МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

Кафедра інформаційних технологій

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних та самостійних робіт
з дисципліни
«Комп'ютерні мережі»

для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»

Одеса 2020

УДК 004.7(075)

Укладач:

Задерейко О.В. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»,
протокол № 2 від 4 грудня 2020 р.

Рецензент:

Троянський О.В. – кандидат технічних наук, доцент, директор інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Одеського національного політехнічного університета.

Кухаренко С.В. – доцент, кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Розглянуто основні методи і засоби проектування, діагностики та експлуатації комп’ютерних мереж.Містить завдання до лабораторних та самостійних занять, які виконуються у комп’ютерному класів межах навчальної дисципліни.Призначено для студентів з метою закріплення лекційного матеріалу і підготовки до лабораторнихта самостійних занять з дисципліни «Комп'ютерні мережі».

Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Комп’ютерні мережі» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» / Уклад.: О.В.Задерейко. – О.: НУ «ОЮА», 2020. – 69 с.

ПЕРЕДМОВА

В методичних вказівках представлені основні методи і загальні підходи діагностики, налаштування і проектування комп'ютерних мереж з точки зору їх практичного використання.

Основне завдання методичних вказівок – дати студентам загальні систематизовані знання про принципи організації та структури комп'ютерних мереж різного призначення. У методичних вказівках розглянуто загальні поняття комп'ютерних мереж, їх архітектури, види топологій, використовувані для фізичного з'єднання комп'ютерів в мережі і способи адресації. Описуються правила і процедури побудови одноранговых і клієнт-серверних мереж, а також програмного забезпечення, що дозволяє виконувати стандартні операції з визначення різних мережевих параметрів віддалених комп'ютерів. Розглянуто методи тестування та перевірки працездатності комп'ютерних мереж.

В результаті виконання лабораторних і самостійних робіт студент повинен освоїти:

- методи діагностики TCP/ P і DNS;
- правила і методи налаштування статичної і динамічної адресації в мережах з одноранговой і клієнт-серверної архітектурою;
- методи поділу ресурсів в комп'ютерних мережах;
- правила і методи налаштування символьної адресації в комп'ютерних мережах;
- правила і методи дозволу адрес в IP-мережах;
- принципи використання програмного забезпечення з визначення мережевих параметрів віддалених хостів;
- застосування ехо-запиту як засобу діагностики мережі.

ЗМІСТ

Перелік тем лабораторних занять та самостійних робіт

Тема 1. Загальні принципи функціонування комп‘ютерних мереж

Лабораторна робота 1. Аналіз мережевих підключень в операційних системах

Тема 2. Комунікаційна структура комп‘ютерних мереж

Лабораторна робота 2. Діагностика стеку протоколів TCP/IP

Лабораторна робота 3. Організація комутації мережевих інтерфейсів персонального комп'ютера

Лабораторна робота 4. Організація і настроювання локальних мереж

Тема 3. Маршрутизація в комп‘ютерних мережах

Лабораторна робота 5. Аналіз мережевого трафіку локальних комп‘ютерних мереж

Лабораторна робота 6. Аналіз ARP-трафіка в локальних мережах

Лабораторна робота 7. Аналіз DNS трафіка в локальних мережах

Лабораторна робота 8. Принципи організації IP-підмереж

Лабораторна робота 9. Принципи організації файлового обміну в комп’ютерних мережах

Самостійна робота 1. Логічна організація локальних комп’ютерних мереж

Самостійна робота 2. Імітаційне моделювання комп’ютерних мереж в Cicso Packet Tracer.

Самостійна робота 3. Проста адресна маршрутизація в комп‘ютерних мережах

Самостійна робота 4. Керування статичною маршрутизацією в комп'ютерних мережах

Самостійна робота 5. Імітаційне моделювання статичної маршрутизації в комп'ютерних мережах

ТЕМА 1. ЗАГАЛЬНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ КОМП‘ЮТЕРНИХ МЕРЕЖ

ЛАБОРАТОРНА РОБОТА № 1

АНАЛІЗ МЕРЕЖЕВИХ ПІДКЛЮЧЕНЬ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Мета заняття - ознайомитися основними мережевими сервісами і пов'язаними з ними портами. Навчитися використати інструмент **netstat** для отримання інформації про мережеві з'єднання операційної системи.

Навчальні питання:

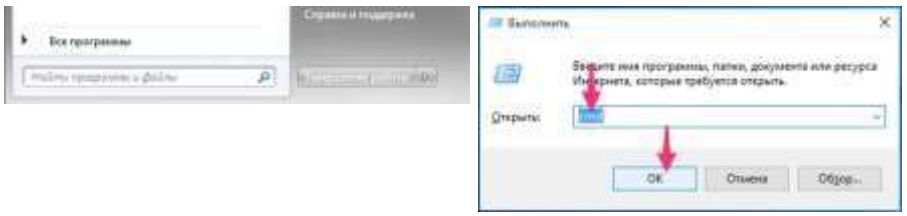
1. Системний інструмент NETSTAT - відображення статистики мережевих з'єднань.

2. Організація посторінкового виведення звітів про з'єднання.

3. Приклади запитів з'єднань для виводу на екран.

Запуск інструменту NETSTAT

Для запуску команди необхідно відкрити командний рядок в операційній системі Windows, як показано на рис.1.



***а*)** ***б*)**

Рис.1. Командний інтерфейс ОС Windows : *а*) Windows 7; *б*) Windows 10.

У командному інтерфейсі ОС Windows набрати команду **cmd.exe** і натиснути клавішу **Enter**. Відкриється вікно для введення команд (див. рис.2).

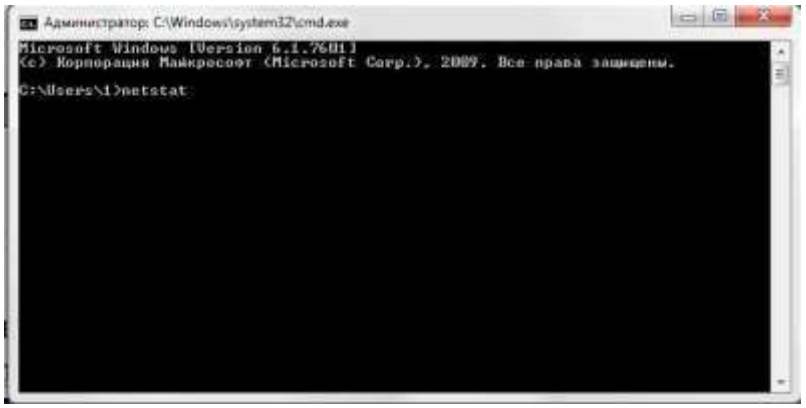


Рис.2. Командний рядок ОС Windows.

Для виконання кожного завдання в командному рядку необхідно послідовно вводити назву інструменту **NETSTAT** в необхідному форматі, згідно із завданням нижче. У разі потреби завершення виконання завдання необхідно натиснути комбінацію клавіш **Ctrl+C**.

ЗАВДАННЯ

Для збереження файлів звітів необхідно вибрати самостійно диск і каталог. Присвоїти каталогу «своє прізвище» англійською мовою.

1. Отримати інформацію про усі з'єднання операційної системи і зберегти всі отримані результати у відповідні файли звітів **nestat*XX.txt**. Символи в імені файлу «**XX**» замінити на порядковий номер в списку групи.

(**netstat -a > D:\zadereyko\nestatallXX.txt**).

1.1. Отримати список усіх мережевих з'єднань операційної системи її прикладного програмного забезпечення зі збереженням усіх отриманих результатів у файл **netstatsoftallXX.txt**.

Примітка: для гарантованого отримання списку програм необхідно перезапустити «командного рядку» с правами адміністратора.

(**netstat -a –b > D:\zadereyko\ netstatsoftallXX.txt**).

1.2. Отримати статистичні дані для обміну по протоколу Ethernet для усіх мережевих адаптерів зі збереженням усіх отриманих результатів у файл звіту **netstatethernetXX.txt**.

(**netstat –e > D:\zadereyko\netstatethernetXX.txt**).

1.3. Отримати сумарні статистичні дані про обмін даними через окремі мережеві інтерфейси зі збереженням усіх отриманих результатів у файл звіту **netstatintfaceXX.txt.**

(**netstat -e –v > D:\zadereyko\netstatintfaceXX.txt**).

1.4. Отримати сумарні статистичні дані для протоколів IP, ICMP, TCP, UDP зі збереженням усіх отриманих результатів у файл звіту **netstatprotocolXX.txt**.

(**netstat -e -s > D:\zadereyko\netstatprotocolXX.txt**).

1.5. Отримати список з'єднань TCP-портів зі збереженням усіх отриманих результатів у файл звіту **netstattcpportsXX.txt**.

(**netstat –a –t > D:\zadereyko\netstatcpportsXX.txt**).

1.6. Отримати таблицю маршрутизації ядра зі збереженням усіх отриманих результатів у файл **netstatyadroXX.txt**.

(**netstat –r > D:\zadereyko\netstatyadroXX.txt**).

1.7. Отримати статистику тільки TCP і UDP портів зі збереженням усіх отриманих результатів у файл звіту **netstattcpudpXX.txt**.

(**netstat –s -t > D:\zadereyko\netstattcpudpXX.txt**).

1.8. Отримати статистику усіх портів зі збереженням усіх отриманих результатів у файл звіту **netstatportsXX.txt**.

(**netstat –s > D:\zadereyko\netstatportsXX.txt**).

1.9. Отримати статистику відображення DNS-імен сервісів, що беруть участь в з'єднанні з операційною системою у файл звіту **DNSstatXX.txt**.

netstat -a -f > D:\zadereyko\DNSstatXX.txt.

netstat -n 5 | find /i "Established" - каждые 5 секунд отображать статистику по установленным соединениям.

2. Ініціювати мережеву активність в операційній системі:

- відкрити декілька веб-браузерів;
- у кожному веб-браузері відкрити по два довільні інтернет-ресурси.
- запустити будь-який месенджер.

2.1. Запустити **NETSTAT** в режимі безперервного виведення даних. Перенаправити виведення даних у файл звіту **outusername.txt**. Символи в імені файлу «**username**» замінити на своє прізвище англійською мовою.

2.2. Почекати 180 - 300 секунд.

2.3. Закрити браузери.

2.4. Завершити роботу інструменту **netstat**. (Комбінація клавіш **Ctrl+C**).

2.5. За даними всіх отриманих файлів визначити:

2.5.1. IP-адреси зовнішніх сервісів з якими було встановлено з'єднання;

2.5.2. Номери портів і домени зовнішніх сервісів, до яких було зафіксоване підключення;

2.5.3. Які клієнтські порти були задіяні;

2.5.4. Які програмні модулі виконували підключення до зовнішніх сервісів;

2.5.5. Загальну статистику по транспортних протоколах.

Примітка: До звіту слід заносити тільки зовнішні з'єднання зі активним станом.

3. Узагальнені результати аналізу отриманих файлів звітів представити у вигляді таблиці 1.

Таблиця 1.

Порядковий номер	**IP-адреси сервісів і номери портів, до яких зафіксовані зовнішні з'єднання**	**Назви сервісів, що відповідають IP-адресам сервісів, до яких зафіксовані зовнішні з'єднання**	**Клієнтські порти (операційної системи), до яких зафіксовані зовнішні з'єднання**	**Назви програмних модулів, що виконують зовнішні з'єднання**	**Транспортні протоколи, що мають участь у зовнішніх з'єднаннях**
1					
2					
…					

4. Проаналізувати отримані файли статистики мережевих з‘єднань. Зробити логічні висновки, стосовно отриманих результатів аналізу файлів статистики звітів і занести їх до звіту .

5. Оформити звіт з лабораторної роботи , який має містити:

5.1. Тему та мету лабораторної роботи.

5.2. Навчальні питання.

5.3. Стислий хід виконання роботи.

5.4. Висновки по виконаній роботі.

5.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

6. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які завдання дозволяє вирішувати інструмент **netstat**?
2. Як здійснюється безперервний вивід даних про з'єднання.
3. Як змінюється число з'єднань при виконанні додаткової активності програм?
4. Як отримати список усіх мережевих з'єднань операційної системи її прикладного програмного забезпечення?
5. Як отримати статистичні дані для обміну по протоколу Ethernet для усіх мережевих адаптерів?
6. Як отримати сумарні статистичні дані про обмін даними через окремі мережеві інтерфейси?
7. Як отримати список з'єднань TCP-портів?
8. Як отримати сумарні статистичні дані для мережевих протоколів?
9. Як отримати таблицю маршрутизації ядра?
10. Як отримати статистику по TCP і UDP з'єднанням?
11. Як отримати DNS-імена серверів, з яким встановлюються з'єднання?
12. Як отримати перелік програмних модулів, які встановлюють з’єднання?
13. По яких протоколах виконуються зовнішні з’єднання в операційній системі?
14. Які стани з’єднання існують?

15. Для чого використовується петлевий інтерфейс?
16. Яка адреса використовується без реальної передачі даних.

ТЕМА 2. КОМУНІКАЦІЙНА СТРУКТУРА КОМП‘ЮТЕРНИХ МЕРЕЖ

ЛАБОРАТОРНА РОБОТА № 2

ДІАГНОСТИКА СТЕКУ ПРОТОКОЛІВ TCP/IP

Мета роботи - вивчити можливості інструментів діагностики мережевих з'єднань і пошуку несправностей стеку протоколів TCP/IP.

Навчальні питання:

1. Системний інструмент IPCONFIG - перевірка та настроювання мережевої конфігурації.

2. Системний інструмент PING - перевірка доступності віддалених вузлів.

3. Системний інструмент TRACERT - перевірка трасування маршруту до заданого вузла локальної мережі або мережі Інтернет.

ЗАВДАННЯ

1. Використовуючи інструмент **IPCONFIG** отримати докладні відомості про всі секції мережевих з'єднань.

(**ipconfig /allcompartments /all**).

1.1. Заповнити нижче наведену таблицю отриманими даними.

Таблиця 1. Мережеві відомості для секції

ім'я комп'ютера	Основний DNS-суфікс	Тип вузла	IP-маршрутизація включена	WINS-проксі включений

Таблиця 2. Ethernet adapter. Підключення до локальної мережі

DNS-суфікс підключення	опис	Фізична адреса	DHCP включений	Автонастройка включена	Локальний IPv6-адреса	IPv4-адреса	Маска підмережі	Основний шлюз	DHCP-сервер	IAID DHCPv6	DUID клієнта DHCPv6	DNS-сервери	NetDIOS через TCP\IP	тунельний адаптер	опис	Фізична адреса

					на лу											

2. Використовуючи інструмент **IPCONFIG** отримати вміст кешу DNS-сервера операційної системи и зберегти отримані результати у файл звіту **displaydnsXX.txt**. Символи в імені файлу «XX» замінити на порядковий номер у списку групи.

(ipconfig /displaydns> D:\zadereyko\displaydnsXX.txt)

2.1. З отриманого файлу **displaydnsXX.txt** перенести адреси DNS-серверів в таблицю 3 і перенести її до звіту.

Таблиця 3.

Порядковий номер	Адреса DNS - сервера (До очищення DNS кешу)	Адреса DNS - сервера (Після очищення DNS кешу)
1		
.....		

2.2. Виконати очищення кешу DNS-сервера операційної системи.

(ipconfig /flushdns)

2.3. Повторно отримати вміст кешу DNS-сервера операційної системи и Зберегти отримані результати у файл звіту **displaydnsXXclean.txt**. Символи в імені файлу «XX» замінити на порядковий номер у списку групи.

(ipconfig /displaydns > D:\zadereyko\displaydnsXXclean.txt)

2.4. З файлу **displaydnsXXclean.txt** перенести адреси DNS-серверів в таблицю 3. Виконати порівняльний аналіз адрес DNS-серверів у кеші DNS операційної системи до і після його очищення. Висновки занести в звіт.

2.5. Звільнити адреса IPv4 для всіх мережевих адаптерів в операційній системі.

(ipconfig /release)

2.6. Перевірити наявність підключення до мережі з доменним простором Інтернету.

2.7. Оновити адресу IPv4 для всіх мережевих адаптерів в операційній системі.

(ipconfig /renew)

2.8. Повторно перевірити наявність підключення до мережі з доменним простором інтернету. Зробити висновки і занести їх до звіту.

3. Перевірити правильність конфігурації протоколу TCP/IP в операційній системі локального комп'ютера. Для цього необхідно задати в командному рядку адресу петлі зворотного зв'язку (loopback address).

(ping 127.0.0.1)

3.1. Отриманий результат у вигляді скріншоту внести до звіту. Проаналізувати отримані результати, зроблені висновки занести до звіту.

3.2. Виконати нескінченний пінг віддаленого вузла.

(ping -t X.X.X.X)

Примітка: IP-адреса **X.X.X.X** задається за погодженням з викладачем. Тривалість пінгування витримати не більше 20 секунд.

3.3. Отриманий результат пінгування у вигляді скріншоту внести до звіту. Проаналізувати отриманий результат, зроблені висновки занести до звіту.

3.4. Визначити «ім'я вузла/доменне ім'я» при пінгуванні публічної IP-адреси.

(ping -a X.X.X.X)

Примітка: IP-адреса **X.X.X.X** задається за погодженням з викладачем.

3.5. Заповнити таблицю 4 отриманими даними і помістити її до звіту.

Таблиця 4.

Публічна IP-адреса	**Ім'я вузла / Доменне ім'я**

3.6. Виконати трасування маршруту до сайту відповідно до свого варіанту в таблиці 5.

Таблиця 5

Порядковий номер в групі	Адреса домену
1.	microsoft.com
2.	google.com
3.	instagram.com
4.	linkedin.com
5.	facebook.com
6.	duckduckgo.com
7.	baidi.com
8.	yahoo.com
9.	bing.com
10.	altavista.com
11.	pinterest.com
12.	lycos.com
13.	naver.com
14.	qwant.com
15.	ask.com

3.7. Отриманий результат трасування маршруту в вигляді скріншоту внести до звіту. Проаналізувати отримані результати, зроблені висновки занести до звіту.

4. Оформити звіт з лабораторної роботи , який має містити:

4.1. Тему та мету лабораторної роботи.

4.2. Навчальні питання.

4.3. Стислий хід виконання роботи.

4.5. Висновки по виконаній роботі.

4.6. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

5. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Для яких цілей застосовується інструмент *ping*?
2. Які завдання дозволяє вирішити інструмент *tracert*?
3. Яку інформацію дозволяє витягти тестування адреси петлі зворотного зв'язку?
4. Яку інформацію дозволяє виявити порівняльний аналіз DNS кешу операційної системи до його очищення?

5. Яку інформацію про операційну систему можна витягти з кешу DNS операційної системи?

6. Яка базова інформація розміщується у кеші DNS операційної системи?

7. Для вирішення якої задачі використовуються команди *ipconfig /release* і *ipconfig /renew*?

ЛАБОРАТОРНА РОБОТА № 3

ОРГАНІЗАЦІЯ КОМУТАЦІЇ МЕРЕЖЕВИХ ІНТЕРФЕЙСІВ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

Мета роботи - вивчити способи безпосереднього підключення комп'ютерів через мережевий інтерфейс LAN і інтерфейс USB. Отримати практичні навички у виготовленні LAN кабелю для комутації мережевих інтерфейсів комп'ютерів.

НАВЧАЛЬНІ ПИТАННЯ:

1. Підключення «комп'ютер - комп'ютер» з використанням LAN-кабелю.

2. Підключення «комп'ютер - комп'ютер» за допомогою спеціального USB кабелю.

ЗАВДАННЯ

1. Здійснити підключення «комп'ютер-комп'ютер» через спеціальний USB кабель:

1.1. Вибрати за вказівкою викладача два комп'ютера і переконатися в їх вимкненому стані.

1.2. Підключити спеціальний USB кабель до робочих USB інтерфейсів комп'ютерів.

1.3. Включити комп'ютери і переконатися в установці драйверів з USB кабеля після завантаження операційної системи.

1.4. Запустити файловий менеджер **Easy Suite**.

1.5. На обох комп'ютерах переконатися в видимості файлових систем підключених комп'ютерів.

1.6. Виконати копіювання файлів з комп'ютера на комп'ютер за вказівкою викладача, попередньо зафіксувавши їх загальний розмір і час передачі.

1.7. Розрахувати середню швидкість передачі інформації і результати занести в звіт.

2. Здійснити підключення «комп'ютер-комп'ютер» через LAN кабель з трасуванням «кросовер».

2.1. Отримати у викладача: кабель, з'єднувальні щипці, коннектори.

2.2. Під керівництвом викладача виконати обтиск LAN кабелю за схемою «кросовер» (див. рис.3).

2.3. Виконати фізичне підключення зробленого LAN кабелю з трасуванням «кросовер» в мережеві карти обох комп‘ютерів.

2.4. Включити обидва комп‘ютера.

2.5. Виконати налаштування мережі на обох комп'ютерах:

2.5.1. Зайти в «**Панель управління**» => «**Центр управління мережами і загальним доступом**» => «**Зміна параметрів адаптера**» (комбінація клавіш **Win+R**, або командному рядку набрати команду **ncpa.cpl**).

2.5.2. У вікні мережеві підключення, вибрати «**Підключення по локальній мережі**» і клікнути по ньому правою кнопкою. У контекстному меню вибрати пункт **Властивості**. Відкриється вікно властивостей «**Підключення по локальній мережі**».

2.5.3. Двічі клацнути лівою кнопкою миші по пункту «**Протокол Інтернету версії 4 (TCP/IPv4)**».

2.5.4. На першому комп'ютері в поле **IP-адреса** вказати **192.168.1.1**. В поле **Маска підмережі** вказати **255.255.255.0**.

2.5.5. На другому комп'ютері в поле **IP-адреса** вказати **192.168.1.2**. В поле **Маска підмережі** вказати **255.255.255.0**.

2.6. Переконатися, що комп'ютери доступні за IP-адресами і видимі в мережевому оточенні.

2.7. Виконати передачу файлів з комп'ютера на комп'ютер:

2.7.1. Виконати копіювання файлів з комп'ютера на комп'ютер за вказівкою викладача, попередньо зафіксувавши їх загальний розмір і час передачі.

2.7.2. Розрахувати середню швидкість передачі (Мбіт/с) і занести її до звіту.

2.10. Розрахувати середню швидкість передачі файлів і отримані результати занести до звіту.

3. Оформити звіт з лабораторної роботи, який має містити:

3.1. Тему та мету лабораторної роботи.

3.2. Навчальні питання.

3.3. Стислий хід виконання роботи.

3.4. Висновки по виконаній роботі.

3.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

4. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Для чого може бути використано пряме підключення комп'ютерів?
2. Яка послідовність операцій при обтиску LAN кабелю конекторами RJ-45B?
3. Які особливості вибору LAN кабелю для прокладки Ethernet мереж?
4. Яка максимально можлива швидкість передачі для мережевого інтерфейсу Ethernet?
5. Яка реальна швидкість при здійсненні передачі з мережевого інтерфейсу Ethernet?
6. Яка максимально можлива швидкість передачі для мережевого інтерфейсу USB?
7. Як розрахувати реальну швидкість передачі для мережевого інтерфейсу?
8. Чому в полях **IP-адреса** необхідно вказувати адреси 192.168.1. і 192.168.1.2 для Ethernet з'єднання?
9. Чому в поле **Маска підмережі** необхідно вказувати адресу 255.255.255.0.?
10. Наведіть схему з трасування «кросовер» для LAN кабелю в чому її особливість ?
11. Чим відрізняється трасування LAN кабелю типу «кросовер» від звичайного LAN кабелю?

ЛАБОРАТОРНА РОБОТА № 4

ОРГАНІЗАЦІЯ І НАСТРОЮВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Мета роботи - вивчити структуру мережевого обладнання та способи його настроювання для організації підключення комп'ютерів у локальній мережі

Навчальні питання:

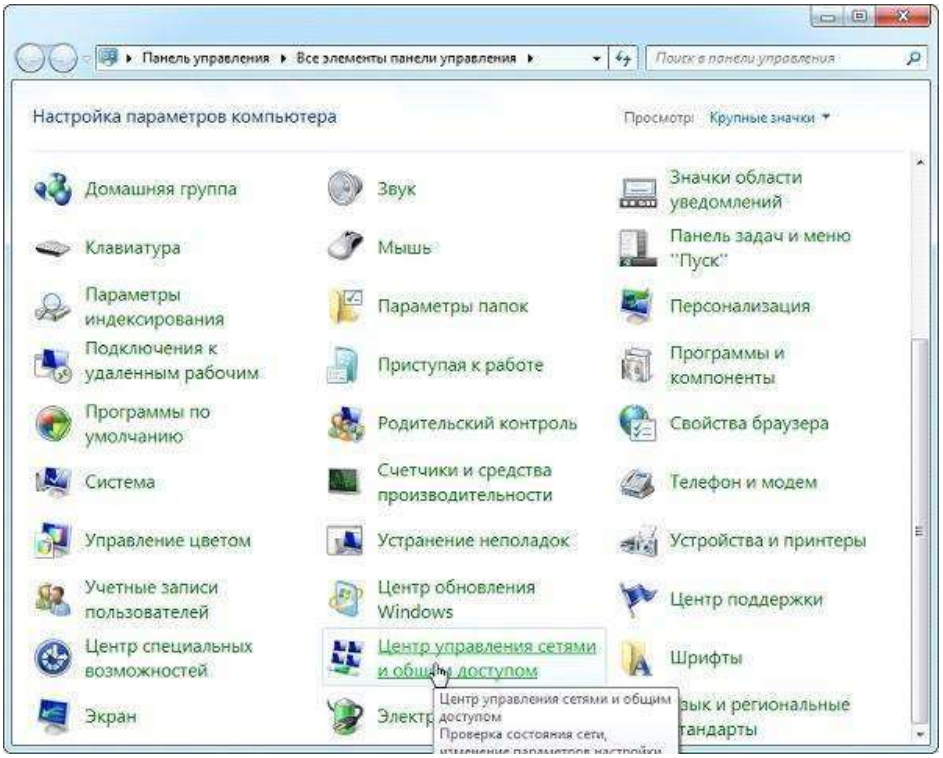
1. Загальна структура локальної мережі.

2. Устаткування локальної комп'ютерної мережі.

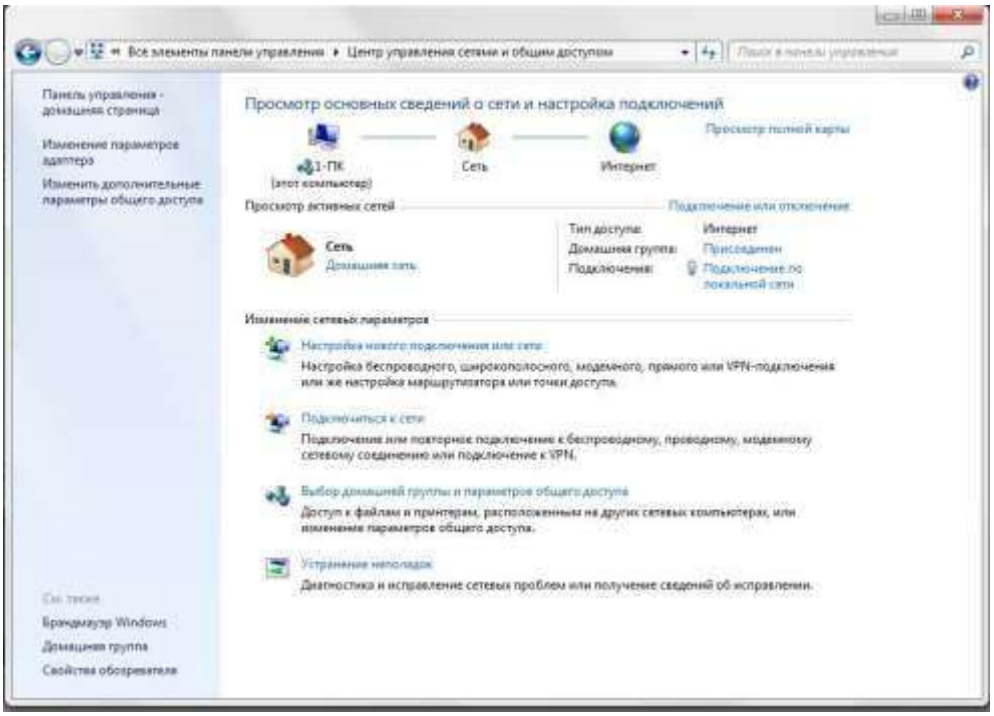
ЗАВДАННЯ

1. Виконати налаштування локальної мережі в операційній системі:

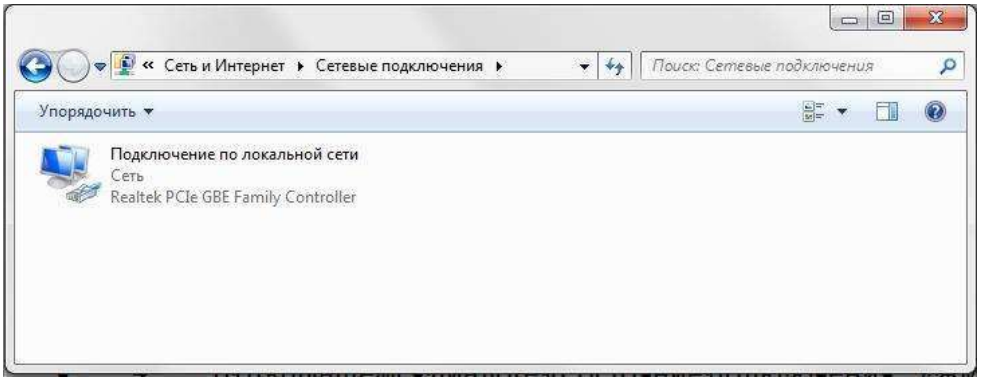
1.1. Відкрити панель керування: **Пуск** ® «**Панель управления**». Відкриється вікно:



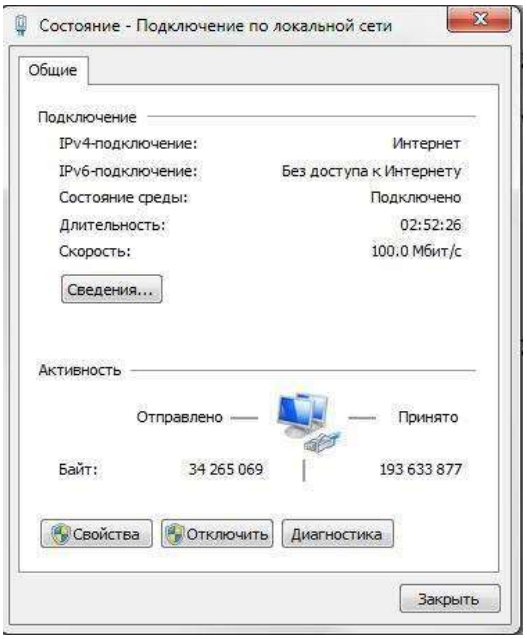
1.2. Вибрати панель **«Центр управления сетями и общим доступом».** Відкриється вікно:



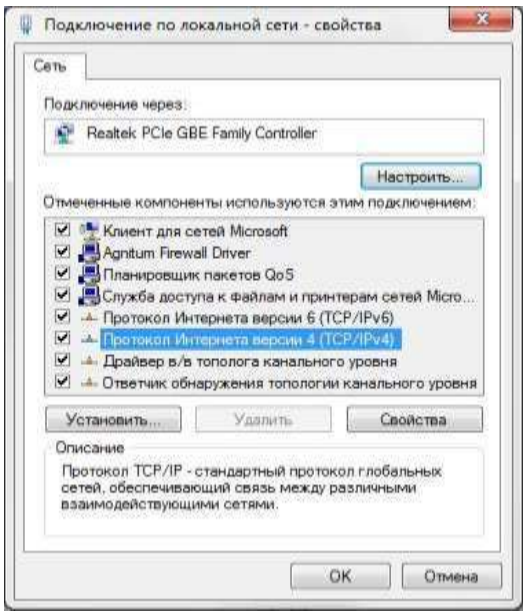
1.3. Обрати «**Изменение параметров адаптера**». Відкриється вікно:



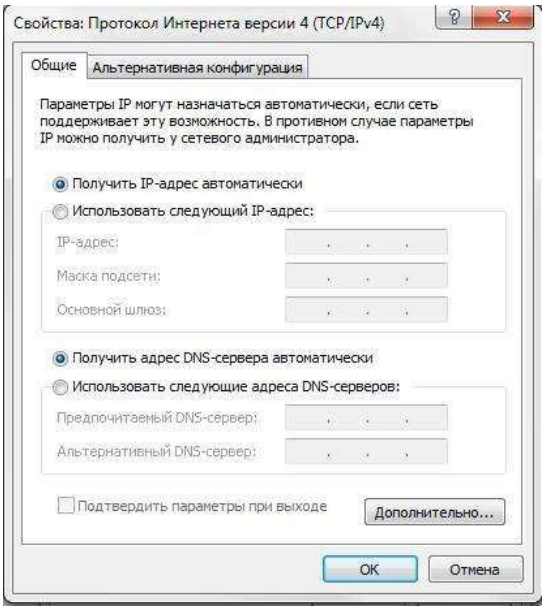
1.4. Виконати подвійний клік по з'єднанню «**Подключение по локальной сети**». Відкриється вікно:



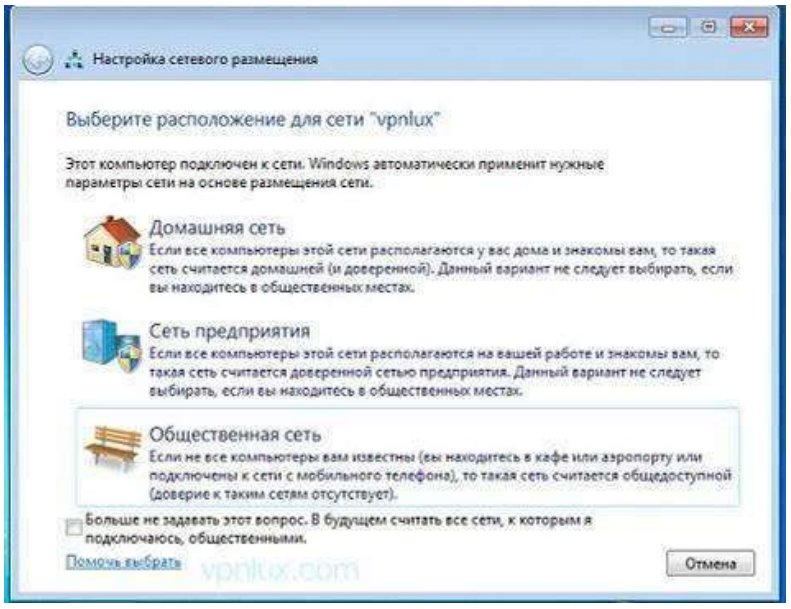
1.5. У вікні «**Состояние подключения по локальной сети**» натиснути кнопку «**Свойства**» для виконання конфігурації мережевого підключення. Відкриється вікно:



1.6. Виконати подвійний клік по «**Протокол Интернета версии (TCP/IPv4)**». Відкриється вікно:



1.7. Перевести маркер ● в положення «**Использовать следующий IP-адрес**». Ввести в поле **«IP-адрес:»** ® «**192.168.0.X»**, де **X** – порядковий номер у групі. В поле **«Маска подсети:»** ® «**255.255.255.0**» і натиснути кнопку **ОК**. Відкриється вікно:



4. Вибрати розташування для типу мережевого розміщення **«Домашняя сеть».**

Примітка: Операційна система пропонує три різновиди мережевого розташування: Домашня мережа – використовується для створення локальної мережі, куди входять довірені комп'ютери. Для такого підключення активізується функція мережевого виявлення, що дозволяє бачити інші пристрої, підключатися до них і використовувати файли, відкриті для загального використання з зазначеними привілеями.

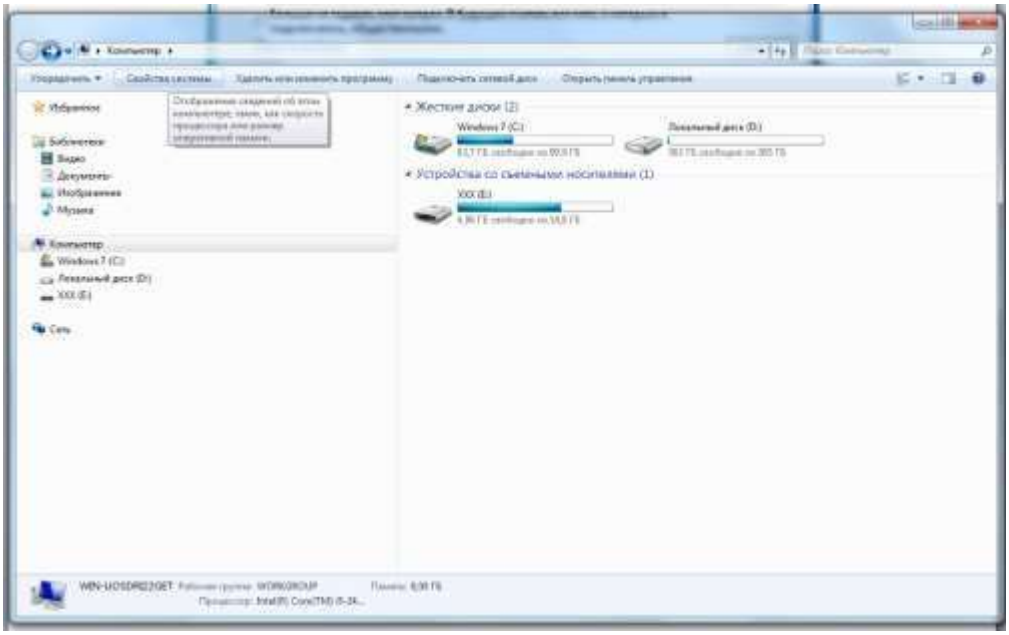
Робоча мережа – може бути застосовна для офісу, комп'ютерного класу і т.д. Між комп'ютерами робочої групи активовано виявлення, загальний доступ до файлів і пристроїв.

Публічна мережа – використовується в громадських місцях. Налаштування такої мережі приховують комп'ютери, підключені до неї, з метою підвищення безпеки та зменшення ймовірності стати жертвою зловмисників.

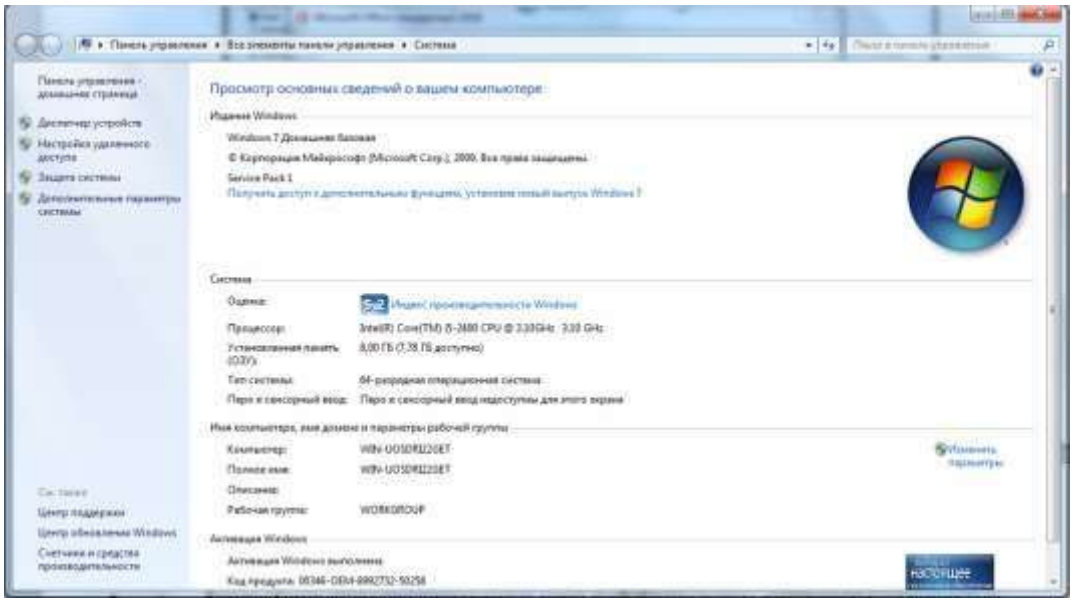
Для кожної мережі, рекомендуються настройки вбудованого фаейрвола і безпеки підключення, рекомендовані операційною системою за замовчуванням.

4. Виконати перевірку операційної системи, на приналежність до «**Домашней сети**».

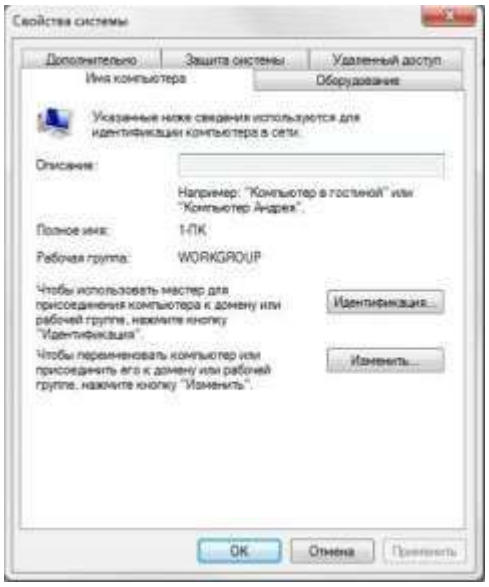
3.21. Викликати контекстне меню «**Мой компьютер**». Відкриється вікно:



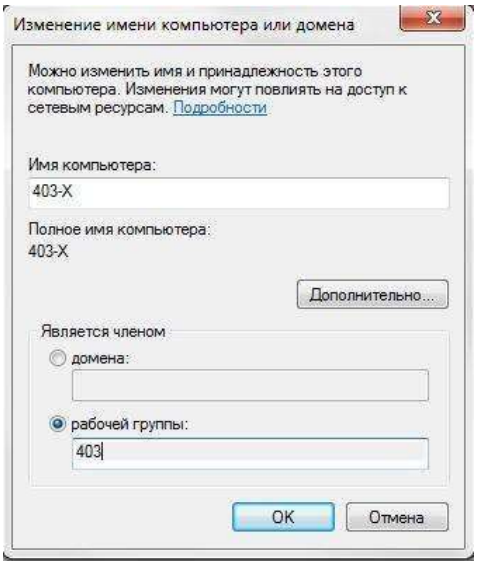
3.22. Вибрати у верхньому меню «**Свойства системы**» і натиснути клавішу мишки. Відкриється вікно:



3.23. Вибрати розділ «**Имя компьютера, имя домена и параметры рабочей группы**» і увійти до підрозділу «**Изменить параметры**». Відкриється вікно:

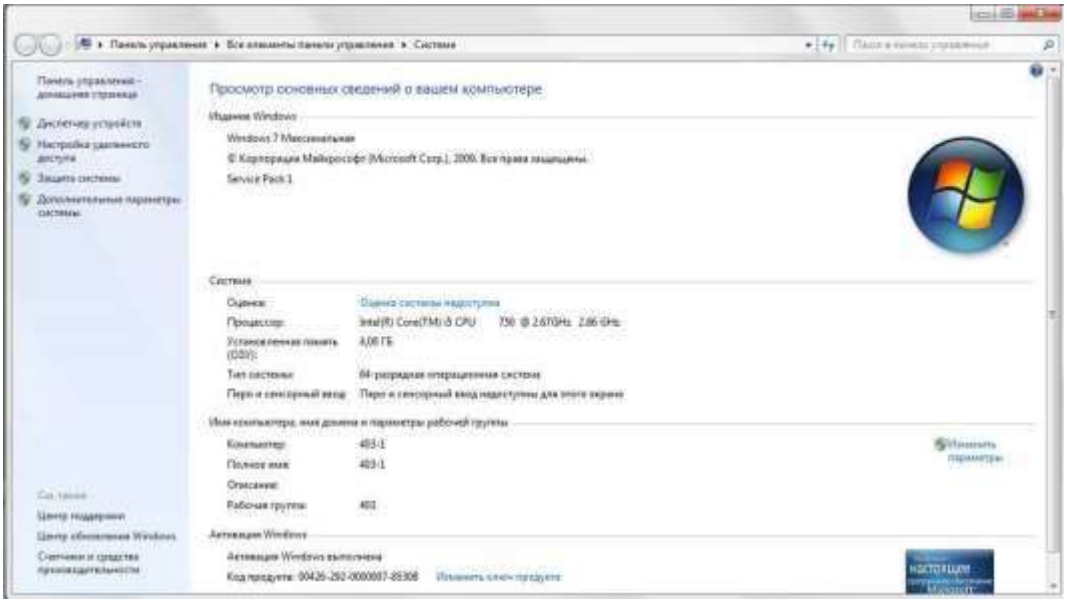


3.24. Виконати перейменування операційної системи. Для цього необхідно натиснути кнопку «**Изменить…**». Відкриється вікно:



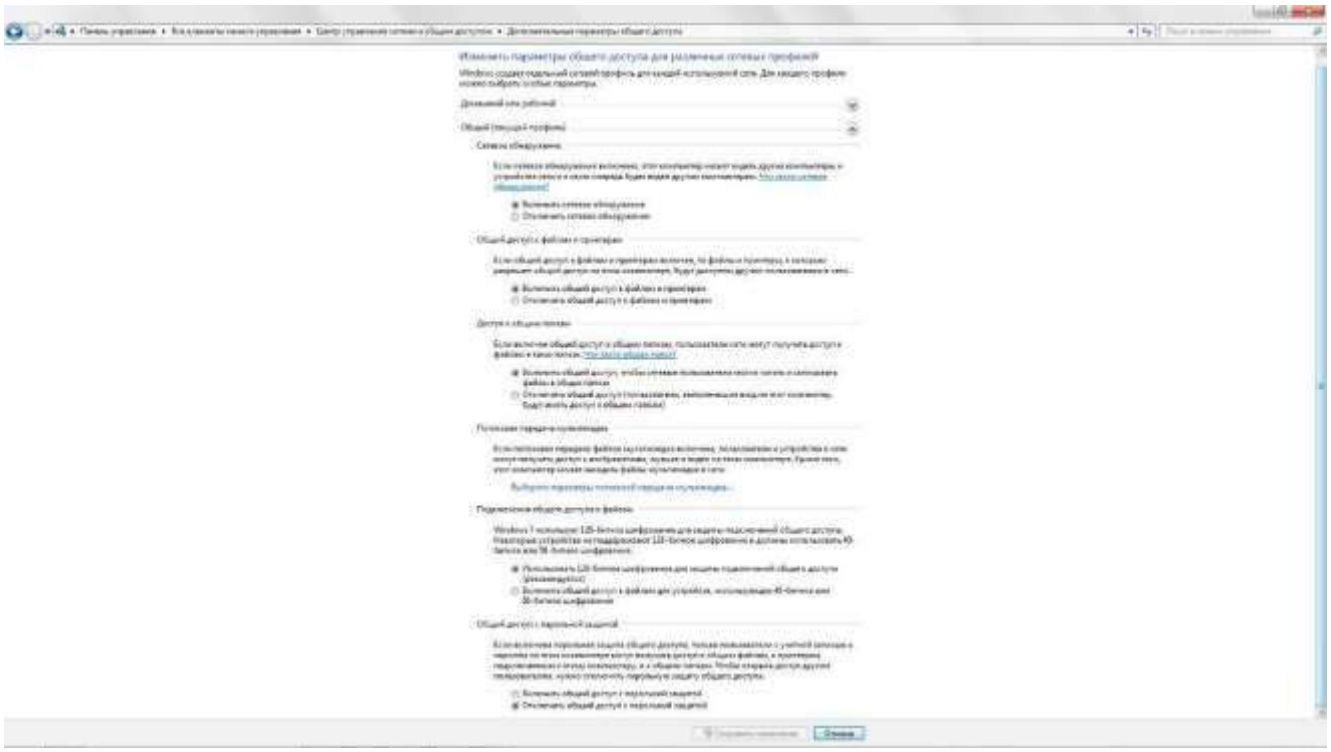
3.25. У полі «**Имя компьютера**» привласнити «**403-X**», де **X** – порядковий номер у групі. В полі «**Является членом**» ® «**рабочей группы**» привласнити «**403**». Натиснути кнопку «**ОК**» і, якщо буде потрібно, перезавантажити операційну систему.

3.26. Повторно виконати пункти **1.9.1** і **1.9.2**. Відкриється вікно:



3.2.1. Переконатися в правильності встановленого «**Имени Компьютера**» і «**Рабочей группы**».

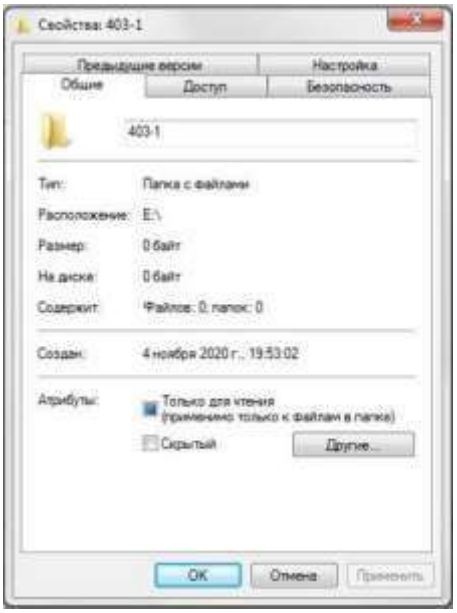
3.27. Обрати **«Панель управления»** ® **«Все элементы панели управления»** ® **«Центр управления сетями и общим доступом»** ® **«Дополнительные параметры общего доступа»**. Відкриється вікно:



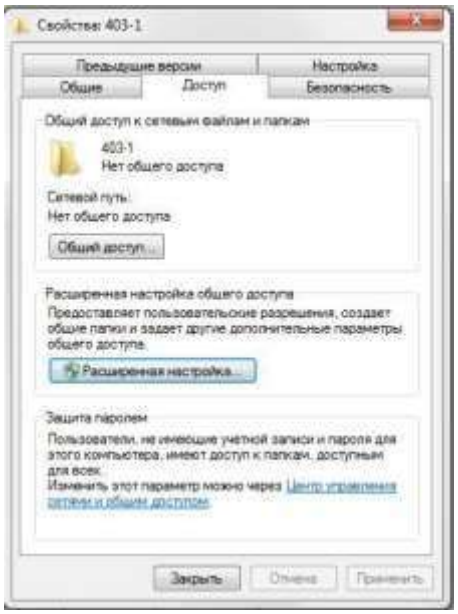
3.2.1. В розділі **«Общий доступ с парольной защитой»** встановити маркер в положення «**Отключить общий доступ с парольной защитой**» і натиснути кнопку **«Сохранить изменения».** Закрити вікно.

4. Відкрити диск **D.** Створити теку і привласнити їй назву **«403-X»,** де **X** – порядковий номер у групі.

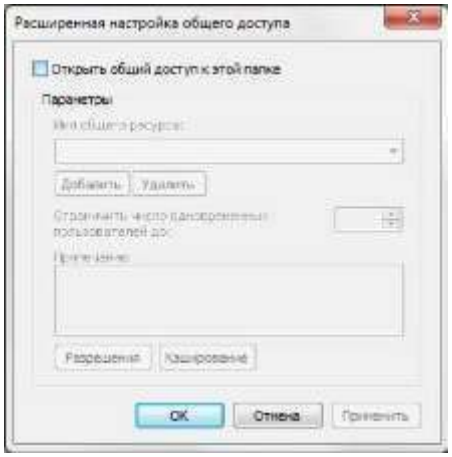
3.31. Встановити курсор миші на теку **«403-X»** і натиснути праву кнопку миші. Відкриється вікно:



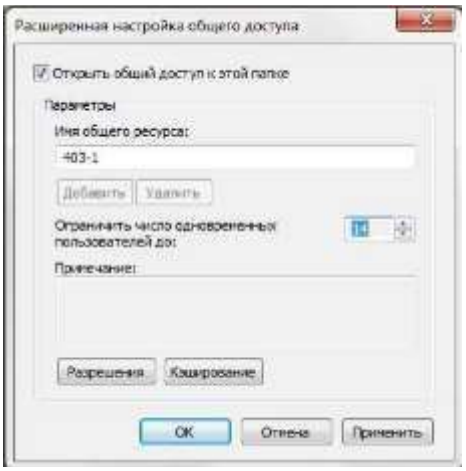
3.32. Перейти на вкладку **«Доступ».** Відкриється вікно:



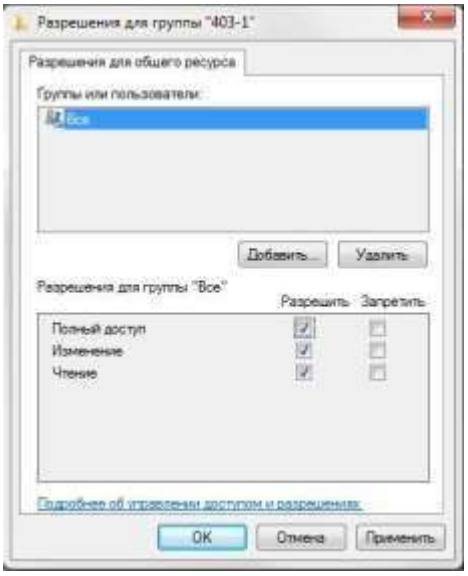
3.2.1. Натиснути кнопку **«Расширенная настройка».** Відкриється вікно:



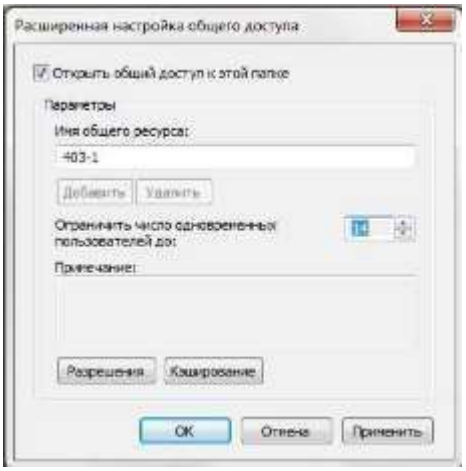
3.2.2. Встановити курсор миші в поле **«Открыть общий доступ к этой папке»** і натиснути ліву кнопку миші. Відкриється вікно:



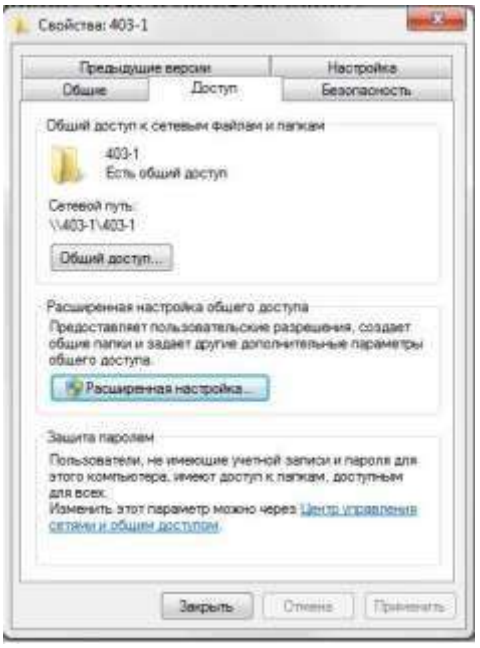
3.2.3. Вказати в полі **«Ограничить число одновременных пользователей до:»** рівним **14.** Встановити курсор миші на кнопку **«Разрешения»** і натиснути ліву кнопку миші. Відкриється вікно:



3.2.4. Встановити маркери в полях **«Полный доступ», «Изменение», «Чтение»** і натиснути кнопку **ОК.** Відкриється вікно:



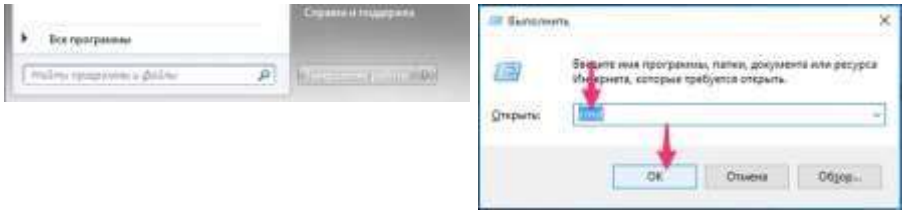
3.2.5. Натиснути кнопку **«Применить»** і кнопку **ОК.** Відкриється вікно:



3.2.6. Натиснути кнопку **«Закрыть»**.

4. Виконати перевірку налаштованого підключення комп'ютера, створеної локальної мережі:

4.11. Відкрити командний рядок операційної системи Windows, як показано на малюнку нижче.



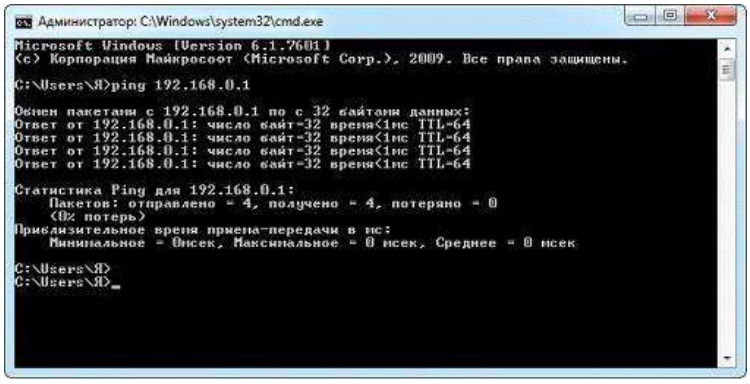
а) ***б)***

Рис.4.1. Командний інтерфейс ОС Windows : *а*) Windows 7; *б*) Windows 10.

4.12. У командному інтерфейсі набрати команду **cmd.exe** і натиснути клавішу **Enter**. Відкриється вікно для введення команд (див. рис. 2).

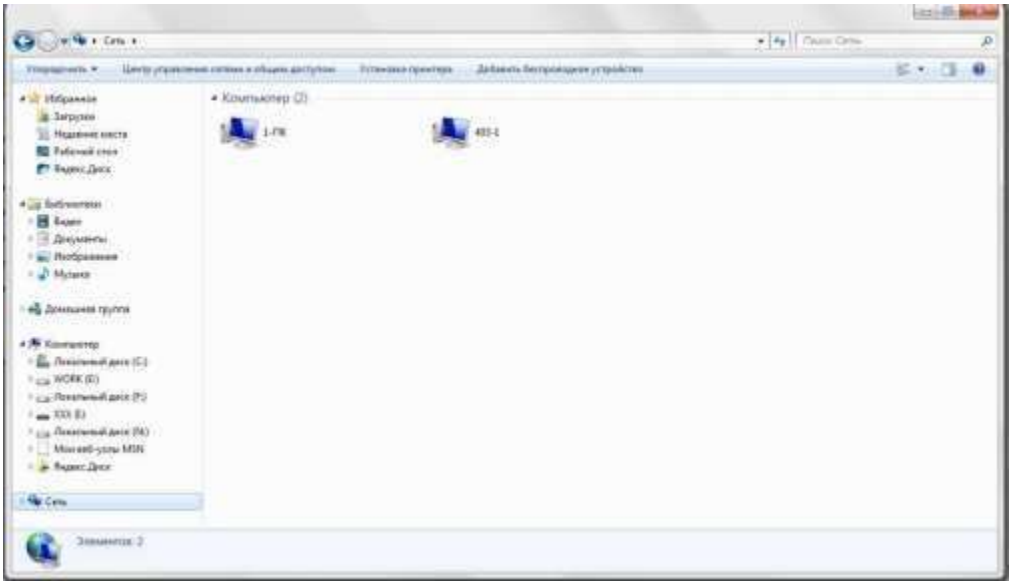
Рис. 2. Командний рядок ОС Windows.

4.13. Ввести команду **ping** з параметрами у вигляді IP-адреси іншого комп'ютера: ping 192.168.0.**X**». Відкриється вікно:



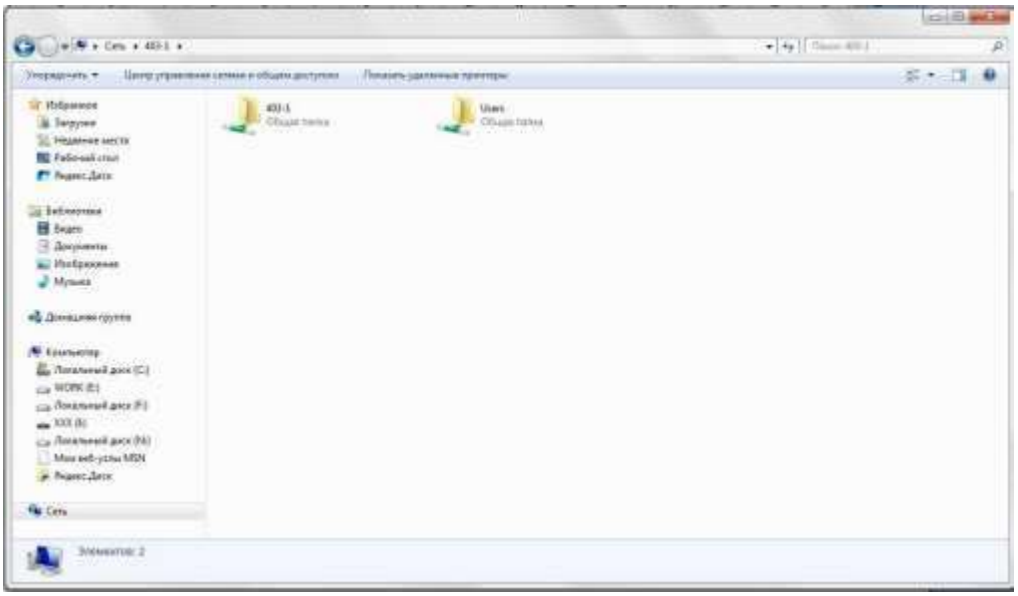
4.14. У разі відсутності втрат пакетів, закрити вікно командного інтерфейсу.

4.15. Відкрити «**Компьютер**» ® «**Сеть**». Відкриється вікно:

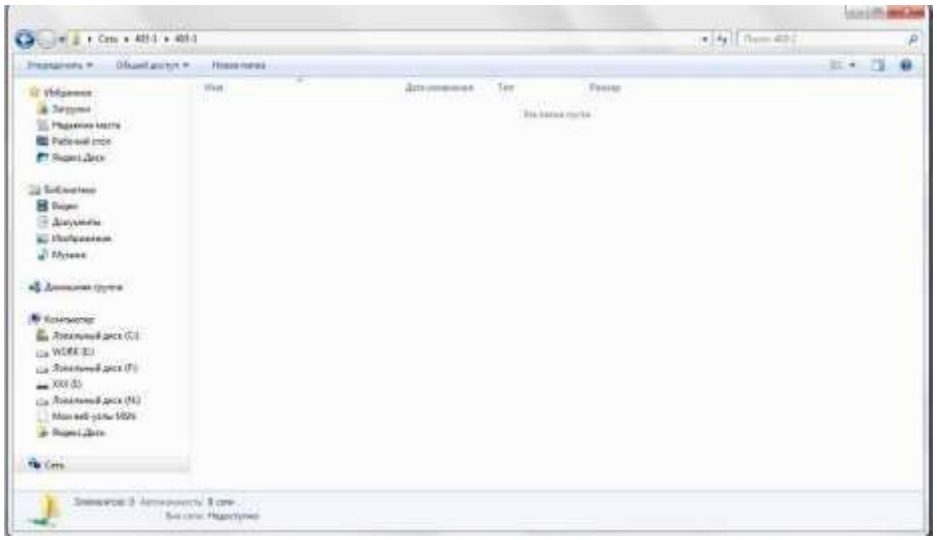


4.16. Переконатися в наявності комп'ютерів, підключених у створеній мережі **«4031», «403-2»**, …, **«403-X».**

4.17. Відкрити будь-який комп'ютер «**403-X**» і переконатися в наявності теки «**403X**». Для цього встановити курсор миші на комп'ютер «**403**» і натиснути ліву кнопку миші. Відкриється вікно:



4.18. Увійти в теку **«403-X».** Відкриється вікно:



4.19. Виконати копіювання і видалення будь-яких файлів у віддаленій теці комп'ютера «**403-X**» і переконатися в наявності повних прав доступу.

5. Оформити звіт з лабораторної роботи , який має містити:

5.1. Тему та мету лабораторної роботи.

5.2. Навчальні питання.

5.3. Стислий хід виконання роботи.

5.4. Висновки по виконаній роботі.

5.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

6. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Яке обладнання застосовується при побудові локальних комп'ютерних мереж?
2. Які завдання необхідно вирішити для організації роботи локальної комп'ютерної мережі?
3. В чому полягають відмінності мережевого комутатора (Switch) при організації локальних комп'ютерних мереж?
4. У чому полягають відмінності мережевого концентратора (Hub) при організації локальної мережі в якості активного мережного обладнання?
5. Чому кількість одночасних користувачів необхідно обмежити до 14?
6. Для чого необхідно відкривати загальний доступ до папок на комп'ютерах, з'єднаних прямим підключенням?
7. Для чого виконується команда **ping** з параметрами у вигляді IP-адреси іншого комп'ютера: ping 192.168.0.**X**»?

ТЕМА 3. МАРШРУТИЗАЦІЯ В КОМП‘ЮТЕРНИХ МЕРЕЖАХ

ЛАБОРАТОРНА РОБОТА № 5

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЛОКАЛЬНИХ КОМП‘ЮТЕРНИХ МЕРЕЖ

Мета роботи – виконати аналіз мережевого трафіку і пакетів за допомогою спеціалізованого програмного забезпечення

НАВЧАЛЬНІ ПИТАННЯ:

1. Методи і засоби аналізу мережевого трафіку

2. Базовий принцип роботи мережевих аналізаторів.

3. Основи роботи з аналізатором протоколів Wireshark.

4. Фільтри аналізатору протоколів Wireshark.

ЗАВДАННЯ

1. Проаналізувати трафік, захоплений програмою Wireshark:

1.1. Розглянути структуру пакета, вказавши призначення кожного заголовка.

1.2. Пояснити механізм інкапсуляції протоколів.

2. Виконати дослідження протоколу IP:

2.1. Запустити програму Wireshark.

2.2. Запустити процес захоплення трафіку.

2.3. Набрати в командному рядку:

tracert кінцевий_вузол

2.4. Зупинити захоплення трафіку.

2.5. В інформаційному полі розгорніть рядок, що містить «**Internet Protocol**». Витягніть наступну інформацію:

2.5.1. Проаналізуйте перший пакет ICMP Echo Request, відправлений комп'ютером: вкажіть IPадресу комп'ютера.

2.5.2. Наведіть значення поля, що визначає протокол верхнього рівня.

2.5.3. Скільки байт міститься в заголовку IP?

2.5.4. Скільки байт у полі даних?

2.5.5. Вкажіть значення TTL. Як змінюється це поле в різних **ICMP Echo Request**?

2.5.6. Яке значення міститься у полі «**Identification**»? Для чого використовується це поле?

3. Виконати дослідження фрагментації пакетів

3.1. Запустити програму Wireshark.

3.2. Запустити процес захоплення трафіку.

3.3. Набрати в командному рядку:

ping -l 2000 кінцевий_вузол

Примітка: (ключ -1 дозволяє вказати завантаження поля «Data» пакета в байтах).

3.4. Зупинити захоплення трафіку.

3.5. Витягніть наступну інформацію:

3.5.1. Проаналізуйте пакет ICMP Echo Request: чи має місце фрагментація вихідного пакета, яке поле на це вказує?

3.5.2. Проаналізуйте фрагменти IP-дейтаграми: яка інформація вказує, чи є фрагмент пакета останнім або проміжним?

3.5.3. Вкажіть кількість фрагментів вихідного пакета.

4. Виконати дослідження HTTP з'єднання: Basic HTTP GET/response

4.1. Запустити програму Wireshark.

4.2. Налаштувати фільтр (http)

4.3. Запустити процес захоплення трафіку.

4.4. Відкрити браузер і в командному рядку набрати https://wiki.wireshark.org/

4.5. Зупинити захоплення трафіку.

4.6. У списку захоплених пакетів знайдіть пару HTTP з'єднань (запит-відповідь): GET повідомлення і відповідь сервера. В інформаційному полі вибраного повідомлення розгорніть рядок, що містить HTTP, і вийміть інформацію:

4.6.1. Версія HTTP.

4.6.2. Прийняті браузером мови.

4.6.3. IP-адреса Вашого комп'ютера і сервера, з яким встановлено з'єднання.

4.6.4. Код стану HTTP і вказати що він означає.

4.6.5. Довжина тіла повідомлення.

Примітка: Вміст поля заголовка об'єкта **Content Length** вказує довжину тіла повідомлення в октетах (десяткове число), або в разі методу HEAD, розмір тіла об'єкта, який міг би бути посланий при запиті GET.

4.6.6. Протокол транспортного рівня, який використовує HTTP.

5. Виконати дослідження DNS з'єднання:

5.1. Очистити кеш DNS за допомогою утиліти ipconfig.

5.2. Набрати в командному рядку:

ipconfig /flushdns

5.3. Очистити кеш браузера.

5.4. Запустити програму Wireshark.

5.5. Налаштувати фільтр: ip.addr == ваша IP адреса.

5.6. Запустити процес захоплення трафіку.

5.7. Відкрити браузер і в командному рядку набрати https://www.ietf.org/

5.8. Зупинити захоплення трафіку.

5.9. У списку захоплених пакетів знайдіть пару DNS з'єднань. В інформаційному полі вибраного з'єднання розгорніть рядок, що містить DNS, і витягніть інформацію:

5.9.1. Вкажіть порти джерела/призначення для DNS-запиту і DNS-відповіді.

5.9.2. На яку IP-адресу відправлений DNS-запит?

5.9.3. Чи збігається ця адреса з адресою вашого DNS-сервера?

5.9.4. Вкажіть тип DNS-запиту.

5.9.5. Яка інформація міститься в полі «Answers» DNS-відповіді?

5.9.6. Витягніть IP-адресу, яка міститься в подальшому пакеті TCP SYN, який був відправлений Вашим комп'ютером.

6. Оформити звіт з лабораторної роботи , який має містити:

6.1. Тему та мету лабораторної роботи.

6.2. Навчальні питання.

6.3. Стислий хід виконання роботи.

6.4. Висновки по виконаній роботі.

6.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

7. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Яку інформацію можна витягнути, використовуючи фільтри програми Wireshark?
2. Яку інформацію можна отримати з DNS з'єднання?
3. Яку інформацію можна отримати з HTTP з'єднання?
4. Яку інформацію можна отримати з протоколу IP?

ЛАБОРАТОРНА РОБОТА № 6

АНАЛІЗ ARP-ТРАФІКА В ЛОКАЛЬНИХ МЕРЕЖАХ

Мета роботи – навчитися аналізувати мережевий трафік комп'ютера на прикладі роботи протоколу ARP.

Навчальні питання:

1. Протокол ARP

ЗАВДАННЯ

1. Виконати налаштування локальної мережі в операційній системі:

1. Переглянути вміст ARP кеша.

2. Виконати очищення ARP кеша.

3. Пропінгувати в локальній мережі будь-який доступний комп'ютер.

4. Проаналізувати **arp** трафік мережевого обміну за допомогою аналізатора мережевого трафіку Wireshark.

2. Приклад виконання лабораторної роботи.

1. Для перегляду ARP-кешу використовувати утиліту **arp** з параметром «**-a**»:

```
C:\>arp -a

Interface: 192.168.1.2 --- 0x10003

Internet Address      Physical Address      Type

192.168.1.1           00-15-e9-b6-67-4f     dynamic

192.168.1.6           00-01-4e-00-21-11     dynamic
```

З даного результату видно, що в кеші знаходиться 2 записи, що містять IP-адреси комп'ютерів і MAC-адреси їх мережевих адаптерів.

2. Вилучити заголовки з ARP-кешу командою:

```
arp -d <IP-адреса>
```

3.1. Запустити аналізатор мережі Wireshark. Для фільтрації ARP/RARP трафіку побудувати фільтр захоплення:

```
arp or rarp
```

3.2. Запустити захоплення трафіку.

3.3. Виконати команду ping за адресою IP:

```
C:\>ping 192.168.1.5
```

Отримаємо результат:

```
Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=64

Reply from 192.168.1.5: bytes=32 time<1ms TTL=64

Reply from 192.168.1.5: bytes=32 time<1ms TTL=64

Reply from 192.168.1.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.5:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

У зв’язку з тим, що на момент початку роботи утиліти ping в arp-кеш не було інформації про MAC-адресу запитаного мережевого адаптера комп'ютера, то спочатку система повинна виконати ухвалу цього MAC-адреса, згенерувавши ARP-запит і відіславши його в мережу широкомовним пакетом.

3.4. Зупинити захоплення трафіку і отримати типовий результат (рис.1).

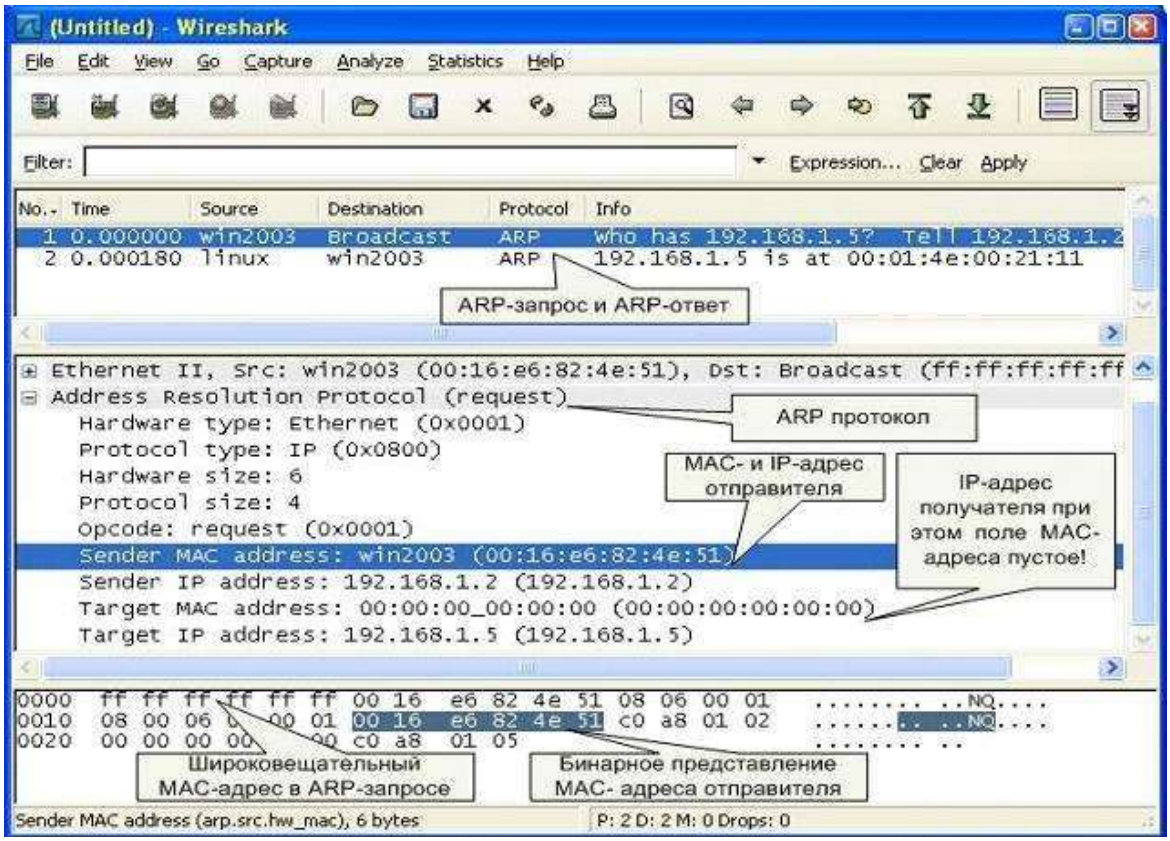


Рис.1. Результати захоплення ARP запиту (пакет №1).

3.4. Проаналізувати отримані пакети.

3.4.1. Розглянути ARP-запит (пакет №1). Виділити пакет курсором і отримати його вміст протоколів Ethernet і ARP в середньому вікні.

Примітка: У структурі пакетів, які використовуються в запитах і відповідях ARP виділяють наступні поля, що визначають параметри роботи протоколу:

Hardware type (HTYPE) – тип протоколу передачі даних (Ethernet, Token Ring і т. д.). Кожен з них має свій номер, який і зберігається в цьому полі. Так, наприклад, Ethernet має номер 0x0001.

Protocol type (PTYPE) – в цьому полі вказується код мережевого протоколу. Наприклад, для IPv4 буде записано 0x0800.

Hardware length (HLEN) – довжина фізичної адреси в байтах. Адреси Ethernet мають довжину 6 байт.

Protocol length (PLEN) – довжина логічної адреси в байтах. IPv4 адреси мають довжину 4 байта.

Opcode – код операції відправника: 1 – при запиті, 2 – при відповіді.

Sender hardware address (SHA) – фізичний адрес відправника.

Sender protocol address (SPA) – логічний адрес відправника.

Target hardware address (THA) – фізичний адрес одержувача. Поле порожньо при запиті.

Target protocol address (TPA) – логічний адрес одержувача.

У пакеті №1 (рис. 2) вказані MAC- і IP-адреси відправника («**Sender MAC address**» і «**Sender IP address**» відповідно). В даному випадку запит направлений на отримання («**Opcode: request**» – запит) MAC-адреси машини, у якій IP-адреса («**Protocol type: IP**») 192.168.1.5 («**Target IP address**»)

При цьому поле «**Target MAC address**» обнулено. У зв'язку з тим, що одержувач ARPзапиту на момент запиту не відомий, Ethernet-пакет відправляється широкомовним запитом всім машинам в даному локальному сегменті, про що сигналізує MACадреса Ethernetпакета «**ff:ff:ff:ff:ff:ff**»

Примітка: Слід звернути увагу, що пакет являє собою бінарну послідовність, і аналізатор Wireshark виконує перетворення полів з бінарного представлення в легкий для читання варіант.

Всі мережеві адаптери комп'ютерів в локальній мережі отримують пакет з ARPзапитом, аналізують його, а відповідь відсилає тільки той мережевий адаптер комп'ютера, чия IP-адреса відповідає IP-адресі в запиті.

3.4.1. Розглянути ARP-запит (пакет №1). Виділити пакет курсором і отримати його вміст протоколів Ethernet і ARP в середньому вікні (рис. 2).

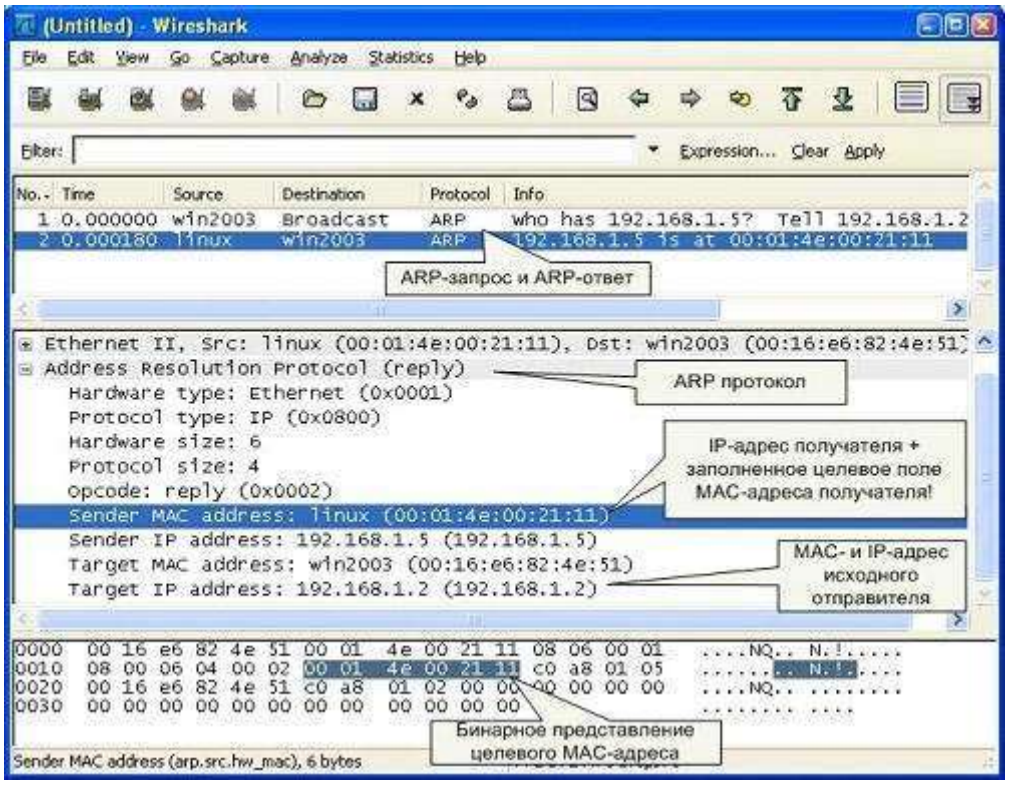


Рис. 2. Результати захоплення ARP відповіді (пакет №2).

Таким чином, пакет №2 є ARP-відповіддю. Це випливає з параметра поля **«Opcode: reply»**. Зверніть увагу, що даний пакет був відправлений саме тим мережним адаптером комп'ютера, на IP-адрес якого був вказаний командою C:\>ping 192.168.1.5, що підтверджує поле **«Sender IP address: 192.168.1.5»**. При цьому поле **«Sender MAC address»** заповнене значенням **«00:01:4E:00:21:11»**

Примітка: Зверніть увагу на поле «**Info**» в списку захоплених пакетів. Аналізатор значно полегшує аналіз мережевого трафіку, підказуючи призначення пакетів.

Переглянути повторно ARP-кеш на хості і звірити дані в ньому з даними, які були отримані з аналізу пакетів ARP-запит/відповідь (див. рис.1,2):

```
C:\>arp -a

Interface: 192.168.1.2 --- 0x10003

  Internet Address      Physical Address      Type

  192.168.1.5           00-01-4e-00-21-11     dynamic
```

4. Оформити звіт з лабораторної роботи , який має містити:

4.1. Тему та мету лабораторної роботи.

4.2. Навчальні питання.

4.3. Стислий хід виконання роботи.

4.4. Висновки по виконаній роботі.

4.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

5. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Що забезпечує ARP-протокол?
2. Поясніть призначення ARP-запиту.
3. Поясніть призначення RARP-запиту.
4. Поясніть типи існуючих записів в ARP-кеші.
5. Поясніть призначення полів ARP-запиту.
6. Поясніть призначення полів ARP-відповіді.

ЛАБОРАТОРНА РОБОТА № 7

АНАЛІЗ DNS ТРАФІКА В ЛОКАЛЬНИХ МЕРЕЖАХ

Мета роботи – виконати аналіз DNS трафіку і UDP пакетів за допомогою спеціалізованого програмного забезпечення

Навчальні питання:

1. Протокол транспортного рівня UDP.

ЗАВДАННЯ

1. Визначити і зафіксувати дані IP-конфігурації комп'ютера.

За допомогою виконання команду **ipconfig/all** на комп'ютері знайти і записати MAC- і IPадреси мережевого адаптера комп'ютера, IP-адресу вказаного шлюзу за умовчуванням і IPадресу DNScервера, вказаного для комп'ютера. Занести отримані дані в таблицю 1. Вони будуть використані при подальшому аналізі пакетів в наступних частинах завдання.

Таблиця 1. Дані конфігурації комп'ютера

IP-адреса	
MAC-адреса	
IP-адреса шлюзу за замовчуванням	
IP-адреса DNS-сервера	

2. Провести захоплення DNS запитів і DNS відгуків протоколу DNS.

Для цього необхідно настроїти програму Wireshark для захоплення пакетів запитів і відповідей DNS і провести захват пакетів транспортного протоколу UDP при обміні даними з DNScервером.

2.1. Запустити програму Wireshark для захоплення пакетів.

2.2. Видкрити **Interface List** (Список інтерфейсів) і вибрати інтерфейс, який пов'язаний з IP- і MACадресами комп'ютера, записаними в таблиці 2.

2.3. Натиснути кнопку **Почати захват пакетів,** щоб почати захоплення пакетів.

2.4. Відкрити веб-браузер і ввести в адресному рядку *www.google.com*. Натисніть клавішу **[Enter]**. Як тільки відкриється головна сторінка Google, натиснути кнопку **[Зупинити захват пакетів],** щоб зупинити захоплення даних.

3. Провести аналіз захоплених пакетів протоколів DNS і UDP відповідно до властивостей їх роботи.

3.1. Вивчити вміст пакетів протоколу UDP, створених при обміні даними з DNSсервером для IPадрес *www.google.com*. Для цього необхідно виконати наступні дії:

3.1.1. Відфільтрувати DNS-пакети. Для цього у головному вікні програми Wireshark введіть **dns** в рядку **Filter** (Фільтр).

Примітка: Якщо після застосування фільтру DNS ніякі результати не відображаються, закрийте веб-браузер і введіть у вікні командного рядка команду **ipconfig/flushdns**, щоб видалити усі попередні результати з кешу DNS. Перезапустіть захоплення даних програмою Wireshark.

Інформація про захоплені пакети представлена на рис. 2.

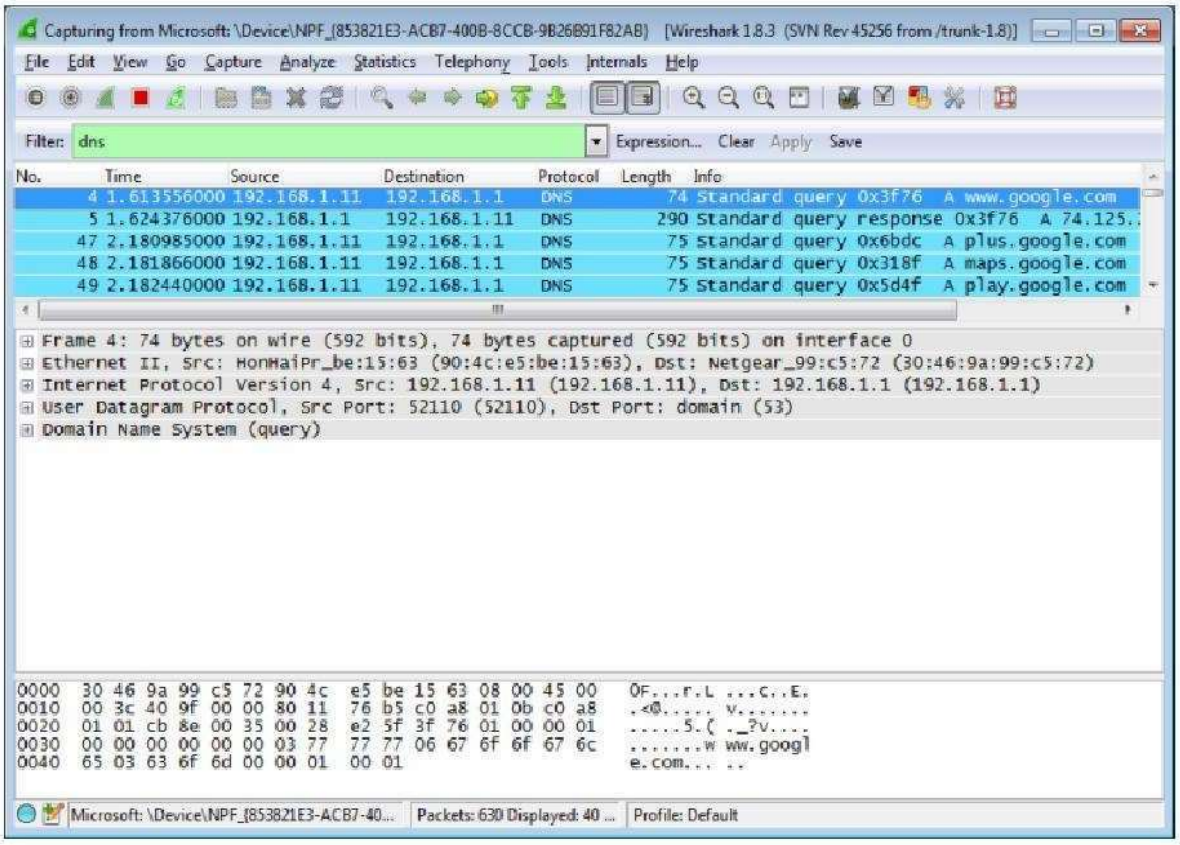


Рис. 2. Захоплені пакети DNS.

3.1.2. На панелі списку захоплених пакетів (верхній розділ) в головному вікні програми знайдіть пакет із словами **Standard query** (стандартний запит) і *www.google.com* (запит сайту *google.com*).

3.1.3. Вивчіть структуру протоколу UDP за допомогою DNS-запиту сайту *www.google.com*, захопленого програмою Wireshark. У цьому прикладі для аналізу вибраний захоплений кадр 4 на панелі списку захоплених пакетів. Протоколи в цьому запиті відображаються на панелі відомостей про пакети (**Details**, середній розділ) в головному вікні. Записи протоколу виділені сірим кольором (рис. 3).

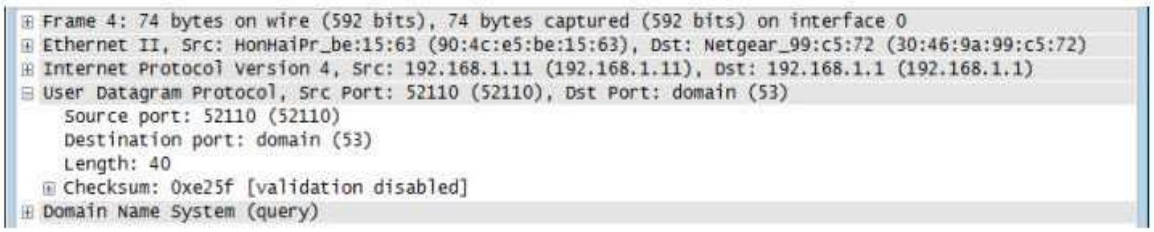


Рис. 3. Захоплений пакет DNS.

3.1.3.1. На панелі відомостей про пакети кадр 4 має 74 байти даних, як показано в першому рядку. Цю кількість байтів треба відправити в якості DNS-запиту на сервер, який відповідає IP-адресі сайту *www.google.com*.

3.1.3.2. Рядок **Ethernet II** містить MAC-адреси відправника і отримувача. MAC-адреса відправника належить Вашому комп'ютеру як відправнику DNS-запиту. MAC-адреса призначення – це шлюз за умовчуванням, оскільки це остання зупинка запиту перед виходом з локальної мережі. MAC-адреса джерела повинна співпадати з адресою Вашого комп'ютера, яка записана в таблиці 1.

3.1.3.3. У рядку інтернет-протоколу версії 4 захоплені дані IP-пакета показують, що IPадреса джерела цього DNS-запиту – 192.168.1.11, а IP-адреса призначення – 192.168.1.1. У цьому прикладі адреса призначення – це шлюз за умовчуванням. У цій мережі шлюзом за умовчуванням є маршрутизатор. IP-пакет і заголовок інкапсулюють сегмент UDP. Сегмент UDP містить DNS-запит у вигляді даних. Отримані дані занести в таблицю 2.

Таблиця 2. Дані DNS запиту

Пристрій	**IP-адреса**	**MAC-адреса**
Комп'ютер відправника DNSзапиту		
Шлюз за замовчуванням		

Заголовок UDP має тільки чотири поля: порт джерела, порт адресата, довжина і контрольна сума. Як показано нижче, довжина кожного поля в заголовку UDP складає всього 16 біт (рис. 4).

Рис. 4. Захоплений пакет DNS.

3.1.3.4. Розгорнути протокол **User Datagram Protocol** (UDP) на панелі відомостей про пакети, натиснувши на значок [+] (рис.5).

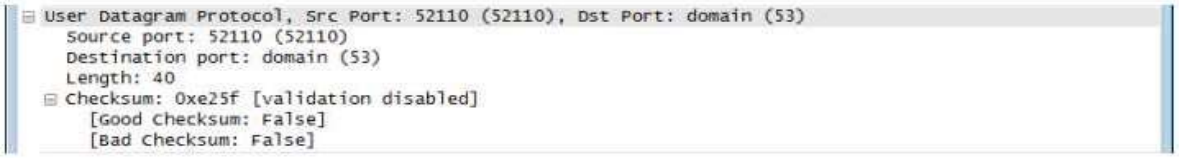


Рис. 5. Розгорнутий протокол UDP (User Datagram Protocol).

Зверніть увагу на те, що у вікні, що відкрилося, будуть тільки чотири поля. Номер порту джерела в цьому прикладі – 52110. Порт джерела був випадково згенерований Вашим комп'ютером з використанням зарезервованих номерів портів. Порт призначення – 53. Порт 53 – це загальновідомий порт, зарезервований для використання з DNS. DNS-сервери отримують DNS-запити від клієнтів через порт 53. У цьому прикладі довжина сегменту UDP складає 40 байт. З 40 байтів вісім складають заголовок. Інші 32 байти використовуються даними DNSзапиту. На рис. 6 виділені 32 байти даних DNS-запиту на панелі відображення пакету у вигляді послідовності байтів (нижній розділ головного вікна програми Wireshark).

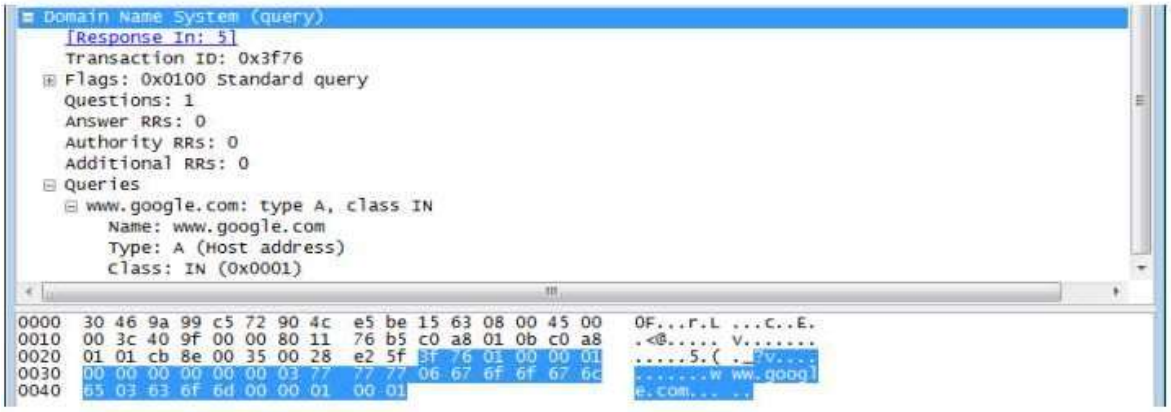


Рис. 6. Структура DNS-запиту.

3.1.3.5. Запишіть результати захоплення даних програмою Wireshark в таблицю 3.

Таблиця 3. Результати захоплення даних.

Розмір кадру	
MAC-адреса відправника	
MAC-адреса отримувача	
IP-адреса відправника	
IP-адреса отримувача	
Порт відправника	
Порт отримувача	

3.1.3.5. Зробити порівняльний аналіз даних в таблиці 1 і таблиці 3:

– чи співпадає IP-адреса відправника з IP-адресою комп'ютера, записаною в таблиці 1?

– чи співпадає IP-адреса отримувача з шлюзом за умовчуванням, записаною в таблиці 1?

4. Вивчити структуру протокола UDP за допомогою DNS-відгуку:

4.1. Вивчіть структуру протоколу UDP за допомогою DNS-відгуку з сайту *www.google.com*, захопленого програмою Wireshark. У прикладі для цього аналізу вибраний захоплений кадр 5 на панелі списку захоплених пакетів (рис. 7).

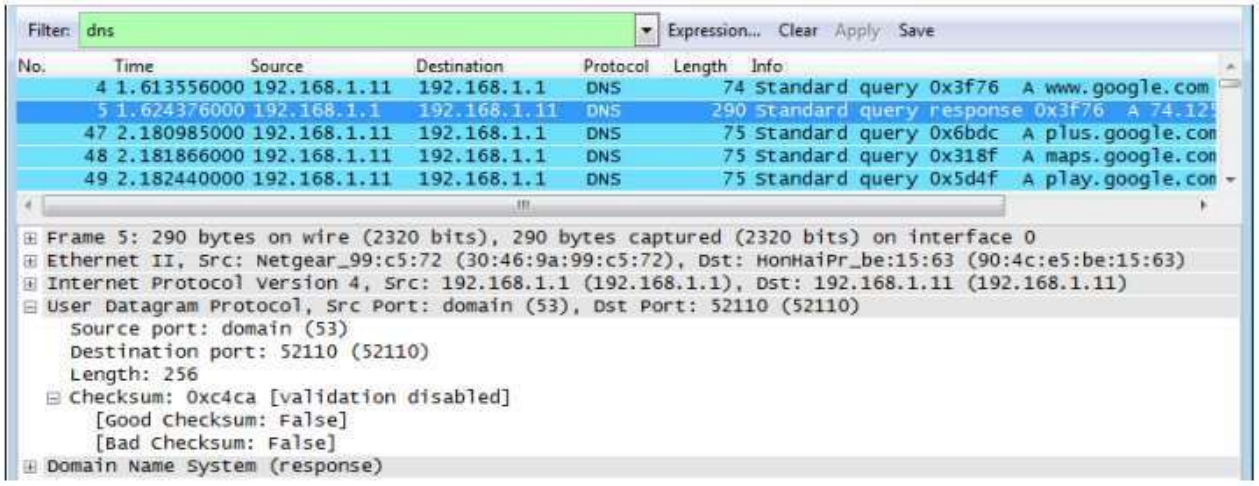


Рис. 7. Структура DNS-відгуку.

4.1.1. Визначити по кадру **Ethernet II** для DNS-відгука, з якого пристрою отримана МАСадреса відправника і який пристрій являється МАСадресою отримувача.

4.1.1.1. Розгорнути пункт **Domain Name System (responce)** на панелі відомостей про пакети, натиснувши на значок плюса **(+)** (рис. 8).

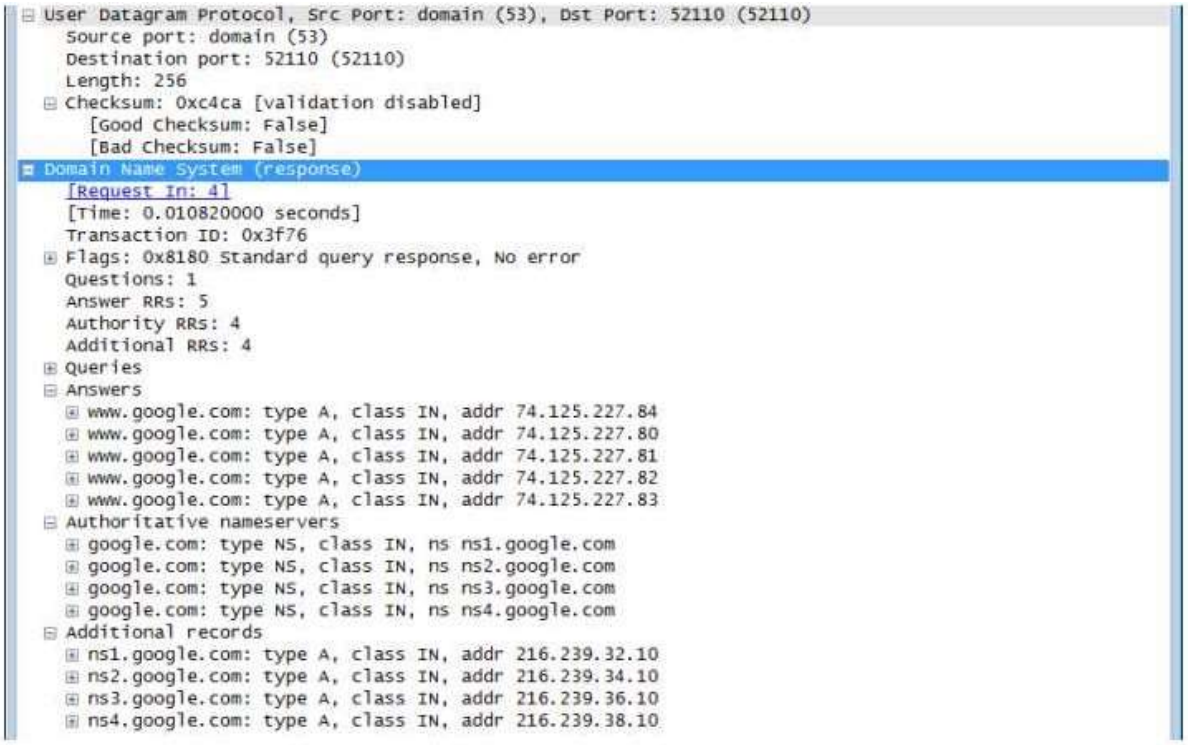


Рис. 8. Розгорнутий протокол DNS.

4.1.2. Визначити зміну в IP-адресах відправника і отримувача в IP-пакеті.

Зробити висновок – що сталося з ролями джерела і призначення локального вузла (комп’ютера) і шлюзу за умовчуванням?

4.1.3. У сегменті UDP ролі номерів портів також змінилися на протилежні. Номер порту призначення – 52110. Номер порту 52110 – це той же порт, який був згенерований комп'ютером при відправці DNS-запиту на DNS-сервер. Комп'ютер чекає DNS-відгук від цього порту. Номер порту призначення – 53. DNS-сервер чекає DNS-запита від порту 53, а потім відправляє DNSвідгук з номером порту джерела 53 відправнику DNS-запита. При аналізі DNS-запита звернути увагу на перетворені IP-адреси сайту *www.google.com*.

5. Оформити звіт з лабораторної роботи , який має містити:

5.6. Тему та мету лабораторної роботи.

5.7. Навчальні питання.

5.8. Хід виконання роботи.

5.9. Висновки по виконаній роботі.

5.10. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

6. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть послідовність роботи протоколу UDP.
2. Поясніть переваги використання протоколу UDP.
3. Поясніть складові протоколу UDP у частині DNS-відгуку.
4. Поясніть складові протоколу UDP у частині DNS-запиту.
5. Поясніть призначення MAC-адреси.
6. Для чого використовується команда ipconfig/flushdns?
7. Як визначити дані IP-конфігурації комп'ютера?

ЛАБОРАТОРНА РОБОТА № 8

ПРИНЦИПИ ОРГАНІЗАЦІЇ IP-ПІДМЕРЕЖ

Мета роботи – ознайомитися із загальними принципами організації IP-підмереж та засвоїти методики розбиття IP-мереж на підмережі.

НАВЧАЛЬНІ ПИТАННЯ:

1. Загальні принципи організації IP-підмереж.

2. Розбиття IP-підмереж на підмережі.

ЗАВДАННЯ

1. Для заданої IP-адреси мережі та маски (отримати таблицю 1 у викладача) визначити кількість підмереж, які входять у дану мережу, та кількість вузлів (IP-адрес вузлів) однієї підмережі.

2. Розбити IP-мережу на однакові підмережі (отримати таблицю 2 у викладача).

3. Визначити маску підмережі, префікс та кількість IP-адрес вузлів, які входять в одну під мережу.

4. Визначити загальну кількість IP-адрес вузлів у всіх підмережах.

3. Розбити IP-мережу на підмережі у кожній з яких функціонує задана кількість вузлів (отримати табл.3 у викладача).

4. Розбити IP-мережу на підмережі з використанням методу CIDR (отримати таблицю 4 у викладача).

5. Визначити префікс під мережі, CIDR-префікс та кількість під мережі IP-адрес вузлів.

6. Оформити звіт з лабораторної роботи , який має містити:

6.1. Тему та мету лабораторної роботи.

6.2. Навчальні питання.

6.3. Хід виконання роботи згідно з варіантом.

6.4. Висновки по виконаній роботі.

6.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи

7. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Дайте визначення IP-мереж).
2. Дайте визначення IP-підмережі.
3. Дайте визначення IP-супермережі.
4. Поясніть структуру IP-адреси 4версії.
5. Дайте визначення класового префіксу.
6. Дайте визначення класової маски.
7. Дайте визначення безкласового префіксу.
8. Дайте визначення безкласової маски.
9. Поясніть структуру IP-адреси мережі 4 версії при розподілу на підмережі.
10. Які умови необхідні для розподілу IP-мережі на підмережі.
11. Яка максимально можлива кількість підмереж існує для класів мереж A, B, C.
12. Дайте визначення CIDR-префіксу мережі.
13. Дайте визначення CIDR-маски мережі.

ЛАБОРАТОРНА РОБОТА № 9

ПРИНЦИПИ ОРГАНІЗАЦІЇ ФАЙЛОВОГО ОБМІНУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Мета роботи – вивчити принципи мережевої взаємодії з файловими серверами по протоколу FTP.

Навчальні питання:

1. Загальні принципи файлового обміну.

2. Основні терміни в протоколі FTP.

3. Авторизований доступ в протоколі FTP.

4. Анонімний доступ в протоколі FTP.

ЗАВДАННЯ

1. Виконати встановлення ftp-сервера на локальний хост.
2. Зконфігурувати встановлений FTP-сервер наступним чином:
   - дозволити анонімний доступ;
   - дозволити анонімним користувачам створення каталогів;
   - дозволити анонімним користувачам запис файлів;
3. Запустити FTP-сервер.
4. Командою FTP підключитися до сервера **ftp://localhost**.
5. Визначити налаштування сервера (команда **status**).
6. З'ясувати, який каталог є поточним.
7. Закрити з'єднання.
8. Локально створити від імені суперкористувача в каталозі **//ftp** підкаталоги **pub**, **temp** і **upload** з правами доступу 755, 777, 733 відповідно.
9. Анонімно підключитися до FTP-сервера localhost і виконати пакетні команди з файлу, створеного в попередньому завданні. У звіті пояснити причини відмінностей у результатах виконання цих пакетних команд.
10. Змінити конфігурацію FTP-сервера таким чином, щоб дозволити вхід для локальних користувачів.

11. Підключитися до FTP-сервера **localhost** з обліковим записом student і визначити, які каталоги будуть доступні для цього користувача.

12. Встановити параметр chroot_local_user=yes в vsftpd.conf і повторити попереднє завдання. Як відрізняються результати виконання цього і попереднього завдань?

13. Оформити звіт з лабораторної роботи, який має містити:

13.1. Тему та мету лабораторної роботи.

13.2. Навчальні питання.

13.3. Стислий хід виконання роботи.

13.4. Висновки по виконаній роботі.

13.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

18. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. В якому режимі працює навчальний ftp-сервер?
2. Який за замовчуванням режим передачі використовує ftp -сервер?
3. Який код відповіді буде виведений при вдалому підключенні до ftp-сервера?
4. Як визначити, що на ftp-сервері є каталоги, придатні для запису файлів?
5. Які коди відгуку будуть виведені при вдалій і невдалій зміні віддаленого каталогу?
6. Які коди відгуку будуть виведені при невдалій зміні віддаленого каталогу?

САМОСТІЙНА РОБОТА 1. ЛОГІЧНА ОРГАНІЗАЦІЯ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета роботи - вивчення принципів структурної організації локальних мереж та її канального рівня.

Навчальні питання:

1. Ієрархічна організація локальних обчислювальних мереж

2. Семирівнева модель OSI.

2. Відхід від семирівневої моделі OSI, проект стандарту 802 IEEE.

3. Особливості локальних мереж.

ЗАВДАННЯ

1. Вивчити основні теоретичні відомості про організацію локальних мереж та особливостям їх архітектури.
2. Отримати інформацію по мережеве устаткування локальної мережі та її параметри.
3. Проаналізувати отриману інформацію, занести її до звіту.
4. Оформити звіт з самостійної роботи, який має містити:
5.1. Титульний лист
5.2. Стислий опис локальної мережі.
5.3. Опис устаткування локальної мережі.
5.4. Висновки.
5.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.
4. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть структуру семирівневої моделі OSI.
2. Поясніть принцип роботи транспортного рівня мережі.
3. Поясніть п мережинцип роботи канального та фізичного рівня мережі.
4. Поясніть відмінність проекту стандарту 802 IEEE.

5. Поясніть особливості локальних мереж.
6. Поясніть принцип логічної організації локальних мереж.

САМОСТІЙНА РОБОТА 2. УСТАТКУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Мета роботи - вивчення специфіки ієрархічної організації локальних мереж, дослідження структурної організації локальних мереж.

Навчальні питання:

1. Переваги структурованої кабельної системи.

2. Адаптери комп'ютерних мереж.

3. Функції мережних адаптерів.

4. Фізична структура локальних комп'ютерних мереж.

5. Логічна структуризація локальних комп'ютерних мережі.

6. Маршрутизатори комп'ютерних мереж.

ЗАВДАННЯ

1. Вивчити основні теоретичні відомості про устаткування локальних мереж.
2. Оформити звіт з самостійної роботи, який має містити:
2.1. Титульний лист
2.2. Короткий опис фізичної структуризації локальної мережі.
2.3. Функціональну схему структури мережі, побудованої на основі маршрутизаторів.
2.4. Стислий опис алгоритмів роботи маршрутизаторів.
2.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.
3. Надіслати звіт з лабораторної роботи для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Дайте визначення структурованій кабельній системі.
2. Поясніть переваги структурованої кабельної системи.
3. Які функції виконує мережний адаптер?
4. Поясніть відмінності мережних адаптерів?
5. Для чого використовується автосегментація портів?

6. Що надає перевагу розподілу мережі на логічні сегменти?
7. Які функції має алгоритм покриваючого дерева мережі?
8. Які можливості надає маршрутизатор адміністратору мережі?
9. На якому рівні моделі OSI працюють маршрутизатори?

САМОСТІЙНА РОБОТА № 2

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ В CICSO PACKET TRACER

Мета роботи – ознайомитись з програмним забезпеченням для проектування комп‘ютерних мереж Cisco Packet Tracer.

Навчальні питання:

1. Інтерфейс Cisco Packet Tracer

2. Устаткування і лінії зв'язку в Cisco Packet Tracer

3. Приклади емуляції глобальної мережі.

ЗАВДАННЯ

1. Створити мережу: 4 вузли, сервер, принтер і два концентратора. Концентратори між собою з'єднуються кроссоверним кабелем.
2. Виконати пінгування між вузлами.
3. Отримати інформацію про пакети.
4. Отримати у викладача інформацію кількість підмереж та кількість вузлів в підмережі.
5. Оформити звіт з по самостійної роботи, який має містити:
5.1. Тему та мету лабораторної роботи.
5.2. Навчальні питання.
5.3. Стислий хід виконання роботи згідно з варіантом.
5.4. Висновки по виконаній роботі.
5.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.
6. Надіслати звіт для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які мережеві карти дозволяють підключатися до WAN мереж?
2. Який тип інтерфейсу слід вибрати при створенні кластера?
3. Яким типом кабелю з'єднуються роуте між собою?
4. Яким чином організовується зв'язок двох магістральних маршрутизаторів?

5. Які режими роботи існують в Cisco Paket Tracer?
6. Назвіть моделі комутаторів другого рівня?
7. Перерахуйте всі типи зв'язків, які використовуються в Cisco Paket Tracer і вкажіть їх призначення.
8. Для чого використовується режим симуляції в Cisco Paket Tracer?
9. Як переглянути проходження пакета по рівням моделі OSI?
10. Як визначитижіть IP-адреси відправника і одержувача в складі пакету?
11. Як в режимі симуляції визначити, які протоколи були задіяні в роботі мережі?
12. Як в режимі симуляції простежити зміну вмісту пакета при проходженні його по мережі?
13. Які можливості режиму симуляції існують в Cisco Paket Tracer?

САМОСТІЙНА РОБОТА № 3

ПРОСТА АДРЕСНА МАРШРУТИЗАЦІЯ В КОМП‘ЮТЕРНИХ МЕРЕЖАХ

Мета роботи – вивчення основ адресації і дозволів фізичних адрес для простої маршрутизації в комп‘ютерних мережах.

Навчальні питання:

1. Мережевий рівень: статична маршрутизація.

2. Принципи статичної маршрутизації.

3. Таблиці маршрутизації.

ЗАВДАННЯ

1. Визначити і зафіксувати дані IP-конфігурації комп’ютера.

1. Побудувати структуру мережі з трьох локальних мереж, сполучених через два маршрутизатори, забезпечивши коректну доставку кадрів на **фізичному** рівні.

2. Задати IP-адреси, маски підмережі і шлюзи за умовчанням для усіх вузлів мережі, щоб забезпечити коректну доставку ехо-запиту від PC1 до PC2 і ехо-відповіді назад. Обгрунтувати власні установки.

3. Виконати ехо-запит з PC1 на PC2. Подивитися виведення програми.

4. Виконати ехо-запит на неіснуючу IP-адресу 200.100.0.1 с PC1. Пояснити виведення програми.

5. Виконати ехо-запити з PC1 і PC2 на усі вузли мережі. Переконатися, що ехо-відповіді надходять.

У звіт необхідно включити схему мережі, налаштування протоколу TCP/IP для усіх вузлів мережі і результати виводу програми, отримані при виконанні ехо-запитів.

6. Задати маски підмережі і шлюзи за умовчанням для PC1 і PC2, а також IP-адреси з вибраного діапазону разом з масками і шлюзами для маршрутизаторів R1 і R2 так, щоб забезпечити коректну доставку ехо-запиту від PC1 до PC2 і ехо-відповіді назад. Обгрунтувати свої установки.

7. Виконати ехо-запит з PC1 на PC2. Проаналізувати виведення програми.

8. Виконати ехо-запит на неіснуючий IP -адрес 192.168.0.1 с PC1. Пояснити виведення програми.

9. Оформити звіт з по самостійної роботи , який має містити:

9.1. Тему та мету лабораторної роботи.

9.2. Навчальні питання.

9.3. Стислий хід виконання роботи згідно з варіантом.

9.4. Висновки по виконаній роботі.

9.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

10. Надіслати звіт для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. До якого класу IP-адрес належать адреси 10.11.0.1, 127.1.1.1?
2. Як здійснити розподіл адресного простіру 192.168.1.0 на 2 підмережі за допомогою масок.
3. Поясніть принцип роботи концентратора.
4. У чому є відмінність концентратор від повторювача?
5. Дайте визначення «петлі» між двома маршрутизаторами.

САМОСТІЙНА РОБОТА № 4

КЕРУВАННЯ СТАТИЧНОЮ МАРШРУТИЗАЦІЄЮ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Мета роботи – вивчення методів статичної маршрутизації в комп’ютерних мережах на вузлах мережевого рівня.

Навчальні питання:

1. Оптимізація статичної маршрутизації

2. Об’єднання логічних мережевих адрес.

ЗАВДАННЯ

1. Зібрати конфігурацію мережі згідно завданням, виданим викладачем.

2. Для усіх вузлів мережі встановити IP-адреси, маски підмереж і шлюзи за-замовчуванням.

3. Перевірити вдале виконання ехо-запиту вузлів, що знаходяться в одній підмережі.

3. Виконати настроювання таблиць маршрутизації на маршрутизаторах, для успішної доставки пакетів від вузла R1 до вузла R2 і в прямому та зворотньому напрямку.

4. Виконати настроювання таблиць маршрутизації на вузлах R1, R2 для найкоротшої доставки пакетів між вузлами.

5. Задати маски підмережі і шлюзи за-замовчуванням для PC1 і PC2.

6.Задати IP-адреси разом з масками і шлюзами для R1, R і R2 так, щоб забезпечити доставку пакетів від PC1 до PC2.

7. Настроїти таблицю маршрутизації на R для забезпечення доставки пакетів від PC2 до PC1.

7. Виконати ехо-запит з PC1 на PC2 та навпаки.

8. Оформити звіт з по самостійної роботи, який має містити:

8.1. Тему та мету лабораторної роботи.

8.2. Навчальні питання.

8.3. Хід виконання роботи згідно з варіантом.

8.4. Висновки по виконаній роботі.

8.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

9. Надіслати звіт для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Що являє собою маршрутизація?
2. Поясніть призначення маршрутизатора?
3. Які існують типи маршрутизації?
4. Для чого потрібні таблиці маршрутизації?
5. Які типи записів в таблиці маршрутизації можуть бути?
6. Поясніть принцип організації статичної маршрутизації.

САМОСТІЙНА РОБОТА № 5

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Мета роботи – вивчення методів налаштування статичної маршрутизації в програмному середовищі Cisco Packet Tracer.

Навчальні питання:

1. побудова статичних маршрутів.

2. Оптимізація статичної маршрутизації.

ЗАВДАННЯ

1. Створити схему мережі отриману у викладача.

2. Встановити на вузол Comp1 DNS і Web сервер.

3. Встановлений на вузол Comp2 DHCP сервер.

4. В мережі 3 замкнути на Hub міська мережа 100.100.100.0/12. У мережі встановлено DNS сервер провайдера з IP-адресою - 200.200.200.20/12.

5. В мережі 4 – вивести міську мережу в інтернет через комутатор Switch3 (мережа 210.210.210.0/24).

6. Виконати налаштування:

6.1. Мережі організацій;

6.2. DNS сервер провайдера;

6.3. Статичні таблиці маршрутизації на роутерах;

6.4. перевірити роботу мережі - на кожному з вузлів. 7. Налаштувати перший маршрутизатор.

7. Оформити звіт з по самостійної роботи , який має містити:

7.1. Тему та мету лабораторної роботи.

7.2. Навчальні питання.

7.3. Стислий хід виконання роботи згідно з варіантом.

7.4. Висновки по виконаній роботі.

7.5. Відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.

8. Надіслати звіт для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть принцип роботи статичної маршрутизації?
2. За допомогою якої команди можна отримати поточні конфігурацію маршрутизатора?
3. За допомогою яких команд можна налаштувати мережеву конфігурацію маршрутизатора.
4. Перерахуйте основні режими конфігурації при налаштуванні комутатора.
5. Перерахуйте основні режими конфігурації при налаштуванні роутера.
6. Як подивитися за допомогою роутера таблицю маршрутизації?
7. Які команди формують таблицю маршрутизації роутера?

Перелік рекомендованої літератури та інформаційних джерел

Базова література

1. Комп'ютерні мережі : підруч. з дисципліни "Комп’ютерні мережі" / Блозва А. І., Матус Ю. В., Касаткін Д. Ю. ; Нац. ун-т біоресурсів і природокористування України, Каф. комп’ютер. систем і мереж. - Київ : Компринт, 2019 . Т. 2. - 2019. - 382 с.
2. Адресації в IP-мережах:Теоретичні основи та приклади розв'язання задач [Електронний ресурс]: навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка» / Д.І.Могилевич, І.В.Кононова; КПІ ім.Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,590Мбайт). –Київ: КПІ ім. Ігоря Сікорського, 2019. –55 с.
3. Бабчук, С. М. Спеціалізовані комп'ютерні системи і мережі : лабораторний практикум / С. М. Бабчук. - Івано-Франківськ : ІФНТУНГ, 2018. - 102 с.
4. Задерейко О.В. Концептуальні основи захисту інформаційного суверенітету України : монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев. – Одеса : Фенікс, 2018. – 112 с.
5. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Комп’ютерні мережі» для студентів освітнього ступеня бакалавр спеціальності 123 «Комп’ютерна інженерія». / Г.М. Мельник, С.О. Вербовий, С. І. Возняк - Тернопіль: ТНЕУ, 2018.-71 с.
6. Протокол IP: Статична маршрутизація в IP-мережах: Навч.посібник / С.В. Панченко, С.І. Приходько, О.С. Жученко та ін.-Харків: УкрДУЗТ, 2017. – 136с.
7. Адміністрування комп’ютерних мереж та операційних систем: методичне видання для студентів за спеціальністю 121 «Інженерія програмного забезпечення»факультету інформаційних технологій УжНУ / Розробник: к.т.н., доц. Поліщук В.В. –Ужгород: 2019. – 60с.
8. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; В-во освіти і наукиУкраїни, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.

9. Іванюк, Н. І. Комп'ютерні мережі та телекомунікації : метод. вказ. для сам. роботи студ. для заочної форми навчання / Н. І. Іванюк. - Івано-Франківськ : ІФНТУНГ, 2016. - 12 с.

10. Іванюк, Н. І. Комп'ютерні мережі та телекомунікації : метод. вказ. для сам. роботи студ. для денної форми навчання / Н. І. Іванюк. - Івано-Франківськ : ІФНТУНГ, 2016. - 24 с.

11. Заміховська, О. Л. Комп'ютерні мережі : лабораторний практикум для студентів спец. 126 - "Інформаційні системи та технології" / О. Л. Заміховська. - Івано-Франківськ : ІФНТУНГ, 2017. - 30 с.

12. Іванюк, Н. І. Системи та мережі передачі даних : лабораторний практикум / Н. І. Іванюк. - Івано-Франківськ : ІФНТУНГ, 2017. - 71 с.

13. Іванюк, Н. І. Комп'ютерні мережі та телекомунікації : лабораторний практикум / Н. І. Іванюк. - Івано-Франківськ : ІФНТУНГ, 2016. - 255 с.

14. Адміністрування комп’ютерних систем та мереж : конспект лекцій для студентів напряму підготовки 6.050101 «Комп’ютерні науки» / уклад. П. В. Саварин, А. А. Ящук. – Луцьк : Луцький НТУ, 2016. – 68 с.

15. Комп’ютерні мережі. Локальні комп’ютерні мережі. Методичні вказівки до комп’ютерного практикуму. [Текст] / Уклад.: О.Ю. Кулаков, Р.Ю. Берест – К.: НТУУ «КПІ», 2012. –164 с.

16. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. -Х.: Видво Харк. нац. ун-ту внутр. справ, 2010. - 280 с.

17. Корпорация Cisco Systems, Inc. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е изд., с испр. Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 1168с.: ил.

18. Кларк Кеннеди, Гамильтон Кевин Принципы коммутации в локальных сетях Cisco. Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 976с.: ил.

Допоміжна література

1. Косинський В. І. Сучасні інформаційні технології: навч. посіб. /В. І. Косинський, О. Ф. Швець. – [2-ге вид, виправл.] – К.: Знання, 2012. – 318 с.

2. Порєв Г.В. Архітектура сучасних комп’ютерних мереж: Методичний посібник.—Вінниця: УНІВЕРСУМ-Вінниця, 2008 – 98 с.

3. Гожий О.П., Калініна І.О. Інформатика та комп’ютерна техніка: Навчально-методичний посібник. Для самостійного вивчення /О.П. Гожий, І.О. Калініна. – Миколаїв: Вид-во МДГУ ім. Петра Могили, 2006. – Вип. 58. – 212 с.

4. Козловський А.В. Комп’ютерна техніка та інформаційні технології: навч. посіб. /А.В. Козловський, Ю.М. Паночишин, Б.В .Погріщук. – К.: Знання, 2011. – 463 с.

Інформаційні ресурси

1. https://it.inf.od.ua – сайт кафедри інформаційних технологій, на якому розміщено робочі матеріали з курсу «Безпека персональної інформації в мережі Інтернет»

2. http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ ОЮА

3. Спеціалізовані комп'ютерні системи і мережі. [Електронний ресурс]. – URL: http://chitalnya.nung.edu.ua/node/4710

4. Комп'ютерні мережі. [Електронний ресурс]. – URL: https://learn.ztu.edu.ua/course/view.php?id=1890