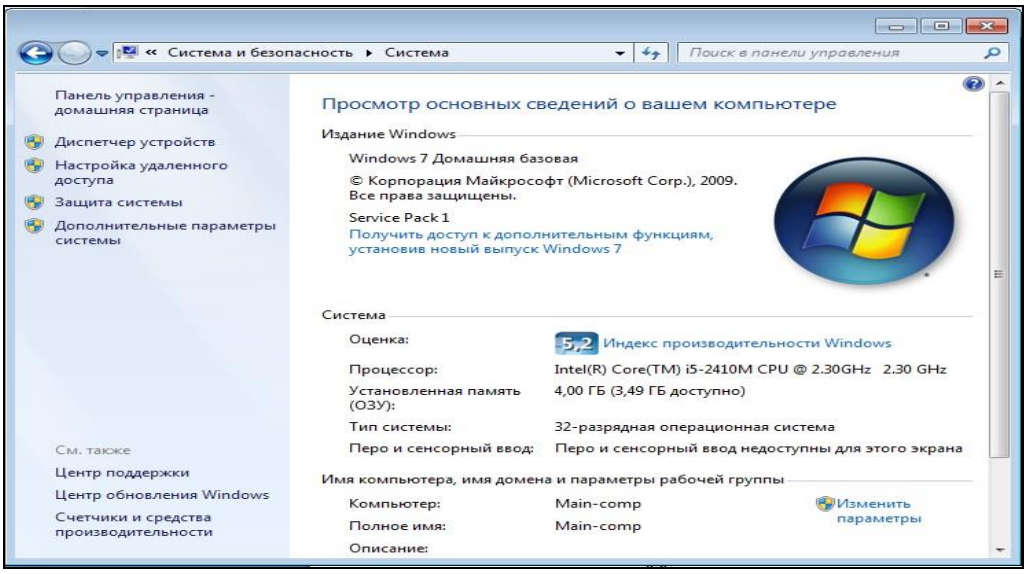


Рис. 55. Настройка інших ПК мережі

Перейдіть на вкладку «Ім'я комп'ютера». В полі «Опис»: вкажіть опис комп'ютера, наприклад «Комп'ютер Анатолія». Натисніть кнопку «Змінити» (рис. 56).

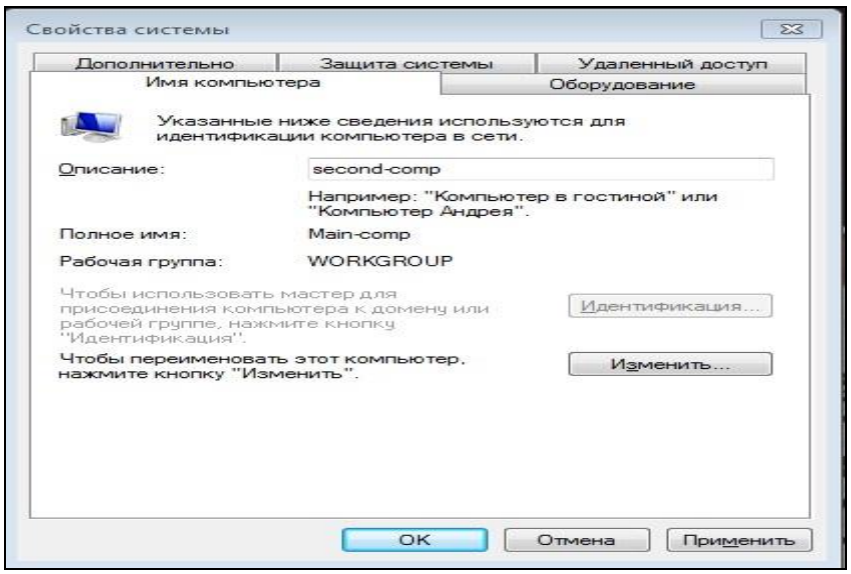


Рис. 56. Опис комп’ютерів мережі

В полі «Ім'я комп'ютера»: задайте ім'я комп'ютера. Ім'я комп'ютера повинно бути унікальним. Не можна ставити ім'я комп'ютера яке вже використовується в мережі. В полі «робочої групи»: вкажіть ім'я робочої групи. Ім'я робочої групи має бути однаковим на всіх комп'ютерах мережі. Натисніть «ОК» (рис. 57).

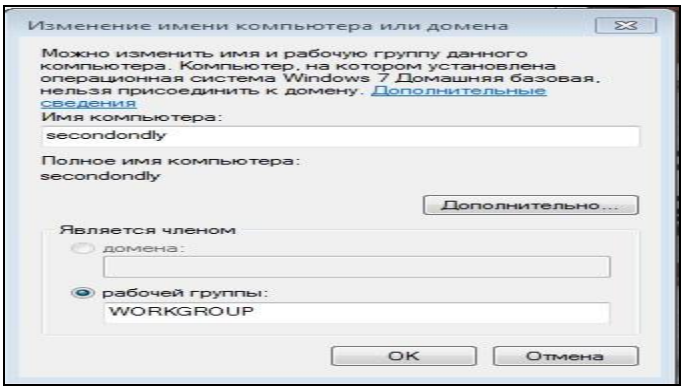


Рис. 57. Створення ідентифікаційних параметрів

Зайдіть в «Центр управління мережами і загальним доступом». Натисніть на посилання "Зміна параметрів адаптера» (рис. 58).

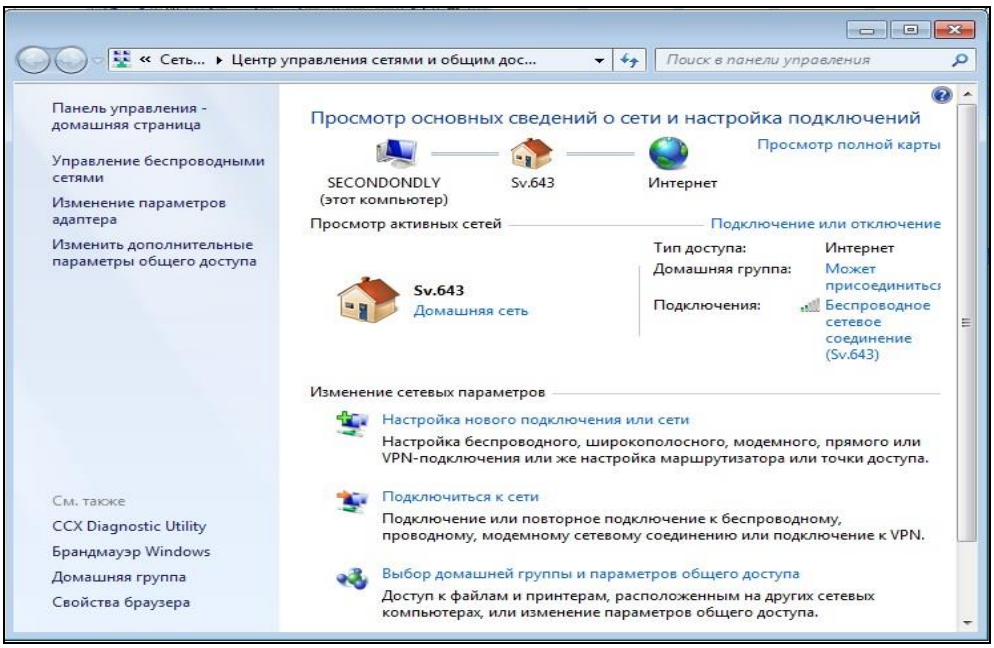


Рис. 58. Настройка параметрів адаптера

Клацніть правою кнопкою миші по значку бездротового підключення до мережі і виберіть пункт «Властивості» (рис. 59).

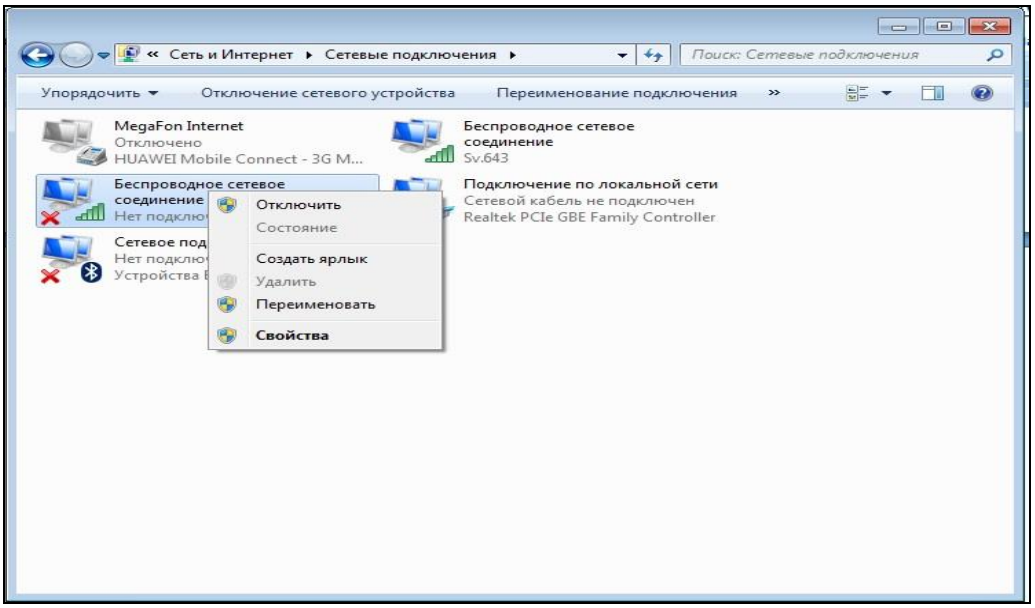


Рис. 59. Налаштування властивостей бездротового мережевого адаптера

Клацніть два рази по рядку «Протокол Інтернету версії 4 (TCP / IPv4)». Відзначте пункт «Використовувати наступний IP-адрес».

В полі IP-адреса: призначте IP адресу бездротовому адаптеру. IP адреса повинна бути унікальною і з тієї ж підмережі що IP адреса бездротового адаптера головного комп'ютера. У мережі не повинно бути пристроїв з однаковими IP. Натисніть «ОК» (рис. 60).

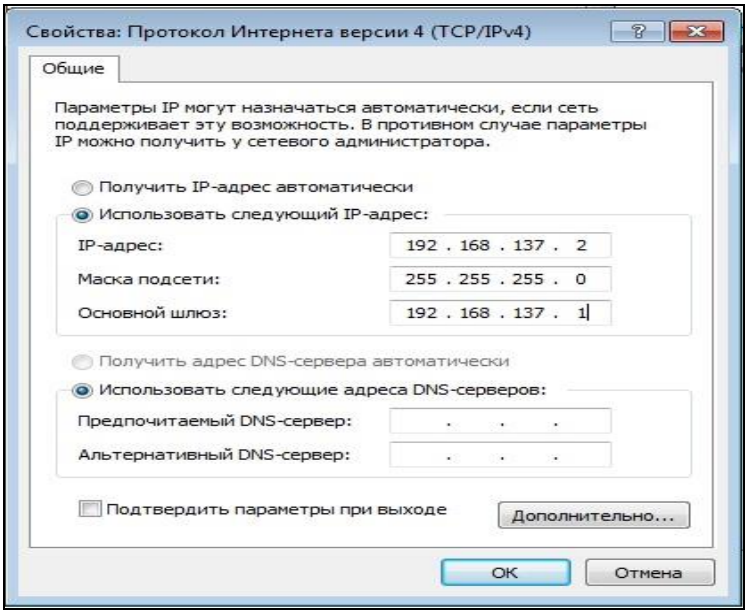


Рис. 60. Призначення адаптера мережного адреси

Клацніть по значку мережевого з'єднання. Клацніть два рази по вашій мережі. Введіть пароль. Натисніть «ОК» (рис. 61).

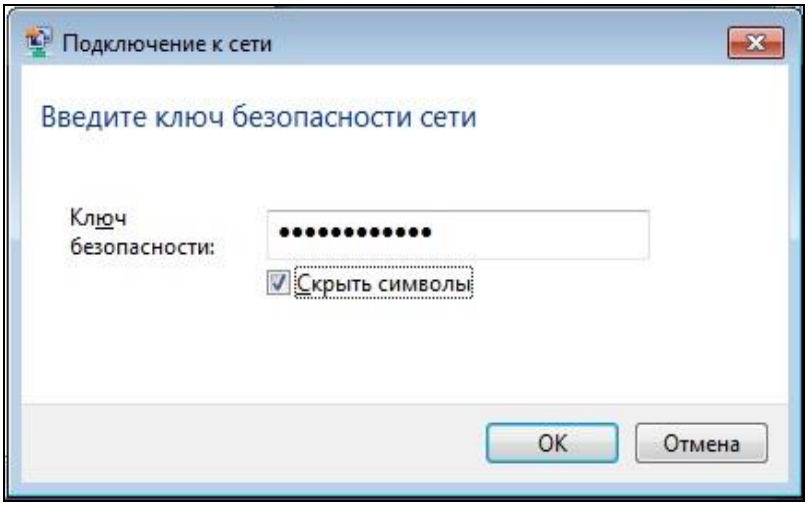


Рис. 61. Створення ключа безпеки

Щоб передавати дані через мережу між комп'ютерами по мережі потрібно зробити ваші диски доступними по локальній мережі і відкрити доступ до них. Відкрийте «властивості» потрібного вам диска, відкрийте вкладку доступ і відзначте «відкрити загальний доступ до папки», вкажіть диск. Далі натиснути «ОК», після чого доступ буде відкритий (рис. 62).

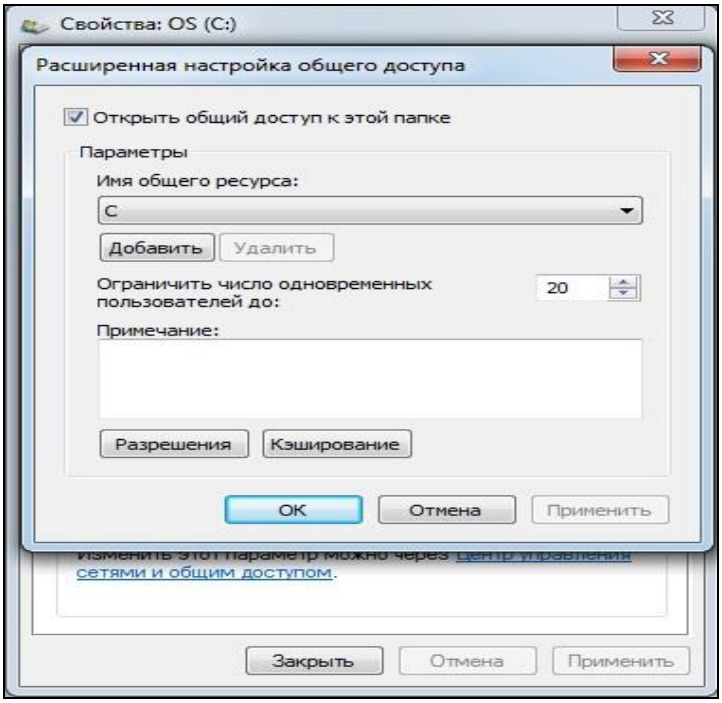


Рис. 62. Визначення характеристик доступу

Завдання на лабораторну роботу

Оформіть звіт по лабораторній роботі, опишіть виконання вправ. Виконати таблиці, які ілюструють швидкості передачі даних.

Лабораторна робота 10. Введення в мережеву безпеку, усунення неполадок мережі

Мета роботи: набуття навичок усунення мережевих проблем і вирішення питань мережевої безпеки.

Теоретичні відомості

Для того щоб убезпечити ваш ПК, підключений до локальної мережі, практично завжди слід використовувати файрвол.

Файрвол (від англійського Firewall) - це програма, яка контролює передачу даних між комп'ютером і мережею. Причому, файрвол може стежити як за трафіком локальної мережі, так і за даними, якими ваш комп'ютер обмінюється з Інтернетом. Найактуальніше використання файрволів при роботі в Інтернеті.

Слід пам'ятати, що комп'ютер, підключений до практично будь-якої локальної мережі (за винятком, мабуть, маленької "кімнатної" мережі), знаходиться під загрозою несанкціонованого вторгнення.

А це означає, що використання файрволу на такому комп'ютері обов'язково. Строго кажучи, навіть хороший файрвол, випущений відомою фірмою, не дає стовідсоткової гарантії безпеки вашого ПК.

Практично будь-який файрвол можна обійти, практично будь-яка система безпеки може бути зламана. Тому, якщо на вашому ПК є щось критично важливе, інформація, знищення або крадіжка якої може дуже дорого вам коштувати - постарайтеся або зберігати таку інформацію на змінних носіях, або шифруйте її, створюйте резервні копії, які недоступні через мережу.

Рішення мережевих проблем

Іноді працююча мережа раптом починає давати збої. Файли копіюються занадто довго, а часом і зовсім не хочуть листуватися з машини на машину, учасники мережевої гри іноді перестають "бачити" один одного і так далі. У переважній більшості випадків причина таких дивацтв лежить десь на поверхні. Мабуть, найкраще, якщо зв'язку немає взагалі - таку мережеву несправність найлегше виявити, діагностувати і усунути.

Нижче наведена таблиця діагностики та усунення несправностей (табл. 1), за допомогою якої ви зможете швидко відновити працездатність вашої локальної мережі в разі відсутності зв'язку.

Таблиця 1.

Проблеми мережі і їх вирішення

Несправність	Можлива причина	Способи діагностики та усунення
Немає зв'язку між комп'ютерами (апаратні проблеми)	Несправний або відключен комутатор	Перевірте, чи включений коммутатор. Зазвичай про те, що на нього надходить живлення, сигналізує світлодіод на корпусі пристрою. Якщо вам не вдається включити комутатор - можливо, проблема полягає в блоці живлення (вони порівняно часто виходять з ладу) або в роз'ємі, яким кабель живлення з'єднується з пристроєм. Спробуйте замінити кабелі живлення і блок живлення.
	Поганий контакт в RJ-45 роз'ємі	Огляньте світлодіоди роз'ємів на комутаторі і мережевих картах комп'ютерів. Якщо світлодіод не горить - це значить, що мережева карта і комутатор не пов'язані. Спробуйте витягнути коннектор з RJ-45 раз'єма і вставити його знову, причому, виконайте цю операцію і на мережевій карті, і на комутаторі.
	Мережева карта нещільно вставлена в роз'єм	Нещільно закріплена мережева карта може "випо-

		взти" з слота PCI. Таке буває і тоді, коли недосвідчений користувач встановлює карту і забуває її закріпити. Для ідентифікації проблеми розкрийте системний блок і подивіться на карту - якщо добре видно позолочені контакти її роз'ємів і вона встановлена в роз'ємі нерівно - це значить, що нормально працювати картка не буде. Якщо карта дійсно відійшла - вставте її в роз'єм і зафіксуйте гвинтом.
	Несправність мережевої карти	Для того, щоб перевірити вашу мережеву карту, спробуйте замінити її іншою, завідомо справною, наприклад, взятою з іншого комп'ютера. Якщо справна карта працює в вашому комп'ютері, а вашу не вдається змусити працювати в іншому системному блоці, значить - міняйте мережеву карту.
	Пошкодження кабелю	Мережевий кабель може бути пошкоджений - особливо - в тих місцях, де він піддається механічним впливам. Якщо все інше виглядає справним, але зв'язок все ж не вдається

		налагодити - спробуйте замінити кабель. Пам'ятайте про те, що за стандартом кабелі відновленню не підлягають.
Немає зв'язку між комп'ютерами (програмні проблеми)	Неправильне налаштування драйверів мережевої карти, конфлікт пристроїв	У вікні Диспетчера пристроїв значок мережевої карти зображений зі знаком питання або знаком оклику. При перегляді інформації про пристрій видно, що його драйвери не встановлені. Для вирішення проблеми знайдіть відповідні драйвери для мережевої карти і встановіть їх. У наш час конфлікти пристроїв - рідкісна проблема. Але якщо це сталося. Скажімо, конфліктують тільки що встановлений в систему модем і мережева карта (це крім діагностичних повідомлень у вікні Диспетчера пристроїв може викликати самовільне перезавантаження ПК). Для вирішення проблеми вимкніть один з пристроїв від системи, налаштуйте інше, а потім підключіть і налаштуйте друге. Так само ви можете скористатися Безпечним режимом роботи Windows для вирішення

		цієї проблеми.
	Неправильна настройка файрвола	Перевірте, чи правильно налаштований ваш файрвол, при необхідності подивіться документацію до нього. Зверніть особливу увагу на налаштування роботи з локальним трафіком - тобто з даними, обмін якими йде по локальній мережі.
	Неправильне налаштування TCP/IP	Перевірте зв'язок за допомогою утиліти Ping. Спробуйте скористатися цією програмою, вказавши в якості параметра IP-адресу власного комп'ютера. Якщо в ході виконання тесту виникають помилки, це може означати, що система неправильно працює з TCP/IP, можливо, драйвер мережевої карти не підтримується системою, або протокол встановлений або налаштований з помилками. Спробуйте перевстановити драйвер мережевої карти, протокол TCP/IP.
	Неправильне налаштування робочої групи та імені комп’ютера	Якщо при перевірці зв'язку з комп'ютером утилітою Ping все виглядає нормально, але, в той же час ви не можете працювати з

		мережею, можливо, неправильно налаштовані імена комп'ютерів (що трапляється вкрай рідко) або імена робочих груп (комп'ютери, що належать до різних робочих груп не зможуть взаємодіяти через мережу). Для вирішення цієї проблеми або вручну відредагуйте імена робочої групи, або запустіть Майстер налаштування мережі.
Нестійкий зв'язок, велика кількість помилок	Електромагнітні завади	Можливо, поруч з вашими мережевими кабелями проходять лінії високої напруги або, кабель прокладений поблизу розподільних щитків, потужних електродвигунів і т.д. Для вирішення цієї проблеми або використовуйте кабелі, які краще захищені від завад, ніж ваші або прокладайте кабель так, щоб він був подалі від джерел випромінювання.
	Пошкодження кабелю або використання відновленого кабелю	Пошкодження кабелю призведе до втрати обміну даними по мережі, або до погіршення характеристик кабелю, і, як результат - до падіння швидкості і до появи помилок при

		передачі даних. Спробуйте використовувати замість проблемного кабелю завідомо справний. Якщо з використанням справного кабелю вам вдалося встановити якісний зв'язок - найкраще замінити несправний кабель новим.
	Неякісний обтиск, "деренчання" контактів	Якщо кабель неякісно обжатий, або роз'єм RJ-45 має будь-які пошкодження, може спостерігатися "деренчання" контактів, коли зв'язок періодично пропадає на короткі проміжки часу. Такий кабель найкраще обтиснути заново.
	Кабелі нестандартної довжини, нестандартні кабелі, 5 і більше комутаторів	Якщо ви використовуєте у вашій мережі кабелі нестандартної довжини (понад 100 метрів), або нестандартні кабелі, або використовуєте багато комутаторів для збільшення дальності зв'язку - будьте готові до виникнення проблем. Якщо зниження швидкості зв'язку вас влаштовує то ви можете нічого не міняти, якщо ні - спробуйте укладатися в стандарти або використовувати обладнання (зок-

		рема - оптоволоконное), яке відповідає вашим запитам.

Завдання на лабораторну роботу

Повторити теоретичний матеріал за темою лабораторного заняття.

Підготувати короткі доповіді на тему:

1. Основи шифрування.
2. Протоколи аутентифікації.
3. Електронний цифровий підпис.
4. Види мережевих атак.
5. Використання засобів мережевої безпеки у різних операційних системах.
6. Конфігурування міжмережевих екранів.
7. Реалізація IPSec.

Надати відповіді на тестові завдання.

1. Алгоритм, який використовує для шифрування два різні ключі (відкритий і закритий):

• алгоритм симетричного шифрування

• алгоритм асиметричного шифрування

• алгоритм використання контрольних сум

• алгоритм автентифікації

2. Процедура перевірки автентичності користувача операційної системи шляхом порівняння введеного ним пароля з паролем у базі даних користувачів – це…

• авторизація

• ідентифікація

• автентифікація

3. Інформація в електронній формі, приєднана до іншої інформації в електронній формі або іншим чином пов'язана з такою інформацією, яка використовується для визначення особи, яка підписала інформацію – це…

• відкритий ключ

• електронний цифровий підпис

• автентифікація

• електронний документ

4. Контроль і фільтрація мережевих пакетів, що проходять, відповідно до заданих правил є основною функцією…

• антивірусу

• операційної системи

• міжмережевого екрану

5. Набір протоколів для забезпечення захисту даних, що передаються за протоколом IP:

• FTP

• UDP

• TCP/IP

• IPSec

Підготувати відповіді на контрольні питання.

1. Як улаштований механізм роботи відкритих ключів?

2. Опишіть механізм роботи протоколу автентифікації Kerberos.

3. Які способи захисту від мережевих атак?

4. Навіщо використовуються міжмережеві екрани?

5. Які основні принципи роботи протоколу IPSec?

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Г.Г. Швачич, В.В. Толстой, Л.М. Петречук, Ю.С. Іващенко, О.А. Гуляєва, О.В. Соболенко Сучасні інформаційно-комунікаційні технології: Навчальний посібник. – Дніпро: НМетАУ, 2017. –230 с.

2. Редька І. Інформаційні технології. Основні якості сучасних інформаційних технологій. Матеріали Всеукраїнської науково-практичної конференції «Соціальні комунікації і нові комунікативні технології». Запоріжжя, 2017. С. 20-25.

3. Павлиш В.А., Гліненко Л.К., Шаховська Н.Б. Основи інформаційних технологій і систем: підручник. – Львів: Видавництво Львівської політехніки, 2018. – 620 с.

4. Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Чанишев Р.І. Офісні технології: навч. посіб. – Одеса: Фенікс, 2019. – 207 с.

5. Мирошниченко В.О. Використання сучасних інформаційних технологій: формування мультимедійної компетентності: навчальний посібник. – Київ: Центр навчальної літератури, 2017. – 296 с.

6. Сучасні мережеві технології: Навчально-методичний посібник для студентів-провізорів очної, заочної та дистанційної форм навчання / Рижов О.А., Андросов А.І., Іванькова Н.А. - Запоріжжя: [ЗДМУ], 2018 - 68 с.

Навчально-методичне видання

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

Методичні вказівки
до виконання лабораторних робіт
для студентів для студентів спеціальності 125 "Кібербезпека"

Укладачі: **Курченко** Олег Анастасійович,
Хлапонін Юрій Іванович

Комп’ютерне верстання *М.М. Власенко*

Підписано до друку 13.04.2023 Формат 60 х 84 1/ 16
Ум. друк. арк. 4,88. Обл.-вид. арк. 2,45.
Електронний документ. Вид № 59/ІІІ-17.

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб’єктів
видавничої справи ДК № 808 від 13.02.2002 р.