В. О. Захаренко, О. С. Носиков

КОМП’ЮТЕРНІ МЕРЕЖІ

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

В. О. Захаренко, О. С. Носиков

КОМП’ЮТЕРНІ МЕРЕЖІ

Навчальний посібник
до лабораторного практикуму

Харків «ХАІ» 2025

УДК 004.7(076.5)
З-38

Рецензенти: д-р техн. наук, проф. А. А. Коваленко,
д-р техн. наук, проф. Ю. О. Романенков

Захаренко, В. О.

З-38 Комп’ютерні мережі [Електронний ресурс] : навч. посіб. до лаб. практикуму / В. О. Захаренко, О. С. Носиков. – Харків : Нац. аерокосм. ун-т «Харків. авіац. ін-т», 2025. – 94 с.

ISBN 978-966-996-072-6

Описано базові навички роботи в симуляторі мережи Cisco Packet Tracer, проєктування локальних мереж та настроювання мережних пристроїв компанії Cisco з використанням спеціальної мови програмування Cisco IOS, діагностування роботи локальних мереж за допомогою мережних утиліт і командного рядка Windows.

Для здобувачів освіти всіх форм навчання спеціальності 121 «Інженерія програмного забезпечення», а також для всіх, хто бажає вивчити курс «Комп’ютерні мережі» та «Основи системного адміністрування».

Іл. 69. Табл. 21. Бібліогр.: 6 назв

УДК 004.7(076.5)

ISBN 978-966-996-072-6

ЗМІСТ

ВСТУП

Дисципліна «Комп'ютерні мережі» є базовою у циклі дисциплін, орієнтованих на застосування мереж і мережних технологій у вирішенні професійних завдань, що вивчаються здобувачами вищої освіти на наступних курсах навчання за спеціальністю «Програмна інженерія».

Мета вивчення цієї дисципліни – оволодіння знаннями використання мережних засобів і базових технологій програмування, а також набуття основних навичок настроювання мережних пристроїв у локальних мережах на базі обладнання Cisco.

Навчальний посібник орієнтований на здобуття здобувачами вищої освіти знань та набуття базових навичок роботи у програмі-симуляторі комп’ютерних мереж Cisco Packet Tracer, набуття навичок використання протоколів рівня доступу, мережного та прикладного рівнів стека протоколів TCP/IP, а також досвіду вирішення практичних завдань з налаштування таких служб локальних мереж, як DHCP і NAT. У матеріалах посібника розглянуто методику та принципи забезпечення безпеки комп’ютерних мереж завдяки розбиттю мережі на логічні віртуальні мережі VLAN, реалізації дистанційного керування мережними пристроями другого та третього рівня (комутаторами та маршрутизаторами) з використанням протоколів TELNET та SSH та створення і використання списків доступу на мережних пристроях. Особливу увагу приділено питанням налаштування мережного інтерфейсу персонального комп’ютера та його діагностики за допомогою мережних утиліт ОС Windows.

Програмні рішення, наведені в посібнику, дають змогу здобувачеві вищої освіти у майбутньому самостійно розробляти архітектуру комп’ютерних мереж на базі обладнання відомих вендорів, таких як Cisco, D-Link, MikroTik та ін.

Розглянуті схеми та алгоритми мережних взаємодій дають уявлення про базові концепції, покладені в основу серверних розробок та організації синхронних взаємодій додатків, що формують основу для розуміння архітектурних принципів розроблення сучасних розподілених інформаційних систем, сприяють більш чіткому та детальному розумінню основних алгоритмів і методів організації взаємодії розподілених об’єктів та служб інформаційних систем.

Лабораторна робота № 1

ОЗНАЙОМЛЕННЯ З ПРОГРАМОЮ CISCO PACKET TRACER

Мета роботи: вивчити процес інсталяції і основних функцій програми-симулятора мережі Cisco Packet Tracer.

Теоретичні відомості

Програмний симулятор мережі Cisco Packet Tracer дає змогу імітувати роботу різних мережних пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережних принтерів, IP-телефонів і т. ін. Робота з інтерактивним симулятором дає дуже правдоподібне відчуття настроювання реальної мережі, що складається з десятків або навіть сотень пристроїв. Настроювання, у свою чергу, залежать від виду пристроїв: одні можна настроїти за допомогою команд операційної системи Cisco IOS, інші – шляхом графічного вебінтерфейсу, треті – через командний рядок операційної системи або графічні меню.

Завдяки такій властивості Cisco Packet Tracer, як режим візуалізації, користувач може відстежити переміщення даних по мережі, появу і зміну параметрів IP-пакетів при проходженні даних через мережні пристрої, швидкість і шляхи переміщення IP-пакетів. Аналіз подій, що відбуваються в мережі, дає змогу зрозуміти механізм її роботи і виявити несправності.

Установка Packet Tracer

Для інсталяції Cisco Packet Tracer на комп'ютер виконайте такі кроки:

1. Створіть обліковий запис на Cisco NetAcad.
2. Перейдіть на сайт Cisco Networking Academy.
3. Зареєструйтеся, якщо у вас ще немає облікового запису.
4. Завантажте інсталяційний файл Packet Tracer.
5. Встановіть завантажений файл.
6. Запустіть інсталяційний файл, який ви завантажили.
7. Дотримуйтесь інструкцій майстра встановлення.
8. Прийміть ліцензійну угоду.
9. Оберіть шлях для встановлення програми (або залиште за замовчуванням).
10. Дочекайтесь завершення процесу встановлення програми.
11. Запустіть Packet Tracer.
12. Після встановлення програми відкритйте Cisco Packet Tracer з меню «Пуск» або ярлика на робочому столі.
13. Під час першого запуску програми, якщо потрібно, введіть дані облікового запису NetAcad для авторизації.
14. Після завершення інсталяції використовуйте Cisco Packet Tracer для моделювання мереж.

Огляд графічного інтерфейсу

Основне робоче вікно Packet Tracer подібно до графічного редактора містить кілька складових (рис. 1.1).

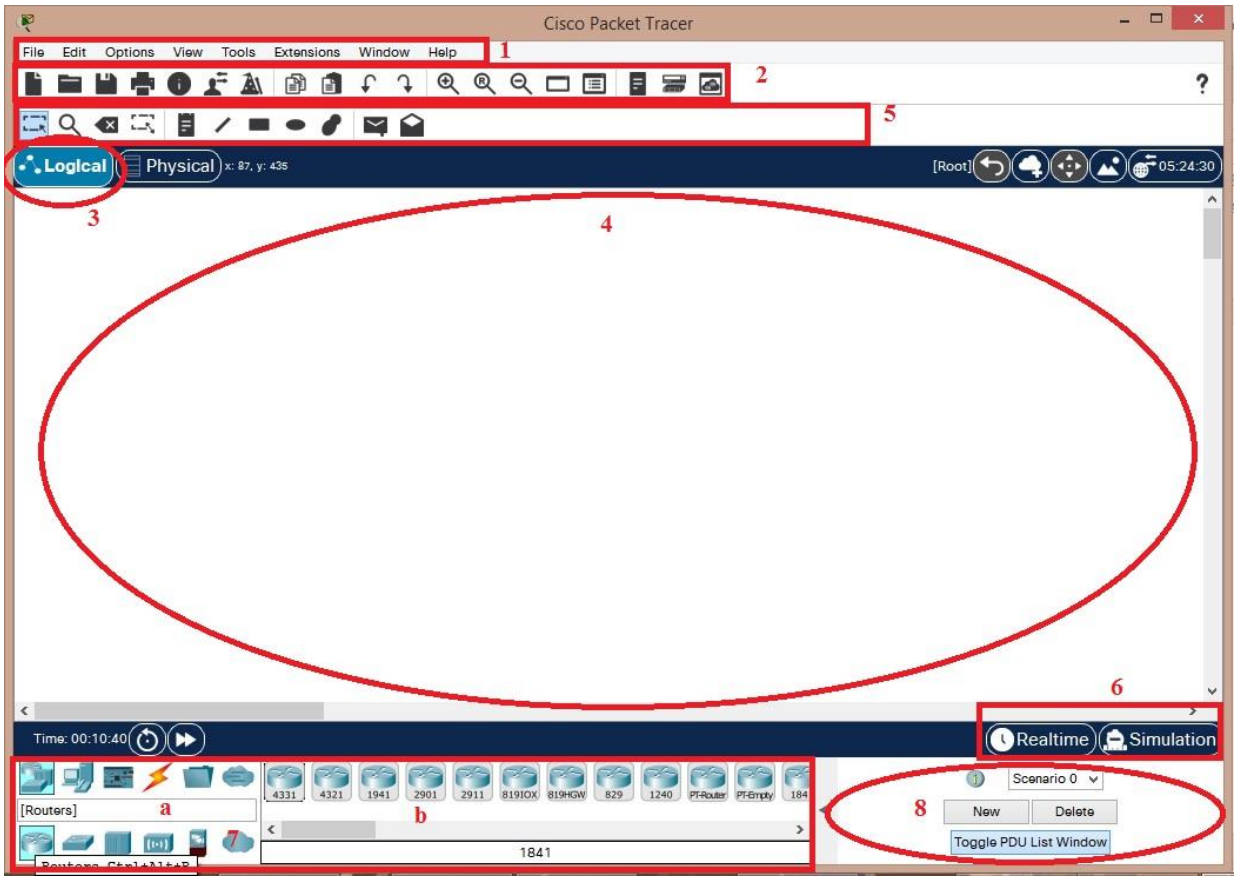

Рис. 1.1. Інтерфейс програми Cisco Packet Tracer

1. **Рядок меню** (Menu Bar). Цей компонент ідентичний для всіх програмних додатків. Використовується для відкривання, збереження, друку, зміни налаштувань і т. ін.
2. **Головна панель інструментів** (Main Toolbar) містить ярлики, що забезпечують швидкий доступ до найбільш часто використовуваних пунктів меню, таких як Відкрити (Open), Зберегти (Save), Масштаб (Zoom), Скасувати (Undo), Повторити (Redo) та ін. У правій частині панелі знаходиться ярлик для введення інформації про поточну топологію.
3. **Перемикач вибору логічної або фізичної топології** (Logical / Physical Workspace Tabs) призначено для перемикання між логічною та фізичною робочими областями.
4. **Робочий простір** (Workspace). Це основна сфера зайнятості в Packet Tracer. Саме тут створюється необхідна топологія (схема мережі) і відображається симуляція процесу мережної взаємодії.
5. **Загальна панель інструментів** (Common Tools Bar) забезпечує можливість вибору інструментів маніпуляції зі схемою мережі, таких як

виділення та зміна розташування пристроїв, розміщення написів і нотаток, видалення, зміна розміру і вибір передачі простого (Simple PDU) або складного (Complex PDU) блока даних користувача.

6. **Перемикач вибору режиму роботи** (Realtime / Simulation Tabs) забезпечує перемикання між реальним режимом роботи або режимом симуляції мережної взаємодії. Цей перемикач також дає можливість контролю часу і захоплення пакетів у мережі.
7. **Вікно вибору мережних компонентів** (Network Component Box) містить доступне в Packet Tracer мережне обладнання та кінцеві пристрої. Поділяється на дві області:
   а) **вікно вибору категорії пристрою** (Device-type Selection Box) містить основні категорії пристроїв (маршрутизатори, комутатори, концентратори, бездротові пристрої, мережні кабелі, кінцеві пристрої тощо);
   б) **вікно вибору конкретного типу пристрою** (Device-specific Selection Box). Після вибору категорії тут стають доступними різні моделі пристроїв.
8. **Вікно створення пакетів користувачів** (User-created Packet Box) призначене для створення користувачами докладних тестів мережної топології і відображення їх результатів.
9. Для успішного подальшого вивчення Packet Tracer необхідно впевнено орієнтуватися в наведених назвах інструментів і їх розташуванні у вікні програми.

Створення простої схеми мережі

У вікні вибору мережних компонентів знайдіть категорію Кінцеві пристрої (End Devices) і виберіть у сусідньому вікні Персональний комп'ютер ПК (Generic PC) і Ноутбук (Generic Laptop). Перетягніть обидва пристрої в робочу область Packet Tracer.

Натисніть Підключення (Connections), потім виберіть Перехресний кабель (Copper Cross-Over). У перехресному кабелі, як і передбачає його назва, волокна перетинаються на шляху від одного кінця до іншого (рис. 1.2). Спочатку натисніть на зображення ПК і виберіть FastEthernet-інтерфейс пристрою у відкритому списку. Після цього натисніть на зображенні ноутбука і також виберіть FastEthernet-інтерфейс. При правильному підключенні індикатори статусу пристроїв повинні відображатися зеленим кольором, що вказує, що інтерфейси пристроїв увімкнені (рис. 1.3).

Для того щоб настроїти пристрій, наприклад ПК, слід натиснути на його зображенні і потім вибрати вкладку Робочий стіл (Desktop). Виберіть інструмент Конфігурація IP (IP Configuration) і введіть IP-адресу (IP Address) та маску (Subnet Mask) пристрою (рис. 1.4).

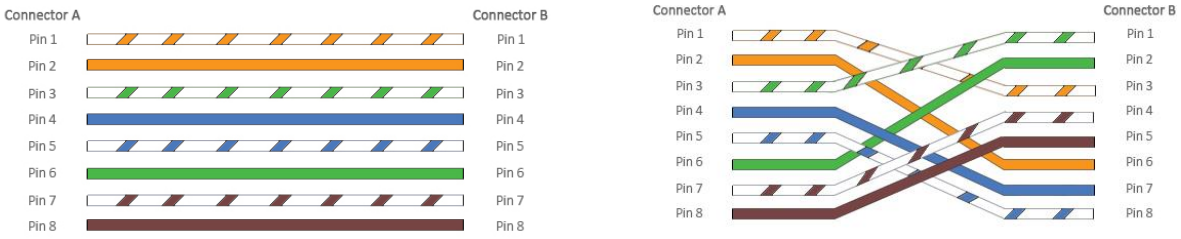

Рис. 1.2. Схема прямого та перехресного обтискання кабелів

Рис. 1.3. Проста топологія мережі

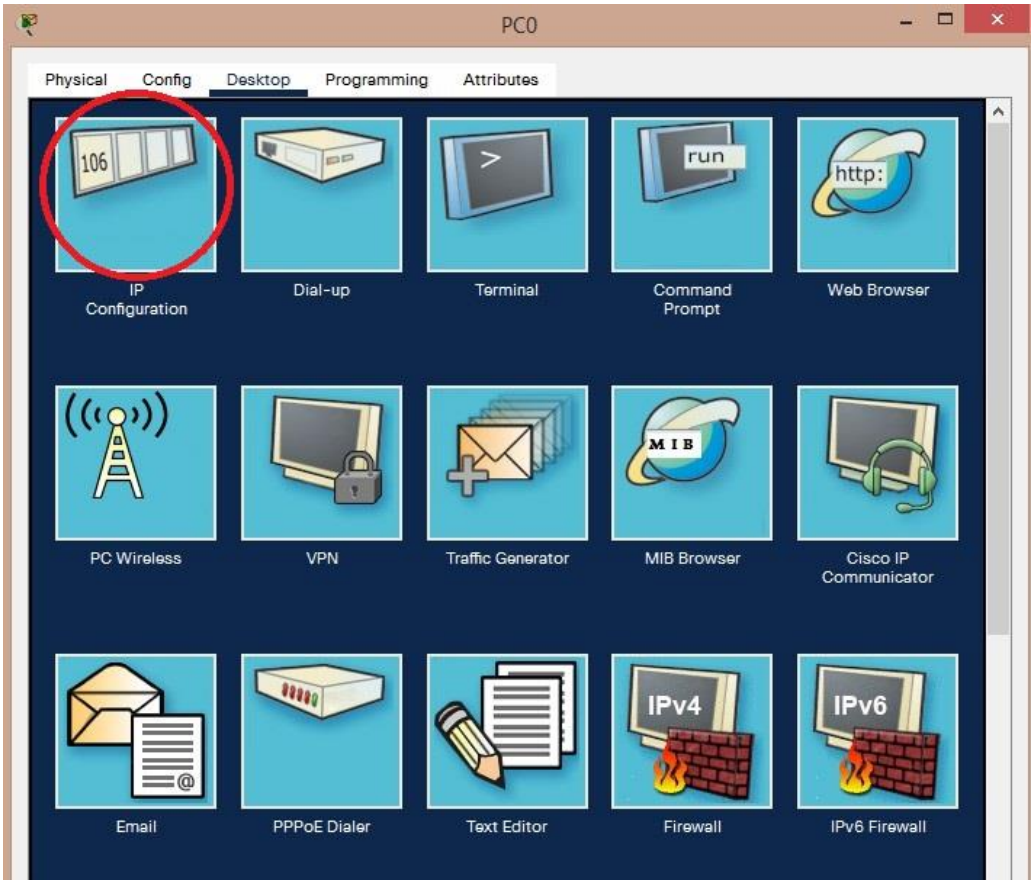

Рис. 1.4. Робочий стіл ПК

Для схеми можна обійтись без IP-адреси шлюза і DNS-сервера, тому що в цьому немає необхідності. Схема складається тільки з двох комп'ютерів і не передбачає вихід в інтернет або під’єднання до інших мереж, а також використання символьних імен (рис. 1.5).

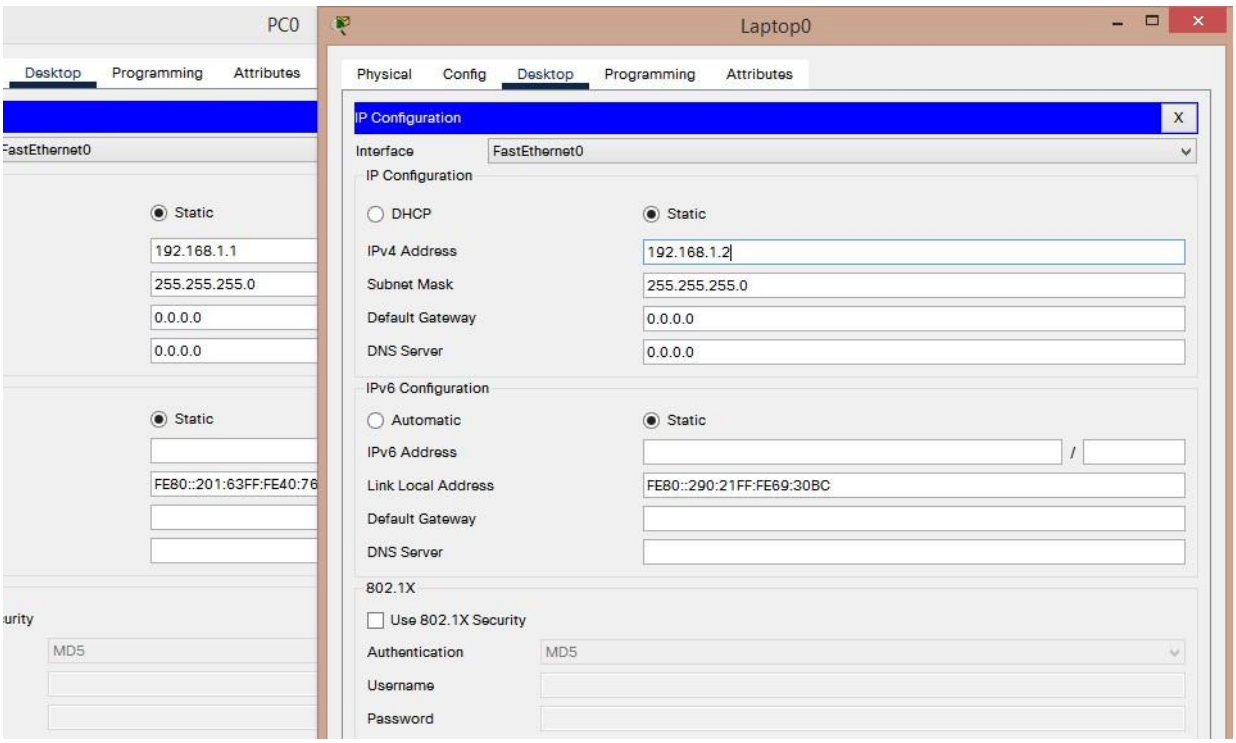

Рис. 1.5. Настроювання IP-адреси і маски підмережі ПК і ноутбука

Закрийте вікно настроювання ПК. Натисніть на зображення ноутбука і таким же чином настройте ноутбук.

Перевірте, чи настроювані IP-адреси знаходяться в одній підмережі. Закрийте вікно настроювання IP-адреси і потім відкрийте інструмент командного рядка (Command Prompt). Скориставшись утилітою **ping**, проведіть тест сполучності, як показано на рис. 1.6.

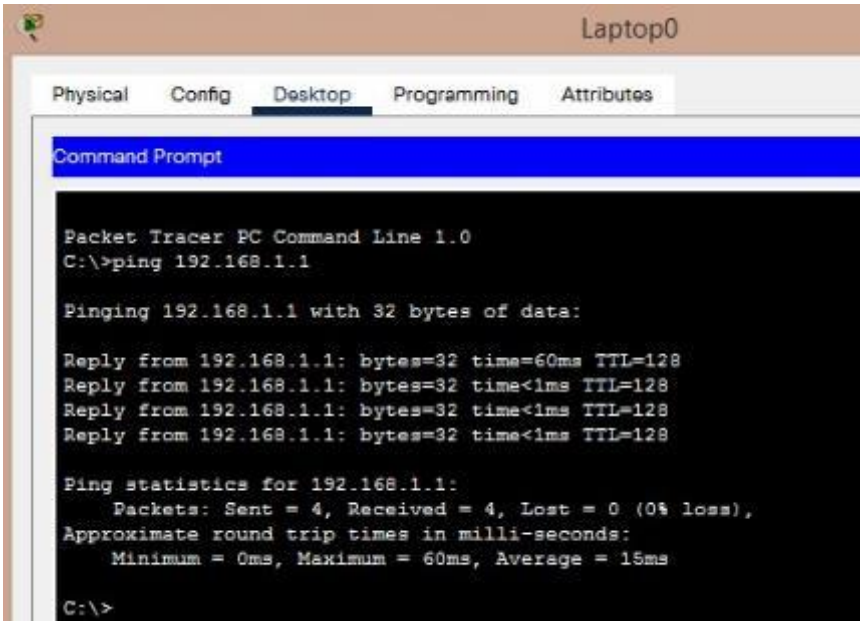

Рис. 1.6. Тест сполучності між пристроями

Дослідження якості передачі трафіку по мережі

Для роботи створіть і настройте таку мережу, як показано на рис. 1.7.

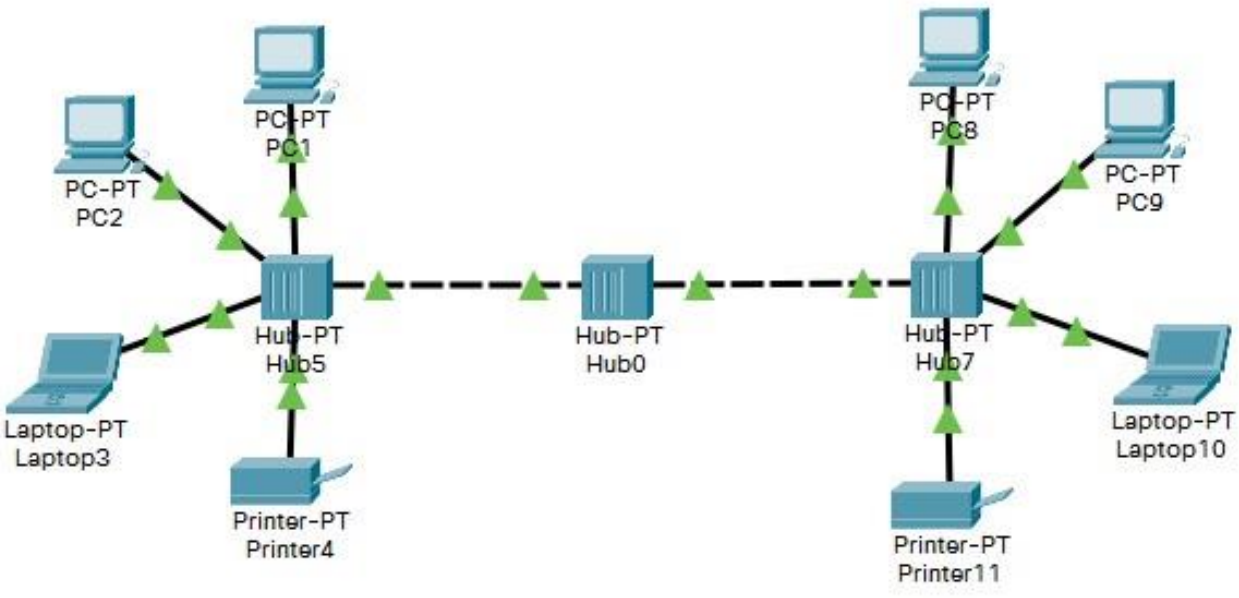

Рис. 1.7. Схема мережі

Під час дослідження пропускної здатності мережі (якості передачі трафіку по мережі) бажано збільшити розмір пакета і відправляти запити з коротким інтервалом часу, не чекаючи відповіді від віддаленого вузла, для того щоб створити серйозне навантаження на мережу [1]. Однак утиліта **ping** не дозволяє відправляти ехо-запит без отримання ехо-відповіді на попередній запит і до закінчення часу очікування. Тому для організації істотного трафіку скористаємося програмою Traffic Generator.

Настроювання параметрів генератора трафіку

У вікні керування PC1 у вкладці Desktop виберіть додаток Traffic Generator (генератор трафіку) і визначте настройки для передачі трафіку від PC1 на PC8 (рис. 1.8). До основних настройок належать такі як розмір пакету, тип протоколу передачі даних, часовий інтервал між пакетами та адреси відправника й одержувача пакета.

Отже, за допомогою протоколу ICMP сформували трафік між комп’ютерами PC1 з адресою **192.168.0.1** і PC8 з адресою **192.168.0.8**. При цьому в розділі Source Settings (Настроювання джерела) необхідно встановити прапорець Auto Select Port (Автоматичний вибір порту), а в

розділі PDU Settings (настроювання IP-пакета) задати такі значення параметрів цього поля:

Select application: PING
Destination IPAddress: 192.168.0.8 (адреса отримувача);
Source IP Address: 192.168.0.1 (адреса відправника);
TTL: 32 (час життя пакета);
TOS: 0 (тип обслуговування, "0" – звичайний, без пріоритету);
Sequence Number: 1 (початкове значення лічильника пакетів);
Size: 1400 (розмір поля даних пакета в байтах);
Simulations Settings – тут необхідно активувати перемикач;
Periodic Interval: 0.3 Seconds (період повторення пакетів).

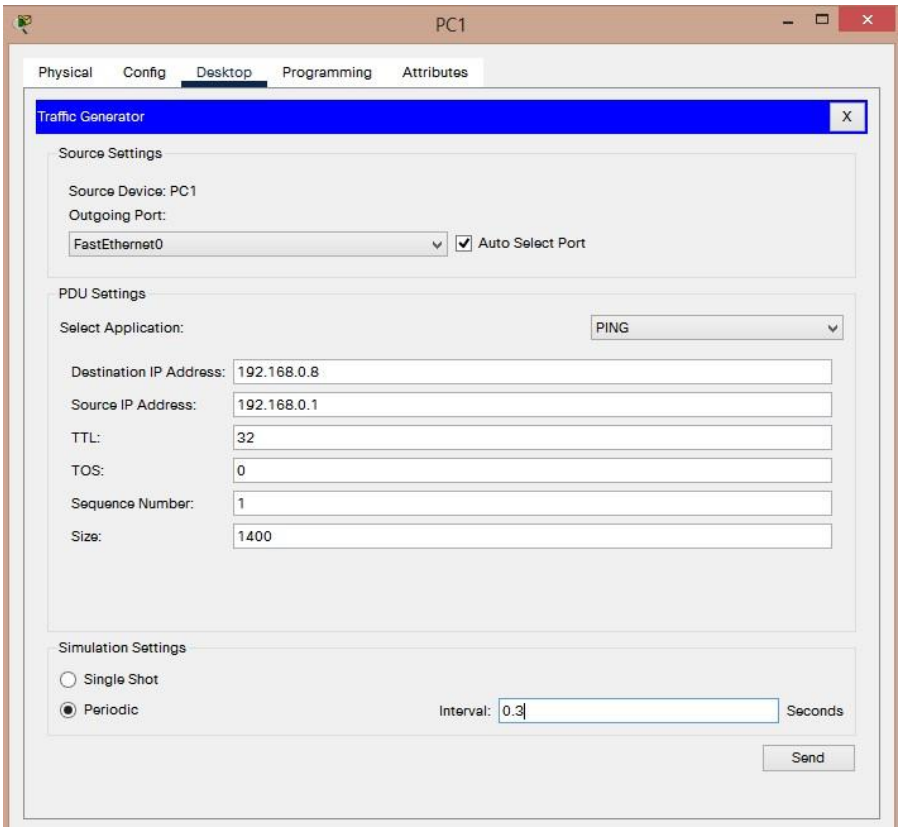

Рис. 1.8. Вікно настроювання Traffic Generator

Після натискання на кнопку **Send** (Послати) між PC1 і PC8 почнеться активний обмін даними. Не закривайте вікно настроювання генератора трафіку, щоб не перервати потік трафіку – лампочки повинні постійно блимати.

Дослідження якості роботи мережі

Для оцінювання якості роботи мережі передамо потік пакетів між PC8 і PC1 за допомогою команди **ping -n 200 192.168.0.1** і будемо оцінювати якість роботи мережі за кількістю втрачених пакетів (рис. 1.9). Параметр **-n** дає змогу задати кількість переданих ехо-запитів (у нас їх 200).

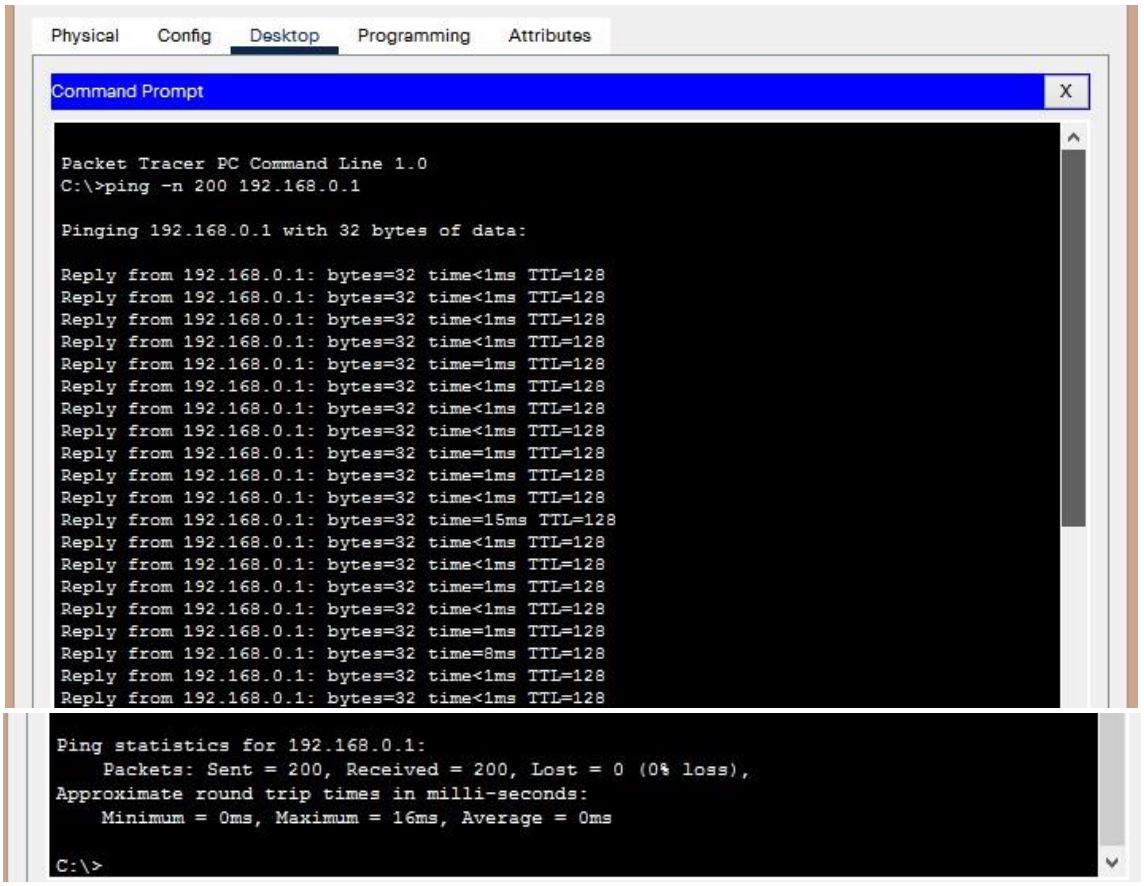

Рис. 1.9. Команда ping

Одночасно з навантаженням за допомогою генератора трафіку, включеного на комп'ютері PC1, навантажте мережу, включивши генератор трафіку на комп'ютері PC2 (рис. 1.10) – вузлом призначення буде також комп'ютер PC8 (розмір поля даних – 2500 байт; період повторення передачі – 0,01 с) та генератор трафіку на комп'ютері PC3 (Laptop) (вузол призначення – PC8; розмір поля даних – 5000 байт; період повторення передачі – 0,01 с) (рис. 1.11).

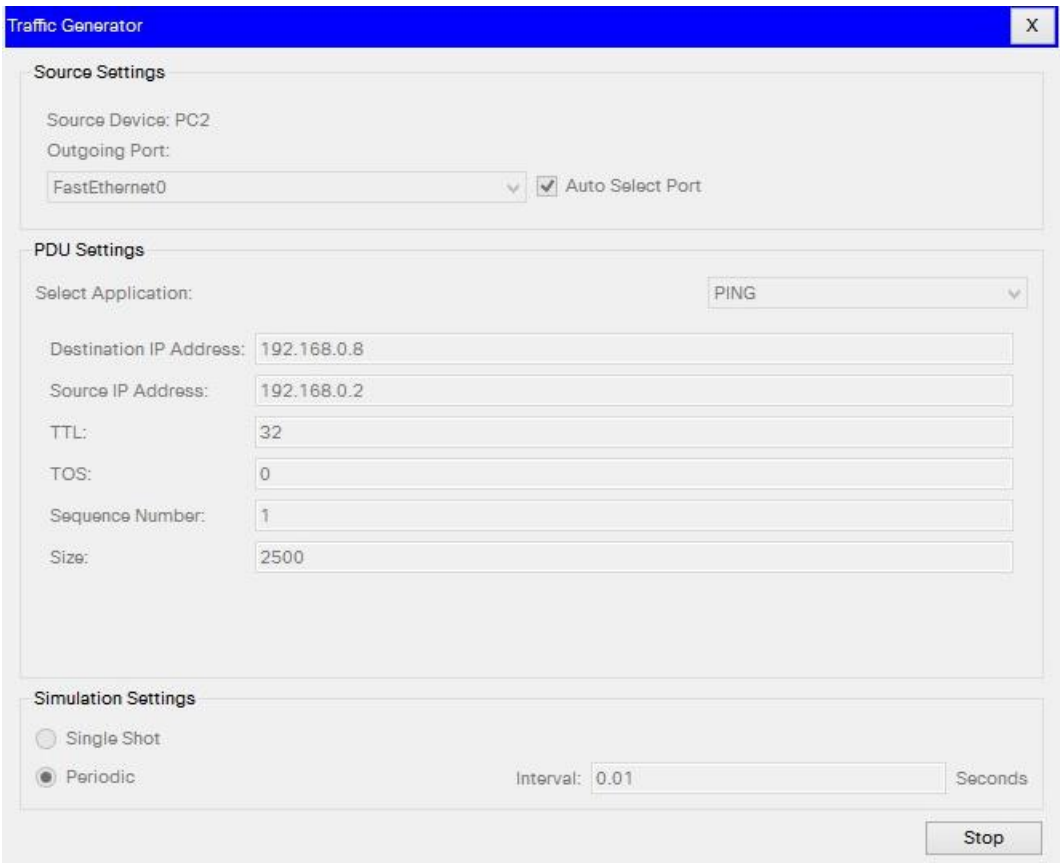

Рис. 1.10. Настроювання генератора трафіку на PC2

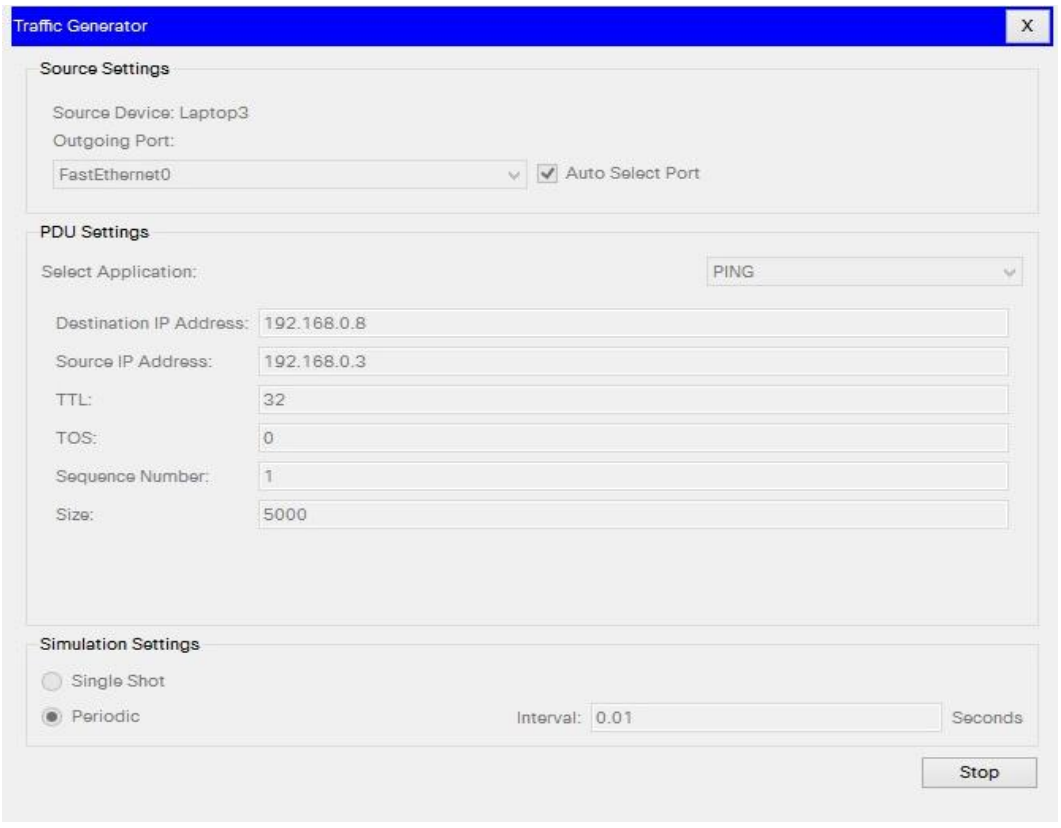

Рис. 1.11. Настроювання генератора трафіку на Laptop

Для оцінювання якості роботи мережі зафіксуйте кількість втрачених пакетів після включення першого, другого та третього генераторів трафіку (рис. 1.12).

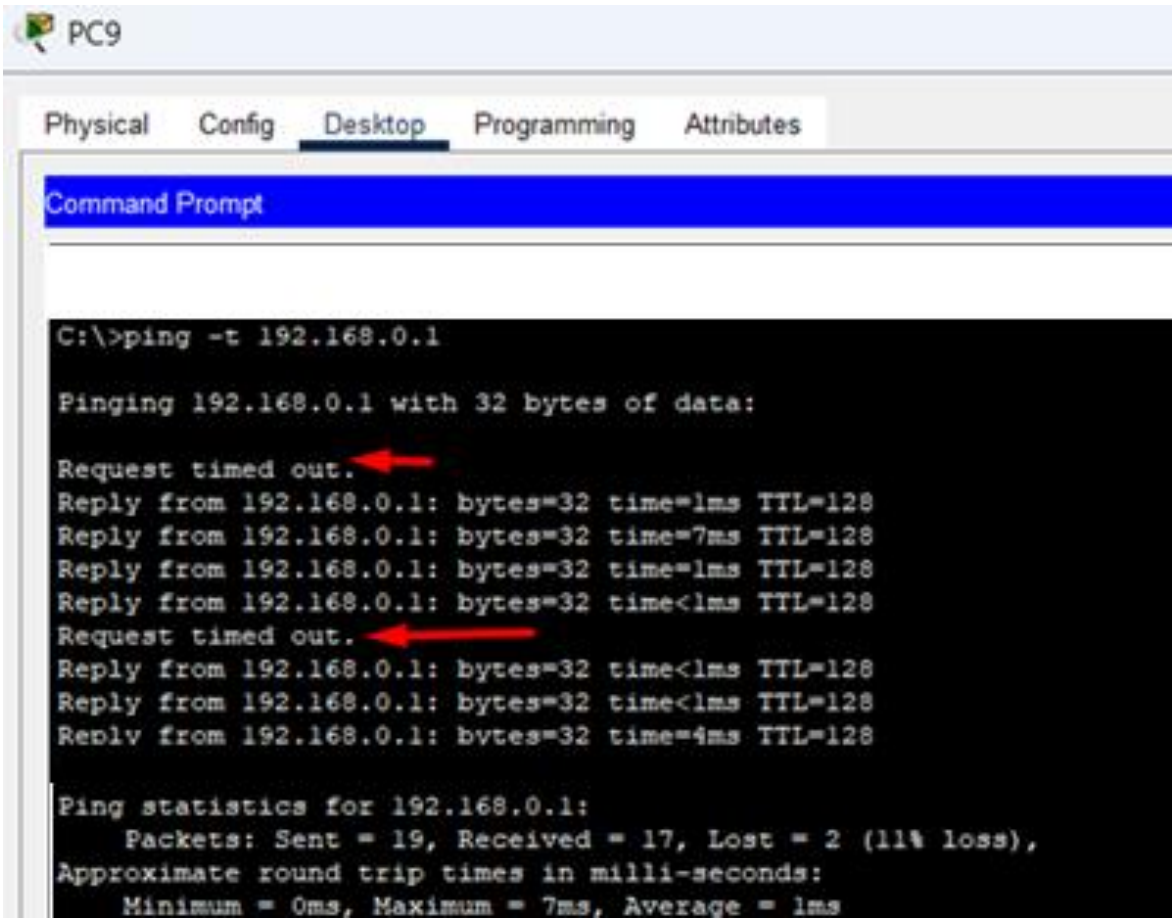

Рис. 1.12. Визначення втрачених пакетів

На закінчення роботи зупиніть Traffic Generator на всіх вузлах, натиснувши кнопку **Stop**.

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.
2. Встановіть програму Cisco Packet Tracer.
3. Знайдіть у мережі Internet одне або кілька додаткових джерел за описом роботи програми, вивчіть і наведіть посилання на них у звіті.
4. За допомогою Cisco Packet Tracer побудуйте мережу, зазначену в теоретичній частині, і настройте мережні інтерфейси кінцевих пристроїв.
5. Самостійно проведіть дослідження якості трафіку в побудованій мережі, провівши послідовно три експерименти, та заповніть табл. 1.1.

Таблиця 1.1

Умови експерименту

Настроювання	Експеримент 1	Експеримент 2	Експеримент 3
Генератор трафіку між комп'ютерами *	PC1–>PC9 PC2–>PC9	PC1–>PC9 PC2–>PC9 Laptop3–>PC9	PC1–>PC9 PC2–>PC9 Laptop3–>PC9 PC8–>PC9
Команда **ping** (200 ехо-запитів)	PC9–>PC1	PC9–>PC1	PC9–>PC1
Кількість втрачених пакетів і їх відсоток від загальної кількості запитів			

* Параметри генератора трафіку беруться згідно з варіантом завдання.

6. У висновках відобразіть залежність кількості втрачених пакетів від інтенсивності трафіку в мережі шляхом порівняння першого, другого та третього експериментів.

Вимоги до звіту

Звіт з лабораторної роботи має містити:

1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 1.2

Варіанти завдань

Номер варіанта	Параметри настроювання генератора трафіку	
	Розмір пакета, байти	Періодичність передачі пакетів, с
1, 11	4100	0,006
2, 12	4200	0,007
3, 13	4300	0,008
4, 14	4400	0,009
5, 15	4500	0,01
6, 16	4600	0,011
7, 17	4700	0,012
8, 18	4800	0,013
9, 19	4900	0,014
10, 20	5000	0,015

Контрольні запитання

1. Які можливості моделювання мережі надає симулятор Cisco Packet Tracer?
2. Які основні компоненти робочого вікна Cisco Packet Tracer ви знаєте?
3. Чим відрізняється прямий кабель від перехресного?
4. Які основні опції настроювання додатка Traffic Generator?

Лабораторна робота № 2

ОСНОВНІ КОМАНДИ ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO IOS. НАСТРОЮВАННЯ СТАТИЧНИХ МАРШРУТІВ

Мета роботи: вивчити основні команди операційної системи Cisco IOS та настроювання статичної маршрутизації у роутері Cisco.

Теоретичні відомості

Основи роботи в командному рядку операційної системи Cisco IOS

Командний рядок – це місце, куди користувач вводить символи, що мають керівний вплив. Робота з командним рядком здійснюється в декількох режимах (табл. 2.1). Наведені в табл. 2.1 команди для керування роутером (**Router>**) може бути використано і для керування комутатором (**Switch>**). Відмінність команд буде наведено у кожному окремому випадку.

Таблиця 2.1

Основні режими конфігурації пристроїв з операційною системою Cisco IOS

Назва режиму	Символи запрошення у командному рядку	Команда входу в режим	Команда виходу з режиму
Користувацький режим	Router>	Установлюється при вході в пристрій після натискання клавіші Enter	exit
Привілейований режим	Router#	enable	disable
Режим глобальної конфігурації	Router(config)#	configure terminal	exit
Режим детальної конфігурації	Router(config-mode) #, де mode – назва об'єкта, що підлягає конфігурації, наприклад: Router(config-if) # − конфігурація інтерфейсу; Router(config-line) # − конфігурація термінальної лінії; Router(config-router) # − конфігурація динамічної маршрутизації; Router(config-vlan) # − конфігурація віртуальної локальної мережі VLAN	Команди, що відповідають об'єкту конфігурації	exit

Router> – запрошення в призначений для користувача режим, в якому можна переглядати деяку статистику і проводити найпростіші операції на кшталт пінга. Це режим для мережного оператора, інженера першої лінії техпідтримки, щоб він нічого не пошкодив і не дізнався зайвої інфомації. Іншими словами, за допомогою команд у цьому режимі можна виводити на екран інформацію без зміни настройок мережного пристрою.

Router# – запрошення в привілейований режим. Привілейований режим підтримує команди настроювання і тестування, детальну перевірку мережного пристрою, маніпуляцію з файлами і доступ в режим конфігурації. Потрапити в нього можна, ввівши команду enable.

Router (config)# – запрошення в режим глобальної конфігурації, що дає змогу вносити зміни в настройки пристрою. Команди режиму глобальної конфігурації визначають поведінку системи в цілому. Активується командою **#configure terminal** з привілейованого режиму.

Доступ до командного рядка операційної системи Cisco IOS у програмному середовищі імітаційного моделювання Cisco Packet Tracer може бути реалізовано різними способами. Розглянемо декілька з них:

- доступ до командного рядка через вкладку CLI діалогового вікна властивостей пристрою;
- доступ до командного рядка через термінальне під’єднання робочої станції (комп’ютера) консольним кабелем;
- доступ до командного рядка через Telnet.

Спочатку розглянемо приклади доступу до командного рядка, а потім приклад входу та виходу із різних режимів конфігурації.

Доступ до командного рядка операційної системи Cisco IOS через вкладку CLI

Можливість доступу до командного рядка операційної системи Cisco IOS через вкладку CLI діалогового вікна властивостей пристрою реалізована в симуляторі Cisco Packet Tracer з метою спрощення та прискорення доступу під час навчання (в реальності такого способу доступу не існує).

Вкладка CLI (Command Line Interface) у Cisco Packet Tracer є одним з основних інструментів для настроювання мережних пристроїв за допомогою командного рядка. Це імітація реального інтерфейсу командного рядка (CLI) на мережних пристроях Cisco, таких як маршрутизатори, комутатори та ін.

Для отримання доступу до командного рядка маршрутизатора Cisco в симуляторі через вкладку CLI необхідно виконати таку послідовність кроків:

1. Вибрати маршрутизатор Cisco в бібліотеці пристроїв та фізичних з'єднань і перетягнути його на логічну робочу область (рис. 2.1).

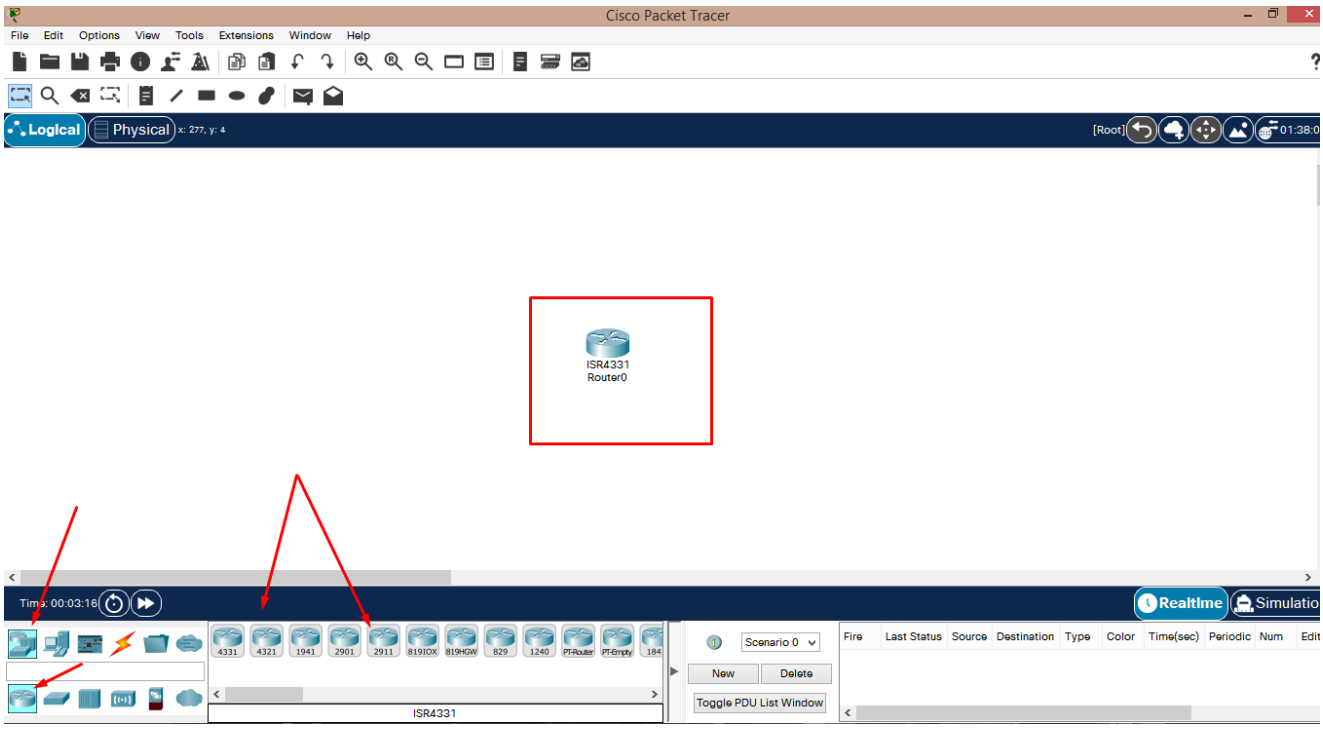

Рис. 2.1. Вибраний маршрутизатор

2. Натиснути на пристрій для виклику діалогового вікна властивостей пристрою.

3. Вибрати вкладку CLI у діалоговому вікні властивостей пристрою (рис. 2.2).

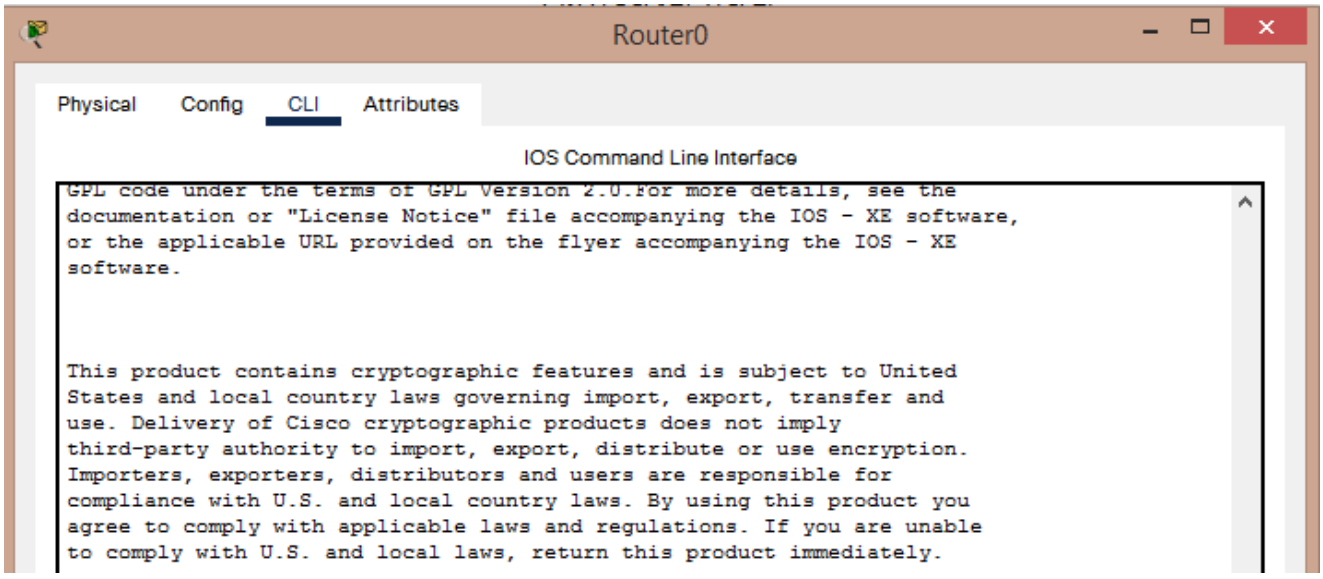

Рис. 2.2. Вкладка CLI

4. За відсутності в енергонезалежній пам’яті пристрою конфігураційної інформації, що з’явиться при першому ввімкненні нового пристрою, у командному рядку з'явиться діалог (System Configuration Dialog) із

пропозицією настроїти основні параметри пристрою (ім'я, паролі, інтерфейси) у режимі діалогу (**Continue with configuration dialog? [yes/no]:**). У цьому випадку слід відмовитися від настроювання основних параметрів, уводячи відповідь «no» і натискаючи клавішу ENTER. У командному рядку з'явиться повідомлення Press RETURN to get started! з пропозицією натиснути клавішу RETURN (ENTER) для того, щоб почати роботу з командним рядком у користувацькому режимі (рис. 2.3). Тому приймаємо пропозицію, натискаючи на клавіатурі клавішу ENTER (клавіша RETURN є тільки на клавіатурах виробництва Apple).

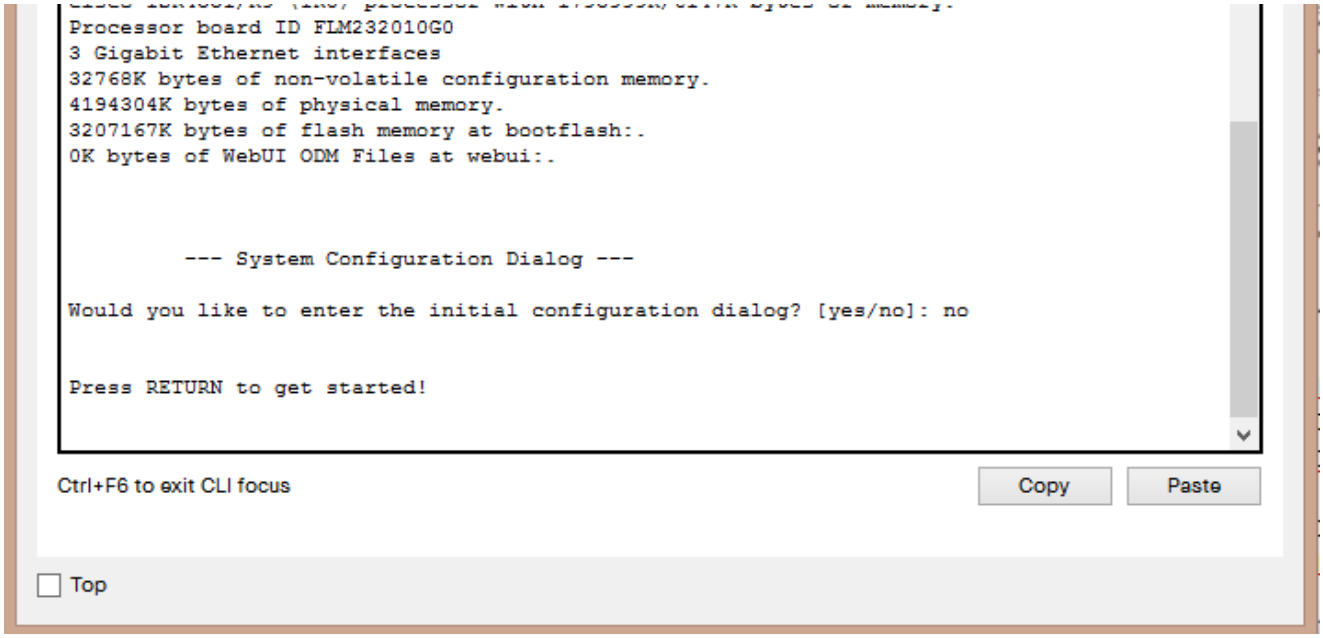

Рис. 2.3. Пропозиція натиснути на клавіатурі клавішу RETURN (ENTER) для роботи з командним рядком у користувацькому режимі

Після цього пристрій переходить у користувацький режим конфігурації, що підтверджується появою запрошення в командному рядку

Router>.

Доступні в користувацькому режимі команди можна побачити, увівши в командний рядок знак питання:

Router>?.

Для переходу в привілейований режим необхідно ввести команду enable. При цьому запрошення в командному рядку змінюється з **Router>** на **Router#**.

Router>enable

Router#

Повернення в користувацький режим відбувається за допомогою команди disable.

Router#disable
Router>

Якщо в привілейованому режимі ввести команду exit, то відбудеться вихід з операційної системи пристрою, що підтверджується появою пропозиції почати роботу з командним рядком у користувацькому режимі «**ENTER Press RETURN to get started!**»

Router#exit
ENTER Press RETURN to get started!

Для переходу в режим глобальної конфігурації необхідно в привілейованому режимі ввести команду **configure terminal** (можна скорочено − **config t**). При цьому запрошення в командному рядку змінюється з **Router>** на **Router(config)#**.

Router>enable
Router#config Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

Повідомлення «Enter configuration commands, one per line. End with CNTL/Z» підказує, що в режимі глобальної конфігурації в кожний рядок уводиться тільки одна команда, а вийти з цього режиму можна натисканням комбінації клавіш на клавіатурі CNTL/Z замість уведення команди **exit**.

Router(config)#exit
Router#

Зауважимо, що в режимі глобальної конфігурації безпосередньо не виконуються команди з інших режимів (наприклад, **show running-config**, **ping**). Для того щоб, не виходячи з режиму глобальної конфігурації, використовувати ці команди, необхідно додати **do** перед командою. Наприклад, для перегляду поточної конфігурації пристрою, завантаженої в цей момент в оперативну пам'ять, необхідно ввести **do show running-config**. **Router(config)**

#do show running-config

Доступ до командного рядка операційної системи Cisco IOS через термінальне під’єднання робочої станції консольним кабелем

Більшість мережних пристроїв компанії CISCO допускають їх конфігурацію. Для цього адміністратор мережі має під’єднатися до пристрою через пряме кабельне (консольне) під’єднання (рис. 2.4).

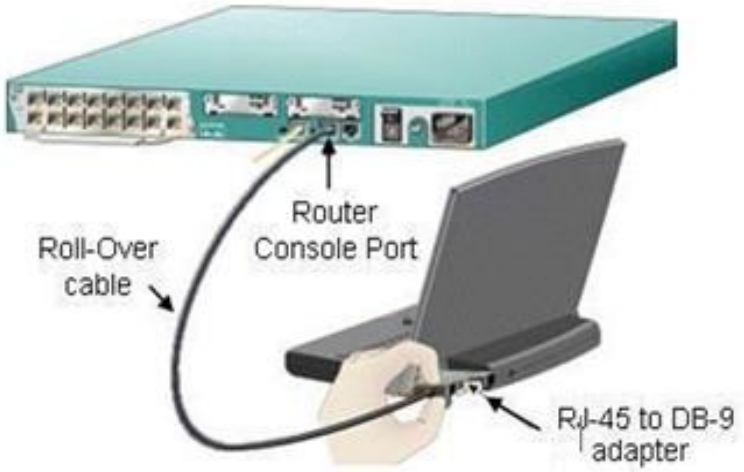

Рис. 2.4. Консольне під’єднання

Програмування пристроїв CISCO найчастіше роблять через консольний порт RJ-45. На рис. 2.5 показано фотографію консольних рознімів на маршрутизаторі і два варіанти консольного кабелю. Класичний консольний кабель має рознім DB9 для під’єднання до COM-порту комп'ютера і рознім RJ-45 для під’єднання до консольного порту маршрутизатора. Зараз Cisco активно просуває нові маршрутизатори серій 28xx, 38xx і т. ін. У них передбачено можливість конфігурації через USB-інтерфейс (використовуються звичайні USB-кабелі).

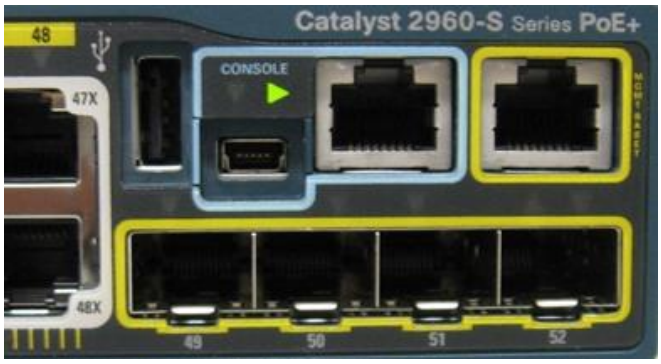

Рис. 2.5. Консольні рознімі

Для отримання доступу з консолі необхідно:

1. Винести на логічне робоче поле ноутбук, що буде використовуватися як термінал і маршрутизатор. У бібліотеці з’єднань

вибрати консольний кабель та з'єднати комп'ютер і маршрутизатор цим кабелем. У процесі з'єднання консольним кабелем виберемо такі типи портів: RS-232 − на ноутбуці та Console – на маршрутизаторі (рис. 2.6).

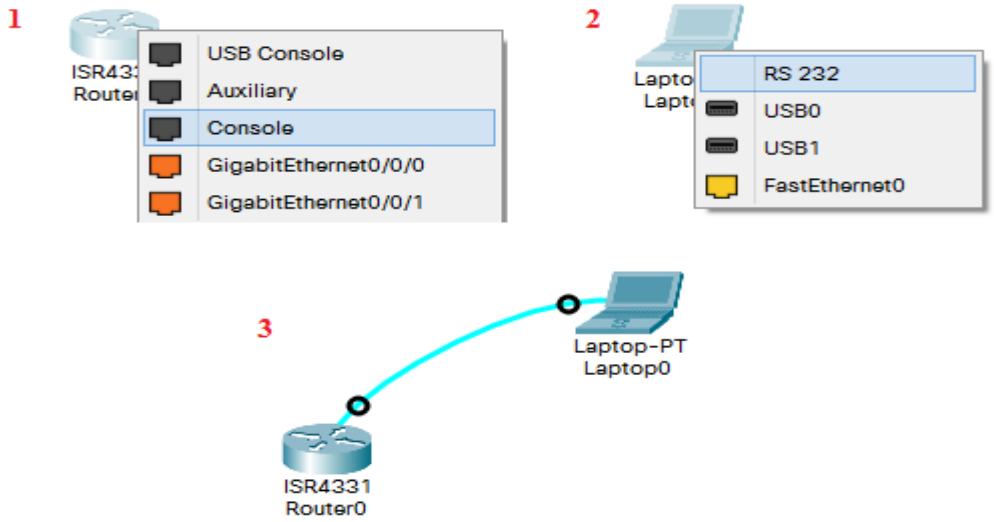

Рис. 2.6. З'єднання термінала (комп'ютера) та пристрою консольним кабелем

2. Натиснути на значок ноутбука для виклику діалогового вікна властивостей, перейти до вкладки Desktop та натиснути на значок Terminal (рис. 2.7). У вікні Terminal Configuration усі параметри залишаємо за замовчуванням та натискаємо на кнопку ОК (рис. 2.8), після чого відкривається вікно симулятора додатка Terminal із відповідним запрошенням до роботи (рис. 2.9) в операційній системі Cisco IOS. Зауважимо, що інформація у вікні терміналу та сама, що й на вкладці CLI у діалоговому вікні властивостей пристрою (див. рис. 2.3).

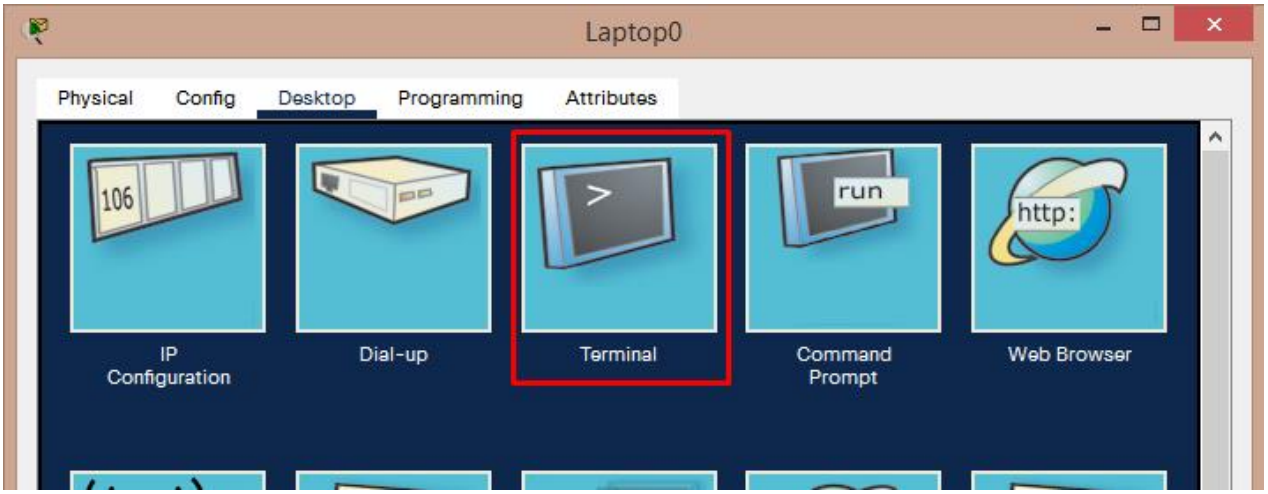

Рис. 2.7. Значок Terminal на вкладці Desktop

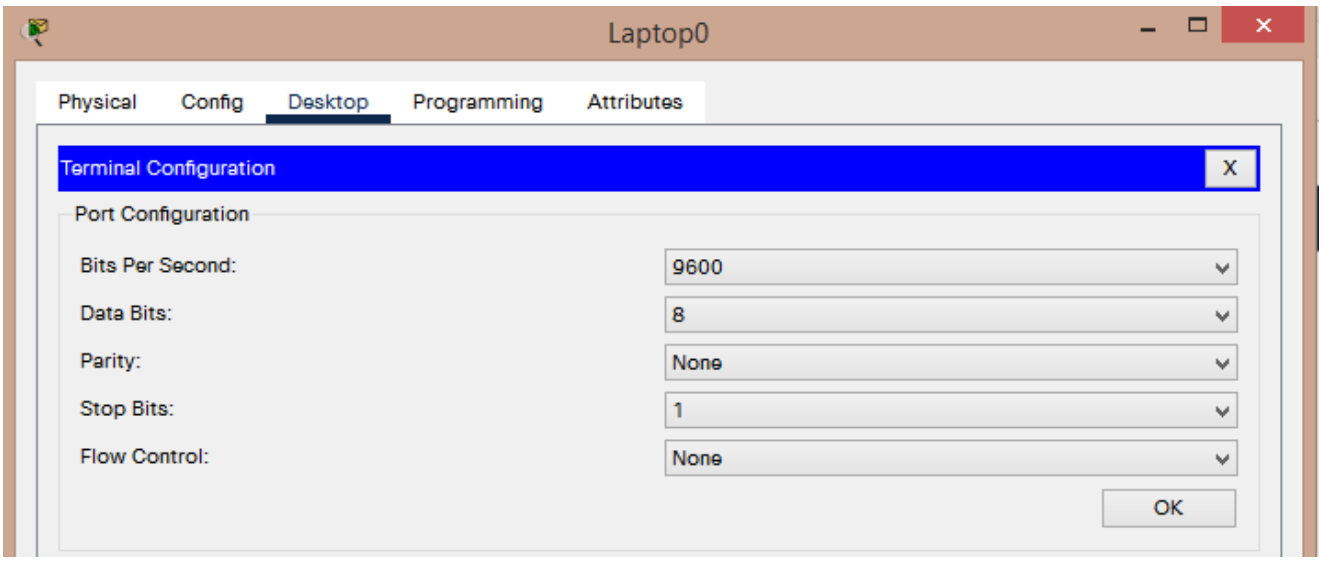

Рис. 2.8. Вікно настроювання параметрів симулятора додатка Terminal

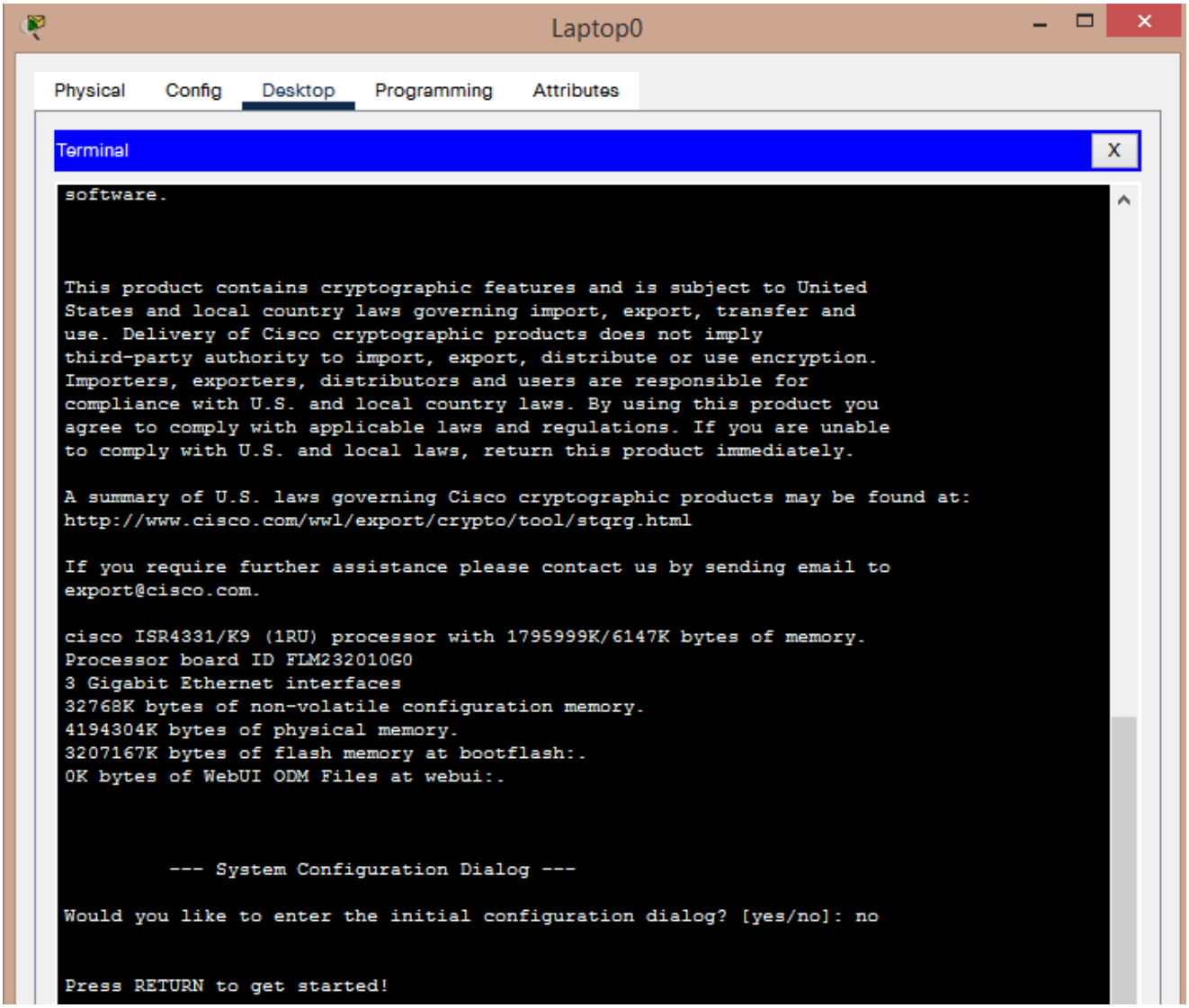

Рис. 2.9. Вікно симулятора додатка Terminal

Під’єднавши консоль і отримавши доступ до пристрою через командний рядок, користувач (адміністратор мережі або мережний інженер) може за допомогою різних команд задавати параметри конфігурації обладнання.

Основні show-команди у режимі користувача

Перейдіть у призначений для користувача режим командою disable. Для перегляду всіх доступних show-команд необхідно ввести у режимі користувача команду show?

Router1>show?

1. Команда show version використовується для отримання типу платформи мережного пристрою, версії операційної системи, імені файлу-образу операційної системи, часу роботи системи, обсягу пам’яті, кількості інтерфейсів і конфігураційного регістру.

Router1>show version

2. Перегляд часу:

Router1>show clock.

3. У флеш-пам’яті мережного пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від оперативної пам’яті, в реальних пристроях флеш-пам’ять зберігає файл-образ навіть при збої живлення.

Router1>show flash

4. Можна побачити список хостів і IP-адреси всіх їх інтерфейсів:

Router1>show hosts.

5. Виведення інформації про наявні інтерфейси:

Router1>show interfaces.

6. Виведення інформації про кожну telnet-сесію:

Router1>show sessions

7. Виведення конфігураційних параметрів терміналу:

Router1>show terminal.

8. Виведення списку всіх користувачів, приєднаних до пристрою по термінальних лініях:

Router1>show users.

Основні show-команди у привілейованому режимі

Після переходу в привілейований режим (Router1> en) для перегляду всіх доступних show-команд введіть таку команду:

Router1#show?

Привілейований режим містить усі show-команди, призначені для режиму користувача, і кілька нових.

Перегляд збереженої конфігурації:

Router1#show configuration
або
Router1#show running-config.

У свою чергу, збереження поточної конфігурації здійснюється за допомогою таких команд:

Router1#write memory
або
Router1#copy run start

Введення в конфігурацію інтерфейсів

Розглянемо команди настроювання інтерфейсів мережного пристрою. На мережному пристрої Router1 увійдемо в режим конфігурації:

Router1#config terminal (скорочено conf t)
Router1 (config) #

Тепер настроїмо Ethernet-інтерфейс. Для цього слід зайти в режим конфігурації інтерфейсу:

Router1 (config)#interface FastEthernet 0/0
або
Router1 (config)#int fa 0/0 (скорочене ім'я інтерфейсу)

Router1 (config-if)#

Список команд, доступних у цьому режимі, можна отримати за допомогою такої команди:

Router1 (config-if)#?

Вимкнути поточний інтерфейс у роутері можна за допомогою команди

Router1 (config-if)# shutdown

Важливо! За замовчуванням усі інтерфейси роутера вимкнені на відміну від інтерфейсів комутатора, які за замовчуванням увімкнені. Для кожної команди можна виконати протилежну команду, поставивши перед нею слово **no**.

Команда, яка включає цей інтерфейс:

Router1 (config-if) #no shutdown

За допомогою команди **ip address 192.168.1.1 255.255.255.0** можна призначити поточному інтерфейсу IP-адресу з відповідною маскою:

Router1 (config-if)#ip address 192.168.1.1 255.255.255.0

Переглянути таблицю маршрутизації (рис. 2.10) можна після виходу з режиму конфігурації інтерфейсу у привілейований режим командою

Router1 (config-if)#end
Router1#show ip route

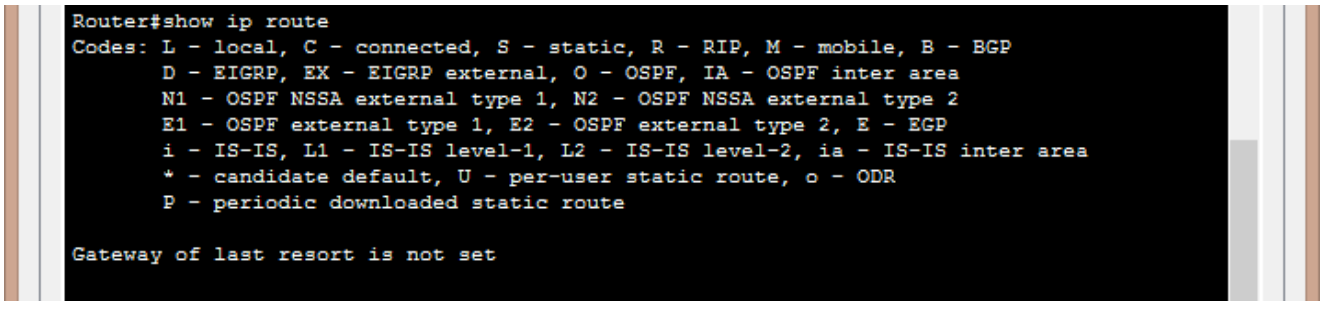

Рис. 2.10. Виведення таблиці маршрутизації

Додати опис до інтерфейсу можна командою

Router1 (config-if) #description Ethernet interface on Router 1

Щоб побачити опис цього інтерфейсу, треба перейти в привілейований режим і виконати команду **show interface**:

Router1 (config-if)#end
Router1#show interface

Ім'я пристрою (наприклад, *Router1* на *Router2*) змінюється за допомогою команди

Router1#conf t
Router1 (config)#hostname Router2
Router2 (config)#

Встановлення та зміна паролю на вхід у привілейований режим здійснюється командою **enable secret**. Наприклад, для встановлення паролю «12345» на вхід у привілейований режим роутера *Router2* необхідно у режимі конфігурації ввести команду

Router2(config)#enable secret 12345

Щоб перевірити це, необхідно перейти у режим користувача та спробувати увійти у привілейований режим. Без уведення паролю це буде неможливо (рис. 2.11).

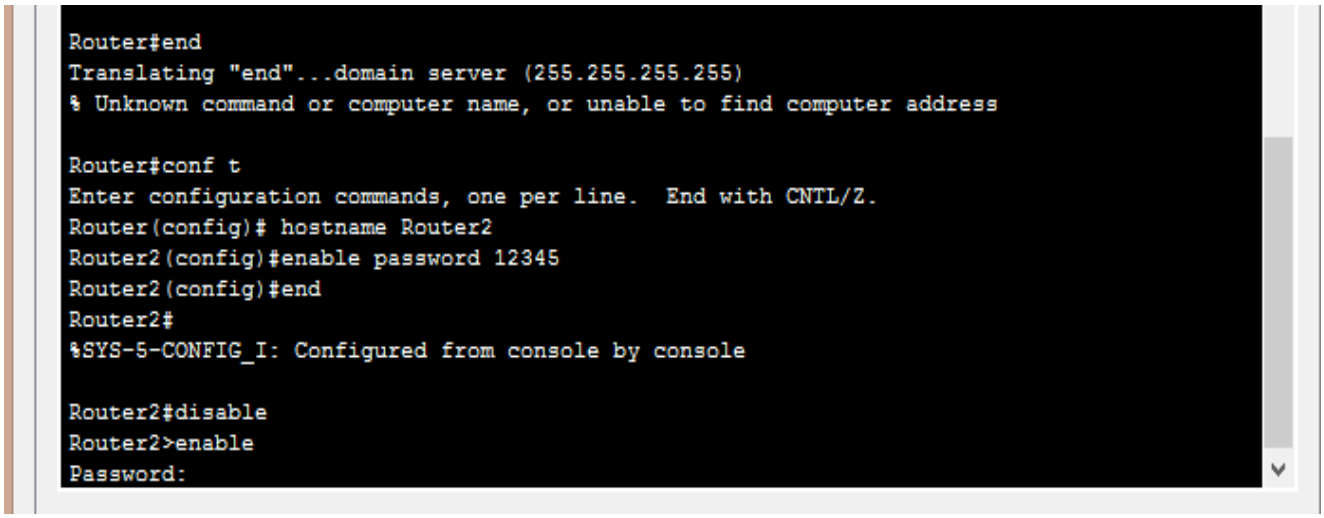

Рис. 2.11. Запрошення на введення паролю на вхід у привілейований режим

Для зміни паролю введемо новий пароль привілейованого режиму, як показано на рис. 2.12.

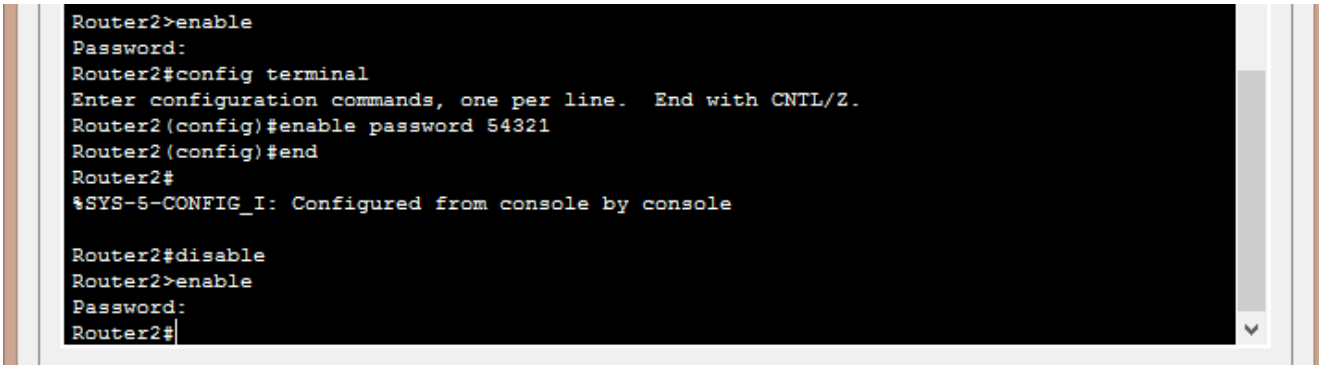

Рис. 2.12. Зміна паролю привілейованого режиму

Поради при роботі з CLI

Усі команди в консолі можна скорочувати, але важливо, щоб скорочення однозначно вказувало на команду. Керування введенням команд здійснюють за допомогою кнопок **стрілка вниз**, **Tab** і знак питання **?**. При натисканні **Tab** скорочена команда дописується до повної, а знак питання **?** після команди виводить список подальших можливостей і невелику довідку про них. Можна перейти до наступної команді, збереженої в буфері. Для цього натисніть на стрілку вниз або **Ctrl+N**. Можна повернутися до команд, введених раніше. Натисніть на стрілку вгору або **Ctrl+P**.

Команди з керування комутатором Cisco

При вході в комутатор командний рядок має такий вигляд:

Switch>

Команди для керування цим пристроєм здебільшого аналогічні командам з керування роутером Cisco, які були описані раніше.

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.
2. Побудуйте у Cisco **Paket Tracer** таку схему, як показано на рис. 2.13.
3. За допомогою команд **Cisco IOS** призначте комутатору і роутеру імена, а також паролі на вхід у привілейований режим згідно зі своїм варіантом (див. табл. 2.2). Настроювання комутатора проводити за допомогою вкладки **CLI**, а настроювання роутера – за допомогою консольного під’єднання.

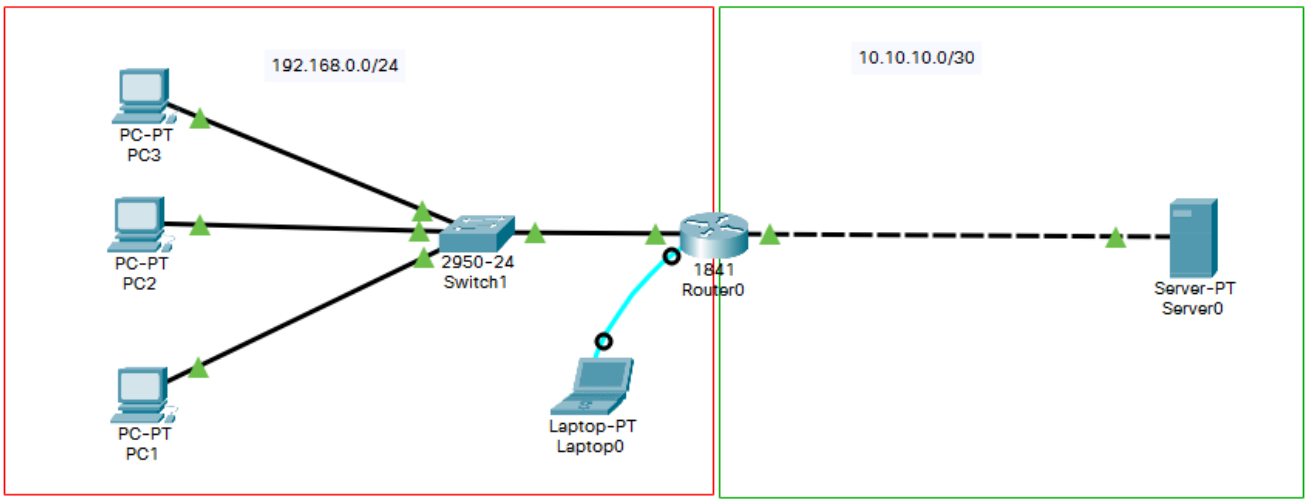

Рис. 2.13. Схема мережі з комутатором

4. За допомогою команд **Cisco IOS** настройте інтерфейси роутера першої та другої підмережі згідно з табл. 2.3.
5. Настройте інтерфейси кінцевих пристроїв підмереж згідно зі своїм варіантом (див. табл. 2.3).
6. Перевірте доступність сервера другої підмережі з комп'ютера PC1 першої підмережі за допомогою команди **ping** та WEB-браузера (на вкладці Desktop).
7. Виведіть таблицю маршрутизації роутера.

Вимоги до звіту

Звіт з лабораторної роботи має містити:
1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 2.2

Імена та паролі мережних пристроїв

Номер варіанта	Комутатор		Роутер	
	Ім'я	Пароль	Ім'я	Пароль
1, 11	Red	0001	London	000101
2, 12	Green	0002	Paris	000201

Закінчення табл. 2.2

Номер варіанта	Комутатор		Роутер	
	Ім’я	Пароль	Ім’я	Пароль
3, 13	Yellow	0003	Belgrade	000301
4, 14	Black	0004	Berlin	000401
5, 15	White	0005	Bratislava	000501
6, 16	Cherry	0006	Brussels	000601
7, 17	Orange	0007	Dublin	000701
8, 18	Pink	0008	Kiev	000801
9, 19	Blue	0009	Madrid	000901
10, 20	Rouse	0010	Monaco	001001

Таблиця 2.3

IP-адреси пристроїв

Номер варіанта	IP-адреси пристроїв першої підмережі			
	PC1	PC2	PC3	Gateway
1, 11	192.168.0.11	192.168.0.21	192.168.0.31	192.168.0.201
2, 12	192.168.0.12	192.168.0.22	192.168.0.32	192.168.0.202
3, 13	192.168.0.13	192.168.0.23	192.168.0.33	192.168.0.203
4, 14	192.168.0.14	192.168.0.24	192.168.0.34	192.168.0.204
5, 15	192.168.0.15	192.168.0.25	192.168.0.35	192.168.0.205
6, 16	192.168.0.16	192.168.0.26	192.168.0.36	192.168.0.206
7, 17	192.168.0.17	192.168.0.27	192.168.0.37	192.168.0.207
8, 18	192.168.0.18	192.168.0.28	192.168.0.38	192.168.0.208
9, 19	192.168.0.19	192.168.0.29	192.168.0.39	192.168.0.209
10, 20	192.168.0.20	192.168.0.30	192.168.0.40	192.168.0.210

Контрольні запитання

1. У яких режимах здійснюється робота у командному рядку?
2. У якій вкладці в симуляторі Cisco Packet Tracer реалізована додаткова можливість доступу до командного рядка операційної системи Cisco IOS?
3. Яку назву має консольний порт, через який здійснюють програмування пристроїв CISCO?
4. За допомогою якої команди можна переглянути поточний час пристрою CISCO?
5. Яка команда відповідає за перегляд поточної конфігурації пристрою CISCO?
6. Яка різниця між початковим станом інтерфейсів у роутера та комутатора?

Лабораторна робота № 3

НАСТРОЮВАННЯ ЛОКАЛЬНИХ ВІРТУАЛЬНИХ МЕРЕЖ. КЕРУВАННЯ МЕРЕЖНИМИ ПРИСТРОЯМИ ЗА ПРОТОКОЛАМИ TELNET ТА SSH

Мета роботи: вивчити процес створення віртуальних локальних мереж та керування мережними пристроями за допомогою термінального доступу за протоколами **Telnet** та **SSH**.

Теоретичні відомості

Схема мережі

Розглянемо схему мережі, зображену на рис. 3.1.

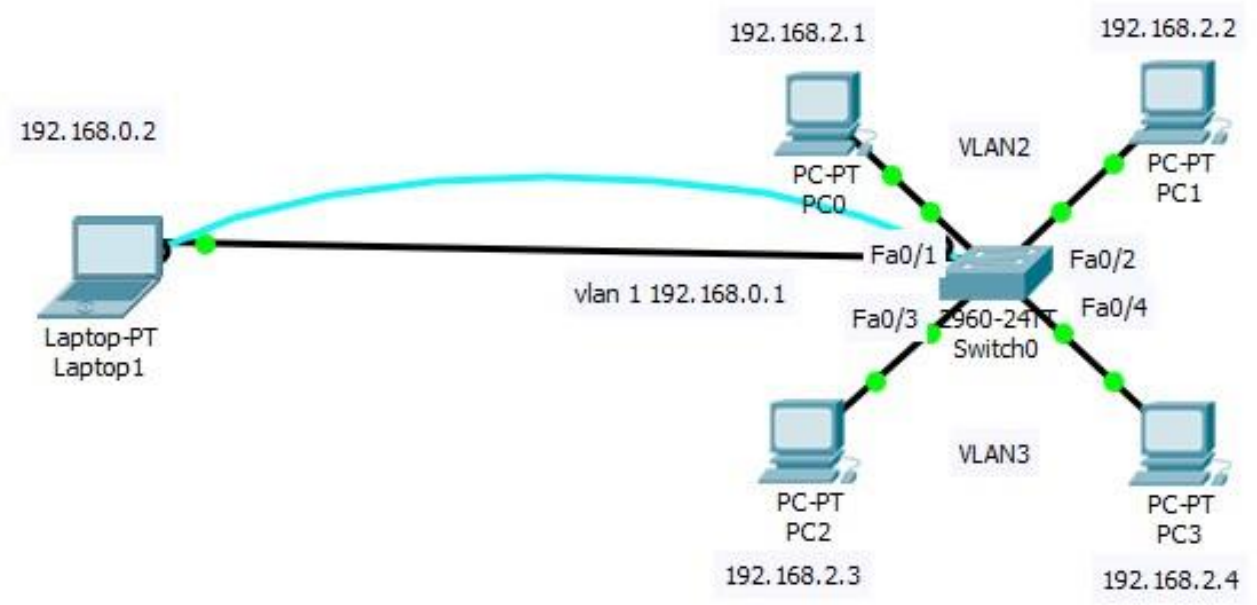

Рис. 3.1. Схема мережі

На базі цієї схеми потрібно:

- створити віртуальні локальні мережі vlan3 та vlan2;
- настроїти мережні пристрої хостів згідно з обраною підмережею;
- призначити нативному vlan1 IP-адресу для керування мережним пристроєм (комутатором);
- настроїти з'єднання керівного комп'ютера з мережним пристроєм за допомогою протоколів **Telnet** та **SSH**.

Первинне настроювання комутатора робимо за допомогою консольного з'єднання (див. лабораторну роботу № 2).

По-перше, необхідно призначити нативному Vlan1 (за замовчуванням) IP-адресу та настроїти відповідний інтерфейс на керівному комп'ютері (Laptop 1).

Switch>*enable*
Switch*#*
Switch*#conf t*
Switch(config)*#int vlan 1*
Switch(config-if)*#no shutdown*
Switch(config-if)*#*
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)*#ip address 192.168.0.1 255.255.255.0*
Switch(config-if)*#end*
Switch*#*

Керування пристроєм через командний рядок за протоколом Telnet

Система підтримує 20 віртуальних **tty/vty**-ліній для **Telnet**, **SSH** та **FTP**-сервісів. Кожна сесія, яка використовує наведені вище протоколи, займає одну лінію.

Щоб настроїти аутентифікацію, перейдіть назад у режим загальної конфігурації (conf t) на комутаторі та введіть такі команди:

Switch>*ena*
Switch*#conf t*
Switch(config)*#enable secret 12345 / Пароль на вхід у привілейований режим потрібен як ступінь додаткового захисту для з'єднання за протоколом Telnet*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)*#line vty 0 15 / Настроювання лінії*
Switch(config-line)*#password* ***cisco*** */ Установлення паролю 'cisco'*
Switch(config-line)*#login*
Switch(config-line)*#end*
Switch*#wr*

На керівному комп'ютері настроїмо мережний адаптер, щоб він знаходився в одній підмережі з керівним VLAN 1 комутатора (наприклад, 192.168.0.2/24) і в режимі командного рядка наберемо таку команду (рис. 3.2):

C:\>*telnet 192.168.0.1*

Далі введемо пароль:

Password: *cisco*

Рис. 3.2. З’єднання за протоколом Telnet

Зробимо подальше настроювання, встановивши протокол SSH. Змінимо ім’я пристрою:

Switch(config)#*hostname SW1*
SW1(config)#*do wr*

Створимо обліковий запис адміністратора:

SW1(config)#*username admin secret ******

Замість зірок ***** задамо пароль для облікового запису, наприклад «**admin**».

Настроювання SSH

Під час використання протоколу Telnet (TCP-порт 23) усі команди та дані про конфігурацію пристрою передаються у відкритому вигляді, що потенційно небезпечно. Для захисту підключення використовується протокол SSH (TCP-порт 22).

Для настроювання підключення через протокол SSH слід задати ім’я домену (будь-яке), згенерувати криптографічний ключ доступу та включити сам протокол SSH версії 2.

SW1 (config)#*ip domain-name deltaconfig.ua*
SW1 (config)#*crypto key generate rsa*
Далі буде виведено пропозицію змінити кількість біт у ключі:

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

Після запиту необхідно вказати 1024.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW1 (config)#*ip ssh ver 2*

Обмеження підключення до маршрутизатора тільки через SSH:

SW1 (config)#*line vty 0 15*
SW1 (config-line)#*transport input ssh*
SW1 (config-line)#*end*

Збережемо конфігурацію:

SW1#*wr*

За допомогою командного рядка з'єднаємось з комутатором **SW1** з використанням протокола SSH, ввівши встановлений раніше пароль «**admin**» (рис. 3.3).

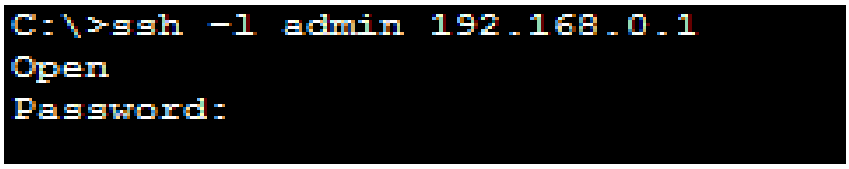

Рис. 3.3. З'єднання за протоколом SSH

Подальші настройки вводимо з командного рядка.

Увімкнення Vlan 3 і Vlan 2

SW1#*conf t*
Enter configuration commands, one per line. End with CNTL/Z.
SW1 (config)#*int vlan 2*
SW1 (config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
SW1 (config-if)#*no shutdown*
SW1 (config-if)#*exit*
SW1 (config)#*int vlan 3*
SW1 (config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up
SW1 (config-if)#*no shutdown*
SW1 (config-if)#*exit*

Призначення імен Vlan 2 і Vlan 3

SW1 (config)#*vlan 2*
SW1 (config-vlan)#*name buhgalter*
SW1 (config-vlan)#*exit*
SW1 (config)#*vlan 3*
SW1 (config-vlan)#*name sklad*
SW1 (config-vlan)#*exit*

Настроювання портів Fastethernet 0/1 і 0/2

SW1(config)#
SW1(config)#*int fa 0/1*
SW1(config-if)#*switch mode access*
SW1(config-if)#*switchport access vlan 2*
SW1(config-if)#*exit*
SW1(config)#*int fa 0/2*
SW1(config-if)#*switch mode access*
SW1(config-if)#*switchport access vlan 2*
SW1(config-if)#*exit*
SW1(config)#

Настроювання групи портів Fastethernet 0/3 і 0/4

SW1(config)#*int range fa 0/3-4*
SW1(config-if-range)#*switchport mode access*
SW1(config-if-range)#*switchport access vlan 3*
SW1(config-if-range)#*exit*
SW1(config)#

Виведення короткої інформації про конфігурацію VLAN

SW1#*show vlan brief*

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    buhgalter                         active    Fa0/1, Fa0/2
3    sklad                             active    Fa0/3, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

SW1#*wr*

Додавання порту у Vlan1 (за замовчуванням) для керування комутатором

Додамо порт 24 у Vlan 1 для подальшого підключення до нього керівного комп’ютера по Ethernet.

SW1#*conf t*
SW1(config)#*int fa 0/24*
SW1(config-if)#*switch mode access*
SW1(config-if)#*switchport access vlan 1*
SW1(config-if)#*exit*
SW1(config)#*exit*
SW1#
%SYS-5-CONFIG_I: Configured from console by console
SW1#*wr*
Building configuration...
[OK]
SW1#

Створення мережі із двох комутаторів

Настроювання мережі (рис. 3.4) робимо згідно з алгоритмом, описаним у пп. 1.1–1.3.

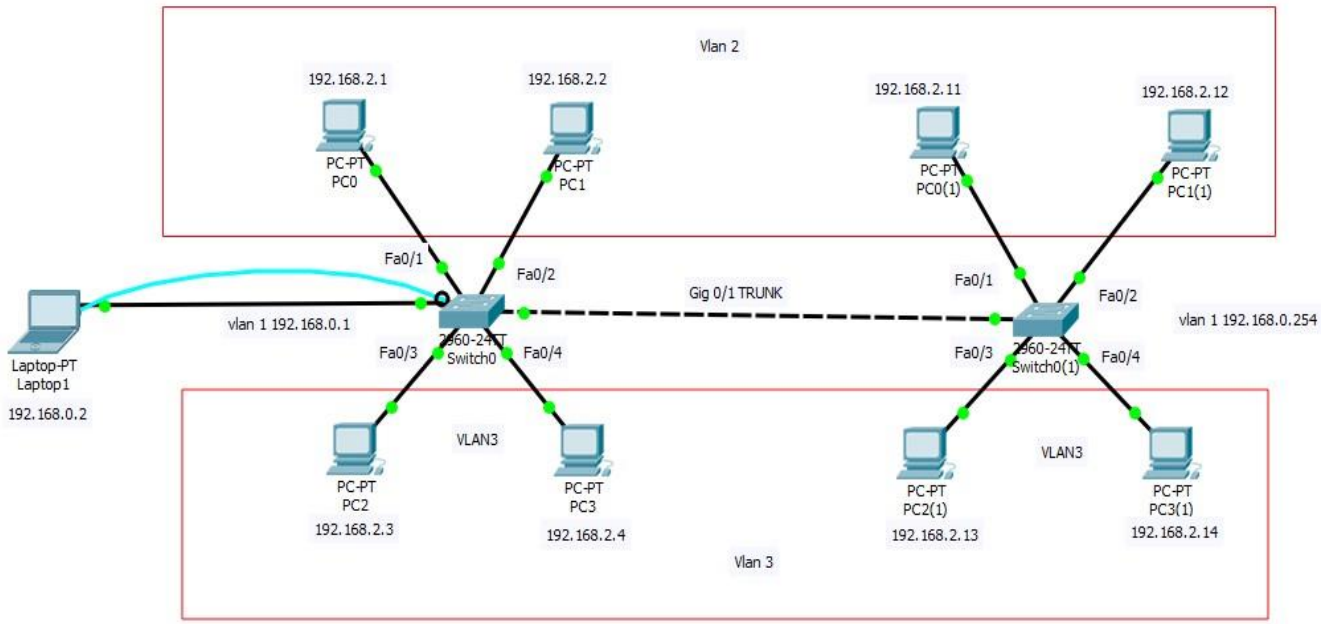

Рис. 3.4. Мережа з двома комутаторами

Настроювання з’єднання комутаторів через транковий порт GigabitEthernet

Для з’єднання комутаторів будемо використовувати порти GigabitEthernet 0/1 комутаторів, надавши їм статус транкових. Для з’єднання будемо використовувати крос-кабель.

Транковий порт мережного пристрою (trunk port) – це порт на комутаторі або маршрутизаторі, призначений для передавання трафіку кількох VLAN (віртуальних локальних мереж) між мережними пристроями. Він забезпечує одночасне передавання кадрів кількох VLAN через один фізичний порт за допомогою тегування кадрів. Тегування зазвичай виконується за допомогою протоколу IEEE 802.1Q, де кожен кадр отримує спеціальний тег, що ідентифікує, до якого VLAN він належить.

Введемо такі команди:

Switch>*ena /Вхід у привілейований режим*
Password: */Введення паролю привілейованого режиму*
Switch#*conf t*
Switch(config)#*int gig 0/1*
Switch(config-if)#*switchport mode trunk*
Switch(config-if)#*switchport trunk allow vlan 1-3 / Можливе перерахування з використанням коми*
Switch(config-if)#*end*
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#*wr*
Switch#

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.
2. Побудуйте у **Cisco Paket Tracer** таку схему, як показано на рис. 3.4.
3. Призначте IP-адреси кінцевих пристроїв згідно зі своїм варіантом (табл. 3.1).
4. Проведіть первинне настроювання другого комутатора за допомогою консольного з’єднання (ip address).
5. Подальше настроювання проведіть за допомогою термінального з’єднання по протоколу SSH (зберегти пароль «cisco»).
6. Змініть імена мережних пристроїв та встановіть пароль на привілейований режим згідно зі своїм варіантом (табл. 3.2).
7. Перевірте доступність комп’ютерів у відповідних Vlan за допомогою команди **ping**.

Вимоги до звіту

Звіт з лабораторної роботи має містити:

1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 3.1

IP-адреси пристроїв

Номер варіанта	Адреси пристроїв підмережі			
	PC1	PC2	PC3	PC4
1, 11	192.168.2.11	192.168.2.21	192.168.2.31	192.168.2.41
2, 12	192.168.2.12	192.168.2.22	192.168.2.32	192.168.2.42
3, 13	192.168.2.13	192.168.2.23	192.168.2.33	192.168.2.43
4, 14	192.168.2.14	192.168.2.24	192.168.2.34	192.168.2.44
5, 15	192.168.2.15	192.168.2.25	192.168.2.35	192.168.2.45
6, 16	192.168.2.16	192.168.2.26	192.168.2.36	192.168.2.46
7, 17	192.168.2.17	192.168.2.27	192.168.2.37	192.168.2.47
8, 18	192.168.2.18	192.168.2.28	192.168.2.38	192.168.2.48
9, 19	192.168.2.19	192.168.2.29	192.168.2.39	192.168.2.49
10, 20	192.168.2.20	192.168.2.30	192.168.2.40	192.168.2.50
	Адреси пристроїв підмережі			
	PC5	PC6	PC7	PC8
1, 11	192.168.2.61	192.168.2.71	192.168.2.81	192.168.2.91
2, 12	192.168.2.62	192.168.2.72	192.168.2.82	192.168.2.92
3, 13	192.168.2.63	192.168.2.73	192.168.2.83	192.168.2.93
4, 14	192.168.2.64	192.168.2.74	192.168.2.84	192.168.2.94
5, 15	192.168.2.65	192.168.2.75	192.168.2.85	192.168.2.95
6, 16	192.168.2.66	192.168.2.76	192.168.2.86	192.168.2.96
7, 17	192.168.2.67	192.168.2.77	192.168.2.87	192.168.2.97
8, 18	192.168.2.68	192.168.2.78	192.168.2.88	192.168.2.98
9, 19	192.168.2.69	192.168.2.79	192.168.2.89	192.168.2.99
10, 20	192.168.2.70	192.168.2.80	192.168.2.90	192.168.2.100

Таблиця 3.2

Імена та паролі мережних пристроїв

Номер варіанта	Switch 1		Switch 2	
	Ім’я	Пароль	Ім’я	Пароль
1, 11	Red	0001	London	000101
2, 12	Green	0002	Paris	000201
3, 13	Yellow	0003	Belgrade	000301
4, 14	Black	0004	Berlin	000401
5, 15	White	0005	Bratislava	000501
6, 16	Cherry	0006	Brussels	000601
7, 17	Orange	0007	Dublin	000701
8, 18	Pink	0008	Kiev	000801
9, 19	Blue	0009	Madrid	000901
10, 20	Rouse	0010	Monaco	001001

Контрольні запитання

1. Що таке нативний Vlan?
2. Скільки одночасно віртуальних tty/vty-ліній для Telnet, SSH та FTP-сервісів підтримує система?
3. Що означає префікс /24 у IP-адресі 192.168.0.2/24?
4. Які порти за замовчуванням призначаються протоколам Telnet та SSH?
5. У чому полягає різниця між протоколами Telnet та SSH?

Лабораторна робота № 4

НАСТРОЮВАННЯ МАРШРУТИЗАЦІЇ У ЛОКАЛЬНІЙ МЕРЕЖІ

Мета роботи: вивчити процес настроювання маршрутизації в локальній мережі між різними підмережами за допомогою роутера Cisco.

Теоретичні відомості

Загальна схема мережі

Розглянемо схему мережі (рис. 4.1).

Маємо один маршрутизатор (Cisco 1841), і до одного з його інтерфейсів (FastEthernet0/0) підключено декілька приватних мереж за допомогою комутатора (Cisco 2960). Адреси мереж: 192.168.2.0/24; 192.168.3.0/24 та 192.168.4.0/24 відповідно. Для простоти уявимо кожну мережу як один комп'ютер. Комутатор настроїмо таким чином, щоб кожна мережа знаходилася в окремому VLAN і комутатор був з'єднаний транковим портом з відповідним інтерфейсом маршрутизатора.

Настроювання маршрутизатора для маршрутизації всередині локальної мережі будемо проводити за допомогою SUB-інтерфейсів.

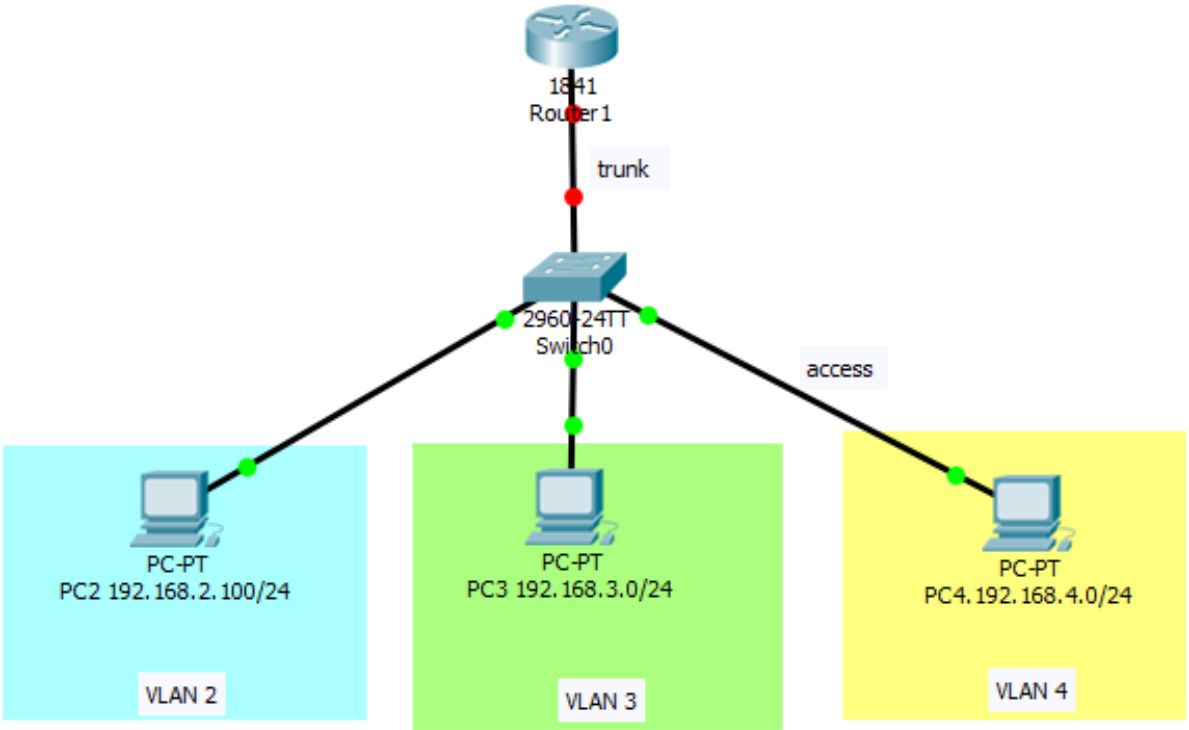

Рис. 4.1. Схема мережі

SUB-інтерфейс – це віртуальний інтерфейс, створений шляхом поділу одного фізичного інтерфейсу на кілька логічних інтерфейсів. Вторинний інтерфейс у маршрутизаторі Cisco використовує батьківський фізичний інтерфейс для надсилання та отримання даних.

Настроювання комутатора

Перше, що необхідно зробити, це створити три VLAN і призначити їм відповідні імена.

Для цього в режимі конфігурації введемо такі команди:

Switch(config)#*vlan 2*
Switch(config-vlan)#*name VLAN2*
Switch(config-vlan)#*exit*
Switch(config)#*vlan 3*
Switch(config-vlan)#*name VLAN3*
Switch(config-vlan)#*exit*
Switch(config)#*vlan 4*
Switch(config-vlan)#*name VLAN4*
Switch(config-vlan)#*exit*
Switch(config)#*do* write (це аналог команди **write**, але за допомогою **do** її можна застосувати в режимі конфігурації)
Building configuration...
[OK]
Switch(config)#

Далі настроїмо відповідні порти комутатора в режимі **access** та віднесемо їх до відповідних VLAN.

Switch(config)#*interface fastethernet0/2*
Switch(config-if)#*switchport mode access*
Switch(config-if)#*switchport access vlan 2*
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
Switch(config-if)#*exit*
Switch(config)#*interface fastethernet0/3*
Switch(config-if)#*switchport mode access*
Switch(config-if)#*switchport access vlan 3*
Switch(config-if)#
Switch(config-if)#*exit*
Switch(config)#*interface fastethernet0/4*

Switch(config-if)#*switchport mode access*
Switch(config-if)#*switchport access vlan 4*
Switch(config-if)#
Switch(config-if)#*end*
Switch#*write*

Виведемо інформацію про активні VLAN за допомогою такої команди:

Switch#*show vlan brief*

Результати роботи цієї команди показано на рис. 4.2.

```
Switch#sh vlan br
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/5, Fa0/6,
Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10,
Fa0/11
                                                Fa0/12, Fa0/13,
Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17,
Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21,
Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
2    VLAN2                            active    Fa0/2
3    VLAN3                            active    Fa0/3
4    VLAN4                            active    Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
Switch#
Switch#
Switch#
```

Рис. 4.2. Результат виконання команди show vlan brief

Тепер необхідно настроїти порт, з’єднаний з маршрутизатором (**fastethernet0/1**) у режимі **TRUNK**, та вказати відповідні VLAN, тегований трафік від яких передаватиметься через цей порт.

Switch(config)#*interface fastethernet0/1*
Switch(config-if)#*switchport mode trunk*
Switch(config-if)#*switchport trunk allowed vlan 2,3,4*
Switch(config-if)#
Switch(config-if)#*end*
Switch#*write*

Далі перейдемо до настроювання маршрутизатора.

Настроювання маршрутизатора

У першу чергу переведемо з'єднаний з комутатором інтерфейс **fastethernet0/0** у стан **Up**.

Router>*enable*
Router#*config terminal*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#*interface fastethernet0/0*
Router(config-if)#*no shutdown*
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#*end*
Router#*write*

Тепер створимо на основному інтерфейсі так звані Sub-інтерфейси, пов'язані з відповідними VLAN. У нашому випадку (див. рис. 4.1) номери VLAN – 2, 3, 4, причому відповідний номер VLAN ставится після операнда *dot1Q,* як у командах, наведених нижче.

Router(config)# *interface fastethernet0/0.2*
Router(config-subif)#*encapsulation dot1Q* ***2***
Router(config-subif)#*ip address 192.168.2.1 255.255.255.0*
Router(config-subif)#*no shutdown*
Router(config-subif)#*exit*
Router(config)# *interface fastethernet0/0.3*
Router(config-subif)#*encapsulation dot1Q* ***3***
Router(config-subif)#*ip address 192.168.3.1 255.255.255.0*
Router(config-subif)#*no shutdown*
Router(config-subif)#*exit*
Router(config)# *interface fastethernet0/0.4*
Router(config-subif)#*encapsulation dot1Q* ***4***
Router(config-subif)#*ip address 192.168.4.1 255.255.255.****0***
Router(config-subif)#*no shutdown*
Router(config-subif)#*end*
Router#*write*

Переглянемо результат за допомогою команди **show run.**

Router#*show run*

Результати роботи цієї команди показано на рис. 4.3.

```
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
```

Рис. 4.3. Виведення інформації за допомогою команди show run

Далі настроїмо відповідні мережні інтерфейси комп'ютерів приватних підмереж (рис. 4.4).

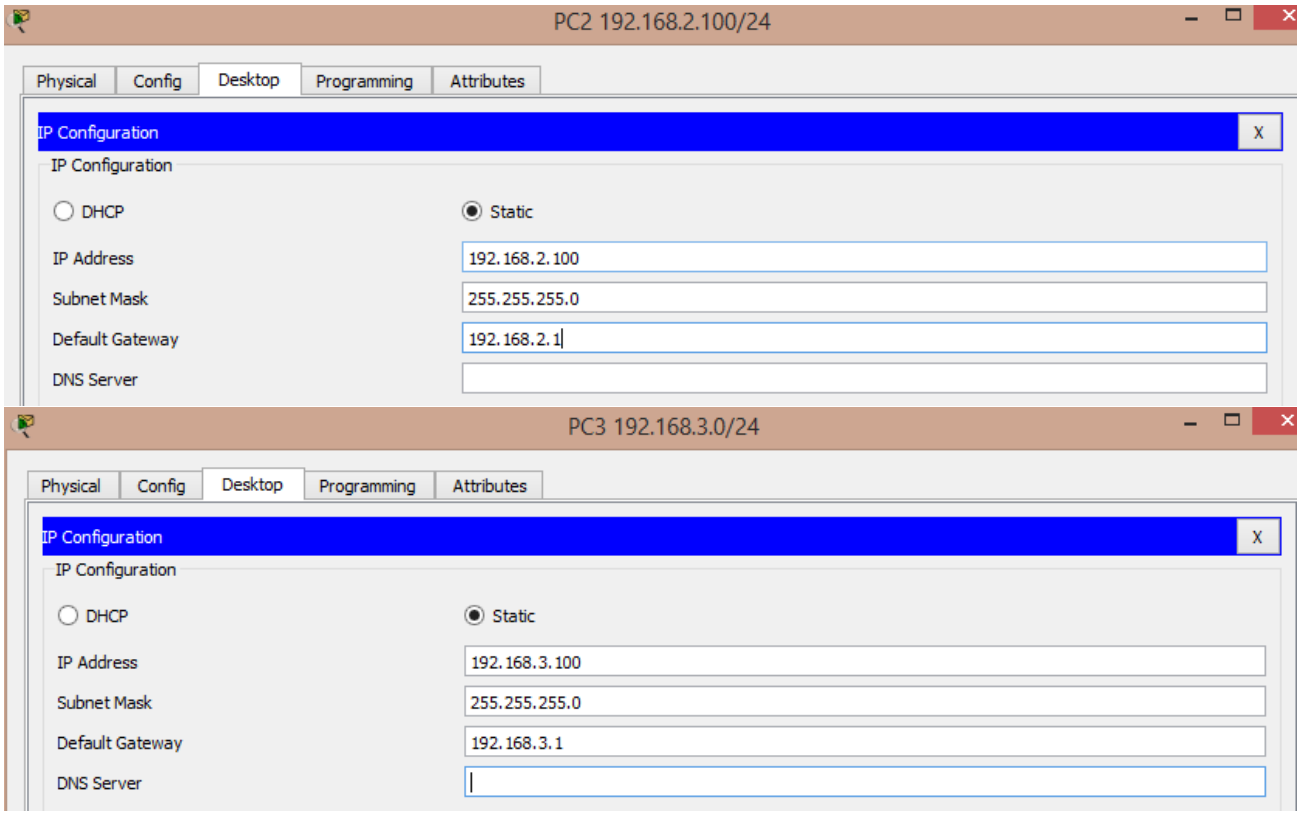

Рис. 4.4. Настроювання мережних інтерфейсів комп'ютерів

Виконаємо команду ping і переконаємося, що ця команда виконана успішно і, отже, настроєна нами внутрішня маршрутизація працює (рис. 4.5).

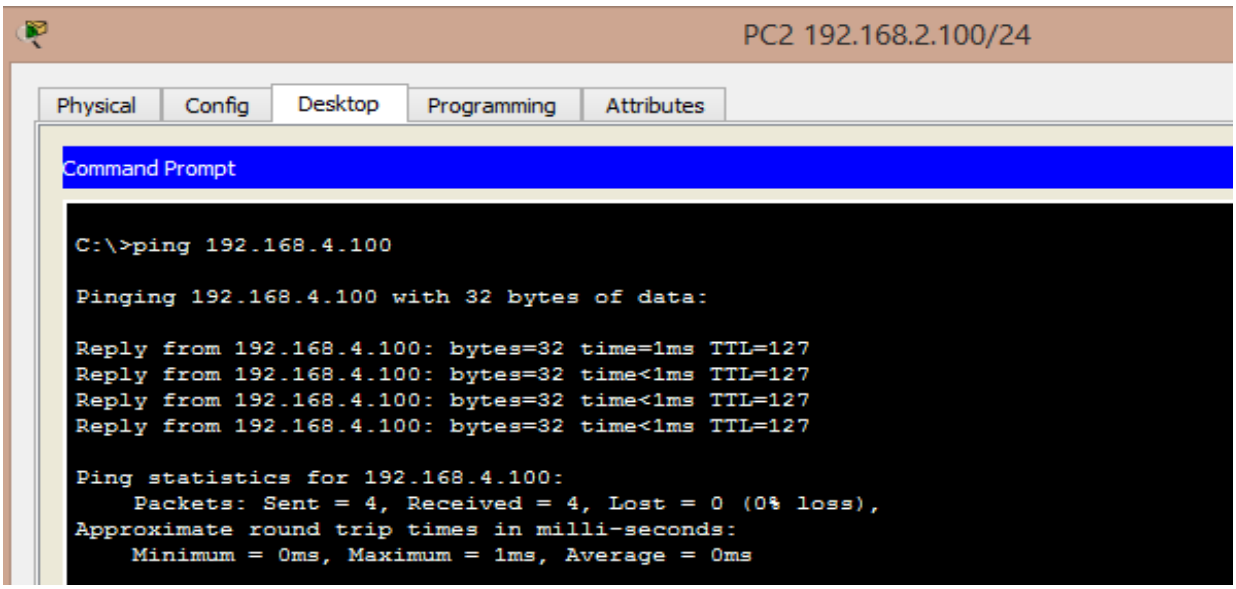

Рис. 4.5. Результати роботи команди ping

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.
2. Побудуйте у Cisco Paket Tracer таку схему, як показано на рис. 4.1.
3. Призначте IP-адреси кінцевих пристроїв згідно зі своїм варіантом (табл. 4.1).
4. Настройте комутатор за допомогою консольного з’єднання, призначивши номери VLAN згідно зі своїм варіантом (табл. 4.2).
5. Виведіть на екран поточну конфігурацію VLAN комутатора за допомогою команди **show vlan brief**.
6. Настройте маршрутизатор, користуючись вкладкою CLI.
7. Виведіть на екран поточну конфігурацію sub-інтерфейсів маршрутизатора за допомогою команди **show run**.
8. Перевірте доступність комп’ютерів у мережі за допомогою команди **ping**.

Вимоги до звіту

Звіт з лабораторної роботи має містити:

1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 4.1

IP-адреси пристроїв

Номер варіанта	IP-адреси пристроїв підмереж		
	PC2 перша підмережа	PC3 друга підмережа	PC4 третя підмережа
1, 11	192.168.2.21	192.168.3.31	192.168.4.41
2, 12	192.168.2.22	192.168.3.32	192.168.4.42
3, 13	192.168.2.23	192.168.3.33	192.168.4.43
4, 14	192.168.2.24	192.168.3.34	192.168.4.44
5, 15	192.168.2.25	192.168.3.35	192.168.4.45
6, 16	192.168.2.26	192.168.3.36	192.168.4.46
7, 17	192.168.2.27	192.168.3.37	192.168.4.47
8, 18	192.168.2.28	192.168.3.38	192.168.4.48
9, 19	192.168.2.29	192.168.3.39	192.168.4.49
10, 20	192.168.2.30	192.168.3.40	192.168.4.50
Варіант	Адреси шлюзів у підмережах		
	перша підмережа	друга підмережа	третя підмережа
1-20	192.168.2.1	192.168.3.1	192.168.4.1

Таблиця 4.2

Номери VLAN

Номер варіанта	Адреси підмереж		
	Перша підмережа	Друга підмережа	Третя підмережа
1, 11	vlan 2	vlan 3	vlan 4
2, 12	vlan 5	vlan 6	vlan 7
3, 13	vlan 8	vlan 9	vlan 10
4, 14	vlan 11	vlan 12	vlan 13
5, 15	vlan 14	vlan 15	vlan 16
6, 16	vlan 17	vlan 18	vlan 19
7, 17	vlan 20	vlan 21	vlan 22
8, 18	vlan 23	vlan 24	vlan 25
9, 19	vlan 26	vlan 27	vlan 28
10, 20	vlan 29	vlan 30	vlan 31

Контрольні запитання

1. Що таке VLAN?
2. З якою метою настроюють маршрутизацію у локальній мережі?
3. Що таке SUB-інтерфейс?
4. Яка різниця між TRUNK-портом та портом ACCESS?
5. Що таке тегований трафік?

Лабораторна робота № 5

НАСТРОЮВАННЯ СЕРВЕРА DHCP У ЛОКАЛЬНІЙ МЕРЕЖІ

Мета роботи: вивчити процес та команди настроювання сервера DHCP у локальній мережі за допомогою обладнання Cisco.

Теоретичні відомості

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічного настроювання вузла) – мережний протокол прикладного рівня, що забезпечує надання IP-адрес та відомостей про мережу хостам, які під'єднуються до мережі. Після отримання цих параметрів хост стає повноправним вузлом мережі та може обмінюватися пакетами у мережі.

На рис. 5.1 показано заголовок протоколу DHCP. Короткий опис кожного поля:

op – тип повідомлення (1 = BOOTREQUEST, 2 = BOOTREPLY);

htype – тип апаратної адреси (наприклад, 1 для Ethernet);

hlen – розмір апаратної адреси (наприклад, 6 для Ethernet);

hops – кількість ретрансляторів, які надіслали DHCP-повідомлення;

xid – ідентифікатор транзакції. Випадкове число, що однозначно визначає діалог між клієнтом і сервером;

secs – кількість секунд від початку процесу отримання або оновлення адреси, яку вказує клієнт;

flags – прапорці;

ciaddr – поточна IP-адреса клієнта;

yiaddr – IP-адреса, яку DHCP-сервер пропонує клієнту;

siaddr – IP-адреса сервера для наступного сервера в процесі конфігурації. Зазвичай використовується для завантаження образу операційної системи;

giaddr – адреса ретранслятора, який передав DHCP-повідомлення;

chaddr – апаратна адреса клієнта;

sname – ім'я наступного сервера у процесі конфігурації;

file – ім'я файлу, що запитується клієнтом із сервера, наприклад, файлу операційної системи;

options – перелік параметрів.

DHCP інкапсулює свої дейтаграми у протокол UDP. Клієнт при цьому слухає порт 67, а сервер – порт 68. Протокол UDP було вибрано тому, що повідомлення DHCP не перевищує максимально можливий розмір корисного навантаження в UDP, отже, не потрібно розв'язувати проблему передачі пакетів у потрібному порядку, а також тому, що у DHCP є механізм повторного відправлення пакета, якщо він не дійшов до отримувача.

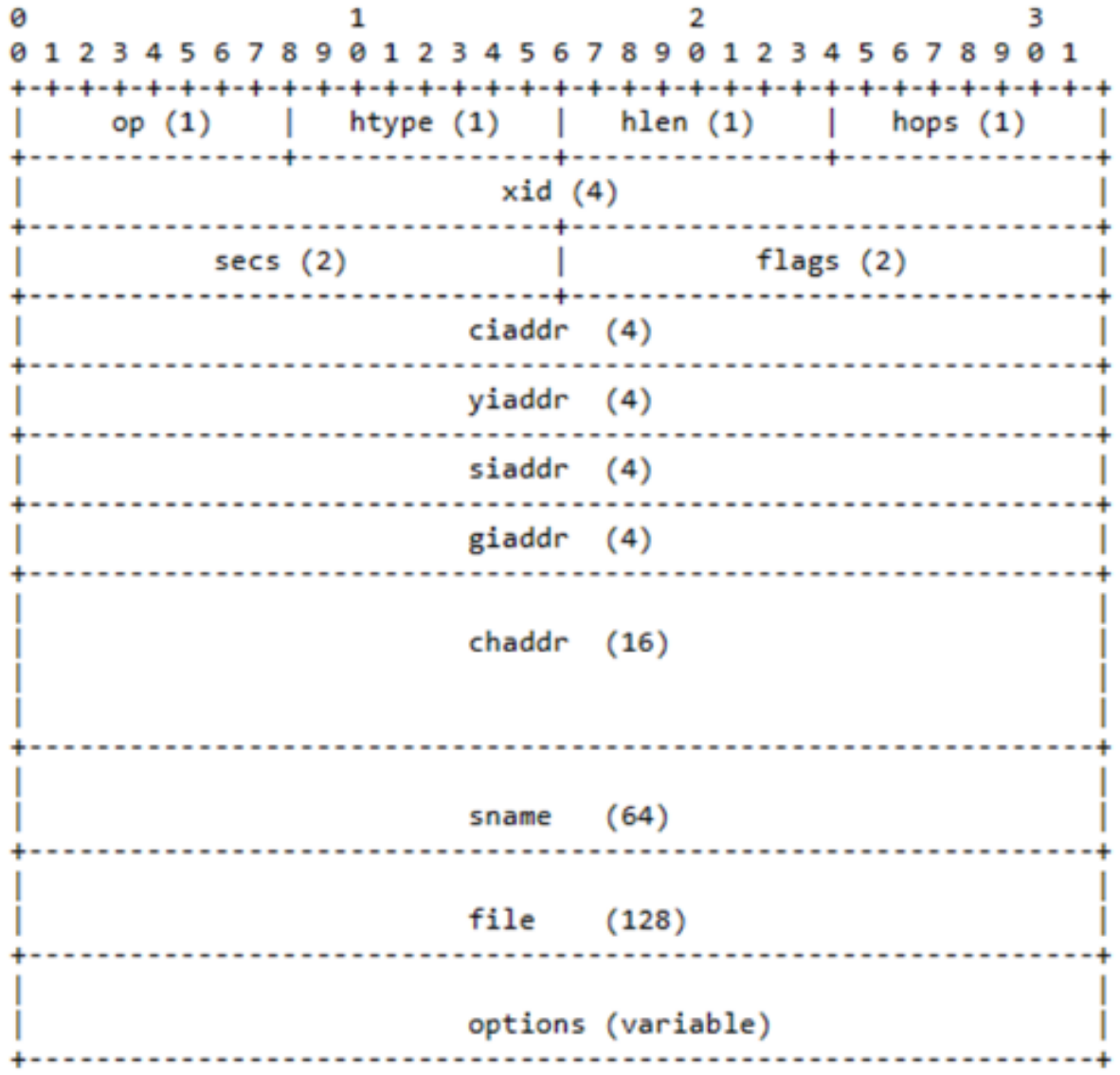

Рис. 5.1. Заголовок DHCP

Поле **op** у випадку повідомлення клієнта містить значення **1** (BOOTREQUEST), а у випадку повідомлення сервера – **2** (BOOTREPLY). Кожне DHCP-повідомлення містить опцію **DHCP Message Type**, яка вказує на тип повідомлення:

1. **DHCPDISCOVER** – широкомовне повідомлення клієнта, який хоче розпочати процес виділення IP-адреси.
2. **DHCPOFFER** – відгук від сервера на DHCPDISCOVER, що містить інформацію про доступну IP-адресу та інші параметри конфігурації мережі.
3. **DHCPREQUEST** – повідомлення від клієнта для: а) підтвердження отриманих параметрів від сервера; б) підтвердження права використання раніше виділеної адреси; в) продовження терміну оренди.

4. **DHCPACK** – відгук сервера на DHCPREQUEST, що підтверджує виділену раніше IP-адресу та параметри мережі.
5. **DHCPNACK** – відгук сервера на DHCPREQUEST, що повідомляє про непридатність запитуваної IP-адреси.
6. **DHCPDECLINE** – повідомлення від клієнта про те, що видана в DHCPOFFER адреса зайнята.
7. **DHCPRELEASE** – повідомлення клієнта про звільнення мережної адреси.
8. **DHCPINFORM** – запит від клієнта, який вже має IP-адресу, але не має параметрів мережі.

Принцип роботи DHCP

Коли комп'ютер з'являється в локальній мережі (рис. 5.2), насамперед він відсилає в мережу широкомовний запит до всіх, хто в мережі. Цей пакет називається **DHCPDISCOVER**, в якому він запитує, чи є в мережі **DHCP**, і якщо так, то яка у нього IP-адреса. Якщо **DHCP-**сервер у локальній мережі є, він відповідає йому пакетом **DHCPOFFER**, у якому повідомляє про свою присутність і пропонує IP-адресу. Комп'ютер, отримавши пакет **DHCPOFFER**, відсилає йому відповідь у вигляді пакету **DHCPREQUEST**, у якому погоджується взяти цю адресу, на що **DHCP**, отримавши цей пакет, відповідає пакетом **DHCPACK**, в якому повідомляється, що цю адресу закріплено за певним комп'ютером.

Розглянемо цю схему більш детально.

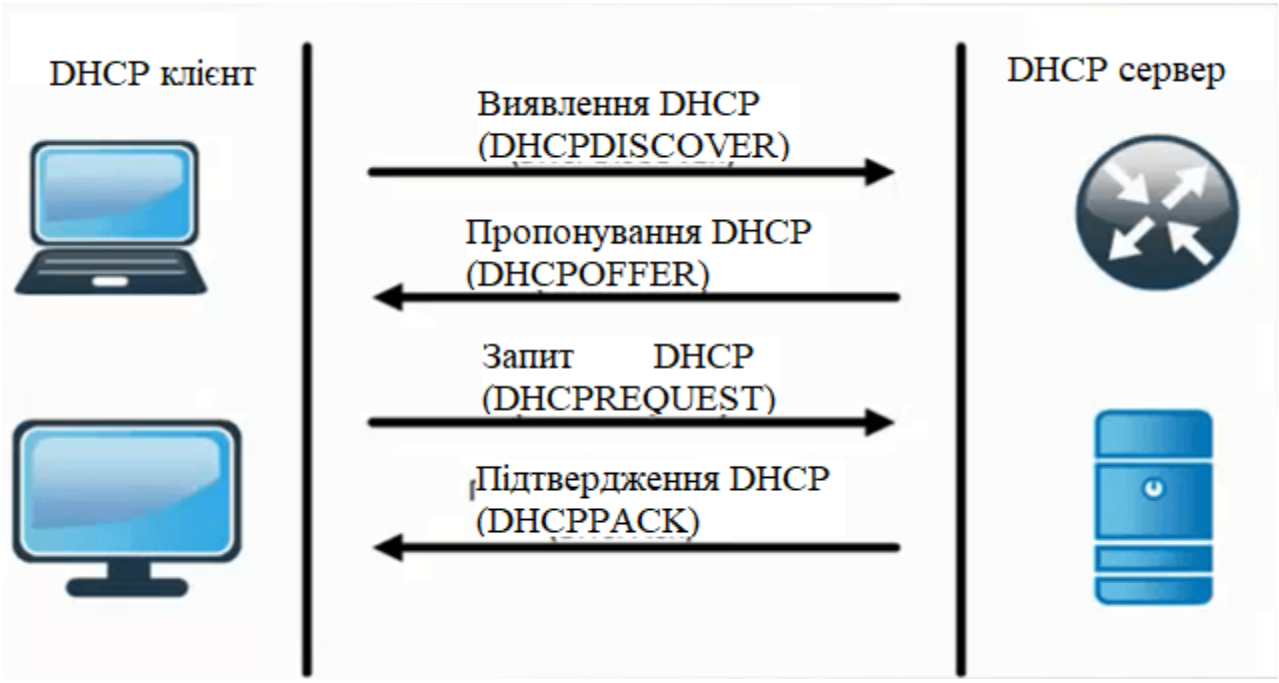

Рис. 5.2. Процес отримання IP-адреси за допомогою DHCP

***Discovery**, або пошук*

Спочатку клієнт перебуває в стані ініціалізації (INIT) і не має власної IP-адреси. Тому він відправляє широкомовне повідомлення **DHCPDISCOVER** на всі пристрої в локальній мережі. У тій же локальній мережі є DHCP-сервер. DHCP-сервер – це, наприклад, маршрутизатор або комутатор, є також виділені DHCP-сервери.

Не завжди одну мережу обслуговує один DHCP-сервер, часто організації встановлюють відразу кілька. Які порти використовує DHCP? Сервер завжди слухає **порт 67**, очікує широкомовне повідомлення від клієнта, а після його отримання відправляє пропозицію у відповідь – **DHCPOFFER**. Клієнт приймає повідомлення на **порту 68**.

***Offer**, або пропозиція*

DHCP-сервер відповідає на пошук пропозицією, повідомляє IP, який може підійти клієнту. IP виділяються з області (**SCOPE**) доступних адрес, що задається адміністратором.

Якщо є адреси, які не повинні бути призначені DHCP-сервером, область можна обмежити лише дозволеними адресами. Наприклад, адміністратор може встановити діапазон використовуваних IP-адрес від 192.0.0.10 до 192.0.0.255.

Буває й так, що не всі доступні адреси мають бути призначені для клієнтів. Наприклад, адміністратор може виключити (**exclude**) діапазон 192.0.0.100–192.0.0.200 з області, що використовується. Таке обмеження називається винятком.

DHCP виділяє доступні IP-адреси з області лише тимчасово (про це пізніше), тому немає гарантії, що при наступному підключенні у клієнта залишиться той самий IP. Але є можливість призначити клієнту певний IP назавжди. Наприклад, забронювати 192.0.0.10 за комп'ютером системного адміністратора. Таке збереження IP окремих клієнтів називають резервацією (reservation).

DHCPOFFER містить IP з доступної області, який пропонується клієнту відправкою широкомовного (**broadcast**, «якщо ви той, хто запитував IP-адресу, то доступна ось така») або прямого (**unicast**, «ви запитували IP, пропоную ось такий») повідомлення. При цьому, оскільки клієнт поки не має IP, для надсилання прямого повідомлення він ідентифікується **MAC-адресою**.

***Request**, або запит*

Клієнт отримує **DHCPOFFER**, а потім надсилає на сервер повідомлення **DHCPREQUEST**. Цим повідомленням він приймає запропоновану адресу та повідомляє DHCP-сервер про це. Широкомовне

повідомлення майже повністю дублює **DHCPDISCOVER**, але містить унікальний IP, виділений сервером. Таким чином клієнт повідомляє всім доступним DHCP-серверам: «Так, я беру цю адресу», а сервери позначають IP як зайнятий.

DHCPACK*, або підтвердження*

Сервер отримує від клієнта **DHCPREQUEST** та остаточно підтверджує передачу IP-адреси клієнту повідомленням **DHCPACK**. Це широкомовне чи пряме повідомлення затверджує як власника IP, так і термін, протягом якого клієнт може використовувати цю адресу.

А якщо в мережі кілька DHCP-серверів, які надіслали пропозицію, яку з них вибере клієнт? У стані **INIT**, якщо клієнт отримує адресу вперше, він прийматиме лише першу пропозицію IP. Однак якщо клієнт вже спілкувався раніше з певним DHCP-сервером, він віддасть перевагу цьому серверу і, навпаки, сервер вибере знайомого клієнта.

Термін оренди

Коли DHCP-сервер виділяє IP з області, він залишає запис про те, що ця адреса зарезервована за клієнтом із зазначенням терміну дії IP. Цей термін дії називається терміном оренди (**lease time**). Термін оренди може становити від 24 годин до декількох днів, тижнів або навіть місяців, він задається в настройках сервера.

Надання адреси в оренду, а не на постійній основі необхідно з кількох причин. По-перше, це розумне використання IP-адрес – клієнти, які відключені або вийшли з ладу, не резервують за собою адресу. По-друге, це гарантія того, що нові клієнти за необхідності зможуть отримати унікальну адресу.

Після отримання адреси з області клієнт бере її в оренду на час, що позначається T. Клієнт переходить у пов’язаний (**BOUND**) стан і продовжує нормальну роботу, поки не настане час половини терміну оренди – T1.

Після настання часу T1 клієнт ініціює процедуру отримання нового IP або оновлення адреси – стан **RENEWING**. Процес повторного отримання відбувається за спрощеною схемою: клієнт прямим повідомленням запитує (**DHCPREQUEST**), а сервер підтверджує запит (**DHCPACK**). Час оренди починає відраховуватись наново.

Якщо підтвердження (**DHCPACK**) від сервера не надходить, клієнт знову запитує адресу, але коли закінчується половина T1. Якщо запит адреси залишається без відповіді вдруге, клієнт надсилає ще одне повідомлення, коли спливає половина від T1/2 (25 % від повного терміну оренди). Наступний запит буде надіслано після закінчення ще половини часу, що залишився, потім ще половини. І так далі, поки не настане T2, що дорівнює 87,5 %, або 7/8 від усього часу оренди. Після T2 усі спроби

продовжити оренду IP будуть широкомовними. Це означає, що якщо перший сервер з якоїсь причини недоступний, на запит адреси зможе відповісти будь-який інший і роботу не буде перервано. Перелічимо ще раз пакети, що використовуються протоколом DHCP.

Особливі DHCP-повідомлення

Крім чотирьох повідомлень для отримання адреси (DORA), DHCP використовує й інші. Давайте розглянемо кожне.

DHCPNAK. Нерідко у джерелах можна зустріти написання **DHCPNACK**, що є неправильним, оскільки RFC 2131 регламентує саме NAK. **DHCPNAK** надсилається сервером замість остаточного підтвердження. Така відмова може бути відправлена клієнту, якщо оренда запитаного IP закінчилася або клієнт перейшов у нову підмережу.

DHCPRELEASE. Клієнт надсилає це повідомлення, щоб повідомити сервер про звільнення займаного IP. Інакше кажучи, це дострокове закінчення оренди.

DHCPINFORM. Цим повідомленням клієнт запитує у сервера локальні настройки. Відправляється, коли клієнт вже отримав IP, але для правильної роботи потрібна конфігурація мережі. Сервер інформує клієнта повідомленням у відповідь із зазначенням усіх запитаних опцій.

DHCPDECLINE – це пакет, у якому клієнт визначив, що IP-адреса від DHCP-сервера в момент пропозиції вже використовується кимось, і тоді буде згенеровано новий запит на іншу IP-адресу.

DHCPRENEW – це пакет, що містить запит на оновлення та продовження оренди IP-адреси.

Опції DHCP

Для роботи в мережі клієнту потрібен не тільки IP, але й інші параметри DHCP – наприклад, маска підмережі, стандартний шлюз і адреса сервера. Опції є пронумерованими пунктами, рядками даних, які містять необхідні клієнту сервера параметри конфігурації. Дамо опис деяких опцій:

Option 1 – маска підмережі IP;
Option 3 – основний шлюз;
Option 6 – адреса сервера DNS (основна та резервна);
Option 51 – визначає, на який термін IP-адреса надається в оренду клієнту;
Option 55 – список опцій, що запитуються. Клієнт завжди запитує опції для правильної конфігурації. Відправляючи повідомлення з Option 55, клієнт виставляє список числових кодів опцій, що запитуються, в порядку

переваги. DHCP-сервер намагається надіслати відповідь з опціями в тому самому порядку;

Option 82 – інформація про агента ретрансляції (relay agent information).

Розглянемо більш детально останню опцію (**Option 82**). Завдяки ретранслятору клієнт та сервер можуть спілкуватися, перебуваючи у різних підмережах. За замовчуванням широкомовні повідомлення клієнта не можуть виходити за межі поточного домену (підмережі). Але за межі підмережі виходять лише широкомовні DHCP-повідомлення. Це стає можливим завдяки агенту ретрансляції, у ролі якого зазвичай виступає маршрутизатор чи сервер. Ретранслятор отримує повідомлення від клієнта у своїй підмережі, направляє його на DHCP-сервер, який так само через ретранслятор відправляє відповідь. Отже, ретранслятор діє як посередник між підмережами (рис. 5.3).

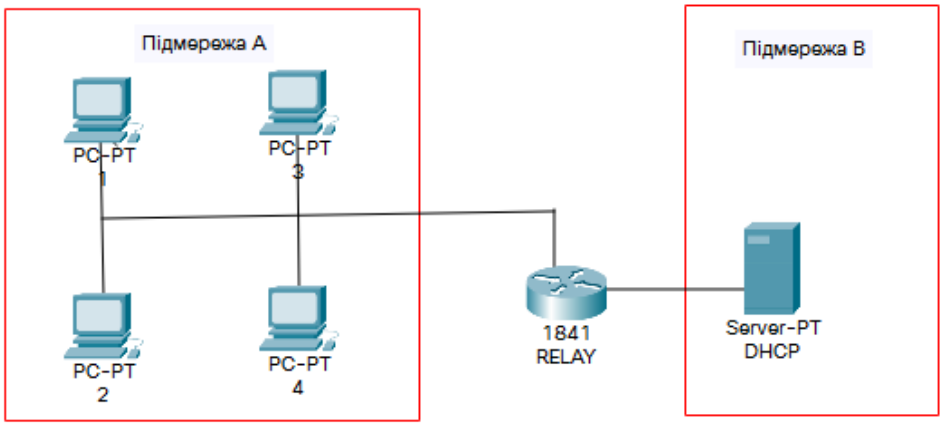

Рис. 5.3. Агент ретрансляції

Настроювання сервера DHCP на маршрутизаторі

Спочатку розглянемо варіант настроювання сервера DHCP безпосередньо на маршрутизаторі. Для цього скористаємося схемою мережі, розглянутою у темі внутрішньої маршрутизації в лабораторній роботі № 4 (рис. 5.4).

У переліку наступних команд визначимо мережні параметри для наявних підмереж, таких як адреса мережі і адреса шлюзу для кожної підмережі. Також зарезервуємо IP-адресу, яку отримав шлюз, щоб не надавати її іншим пристроям. Це необхідно для запобігання ситуації, коли два пристрої у мережі отримають однакові IP-адреси, що призведе до конфліктної ситуації і зробить мережу непрацездатною.

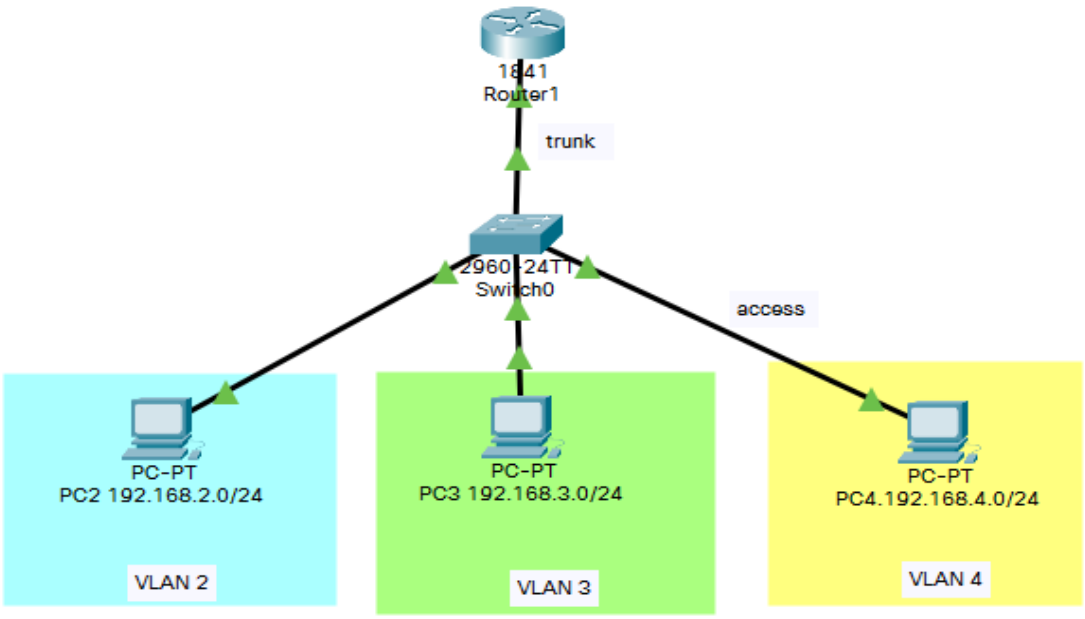

Рис. 5.4. Схема мережі

Настроїмо службу DHCP на роутері для кожної підмережі:

Router(config)*#ip dhcp pool VLAN3*
Router(dhcp-config)*#network 192.168.3.0 255.255.255.0*
Router(dhcp-config)*#default-router 192.168.3.1*
Router(dhcp-config)*#exit*
Router(config)*#ip dhcp pool VLAN4*
Router(dhcp-config)*#network 192.168.4.0 255.255.255.0*
Router(dhcp-config)*#default-router 192.168.4.1*
Router(dhcp-config)*#exit*
Router(config)*#ip dhcp pool VLAN2*
Router(dhcp-config)*#network 192.168.2.0 255.255.255.0*
Router(dhcp-config)*#default-router 192.168.2.1*
Router(dhcp-config)*#exit*
Router(config)*#do wr*

Зарезервуємо на DHCP IP-адреси шлюзу:

Router(config)*#ip dhcp excluded-address 192.168.2.1*
Router(config)*#ip dhcp excluded-address 192.168.3.1*
Router(config)*#ip dhcp excluded-address 192.168.4.1*
Router(config)*#do wr*
Building configuration...
[OK]
Router(config)#exit

Router#

Настроїмо мережні адаптери комп'ютерів для отримання мережних настройок за допомогою DHCP (рис. 5.5).

Рис. 5.5. Приклад настроювання мережного адаптера ПК

Перевіримо адреси, отримані від DHCP-сервера на кожному комп'ютері за допомогою команди ipconfig (рис. 5.6).

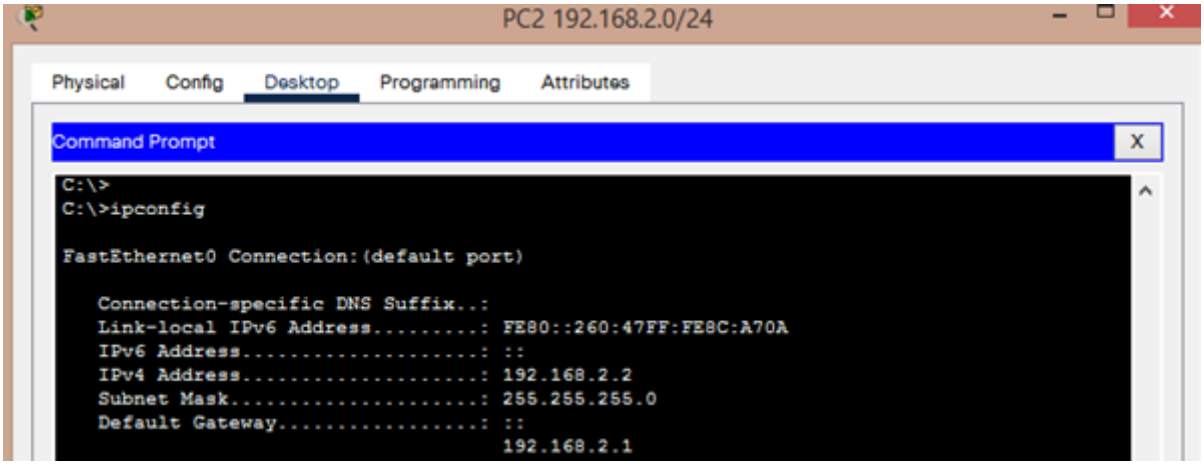

Рис. 5.6. Перевірка отриманих мережних настройок

Перевіримо доступність комп'ютерів з різних підмереж за допомогою команди **ping** (рис. 5.7).

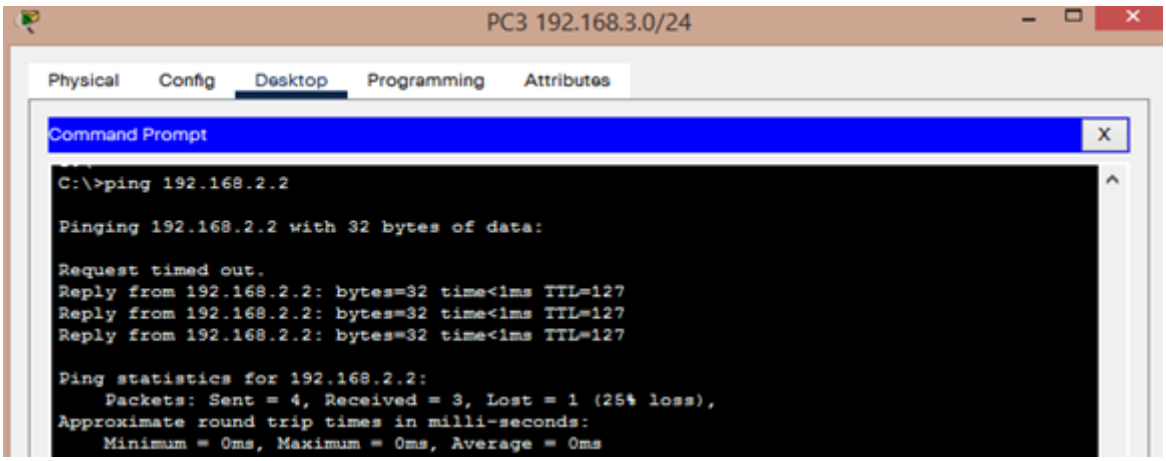

Рис. 5.7. Команда ping

Корисні команди настроювання Cisco DHCP

Для відображення IP-адрес, виданих хостам (рис. 5.8), використовуйте таку команду:

***Router**#show ip dhcp binding*

```
Router#
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration
Type
                 Hardware address
192.168.2.2      0060.478C.A70A           --
Automatic
192.168.3.2      00E0.B087.97D5           --
Automatic
192.168.4.2      00D0.D35E.E2D8           --
Automatic
Router#
```

Рис. 5.8. Відображення IP-адрес, виданих хостам

Відображення конфліктів IP у мережі:

***Router**#show ip dhcp conflict*

Відображення подій DHCP у міру їх виникнення:

***Router**#debug ip dhcp server events*

Відключення настроювання:

***Router**#undebug ip dhcp server events*

Вимкнення та увімкнення служби DHCP

Для ввімкнення та вимкнення служби DHCP використовуємо такі команди:

***Router(config)**#no service dhcp*
***Router(config)**#service dhcp*

Настроювання служби DHCP на окремому сервері

Проведемо настроювання DHCP у мережі такої конфігурації, як описано у пункті «Настроювання сервера DHCP на маршрутизаторі» цієї лабораторної роботи.

Для настроювання нової конфігурації підключимо сервер зі статичним IP 192.168.4.2/24 до комутатора інтерфейсу fa0/5. У настройках комутатора віднесемо цей access port до VLAN4 (рис. 5.9).

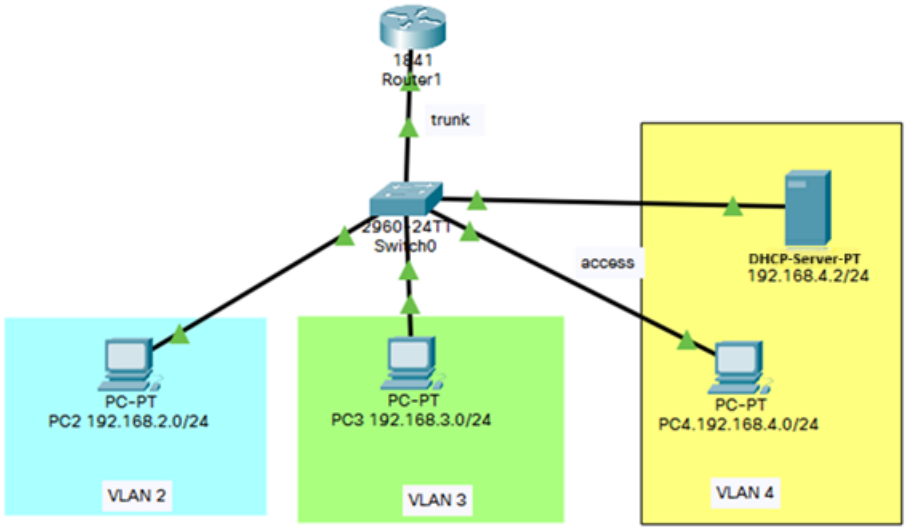

Рис. 5.9. Схема мережі

Відключаємо службу DHCP на маршрутизаторі такою командою:

***Router(config)**#no service dhcp*

У настройках сервера пропишемо мережі та діапазони адрес, що видаються пристроям (рис. 5.10).

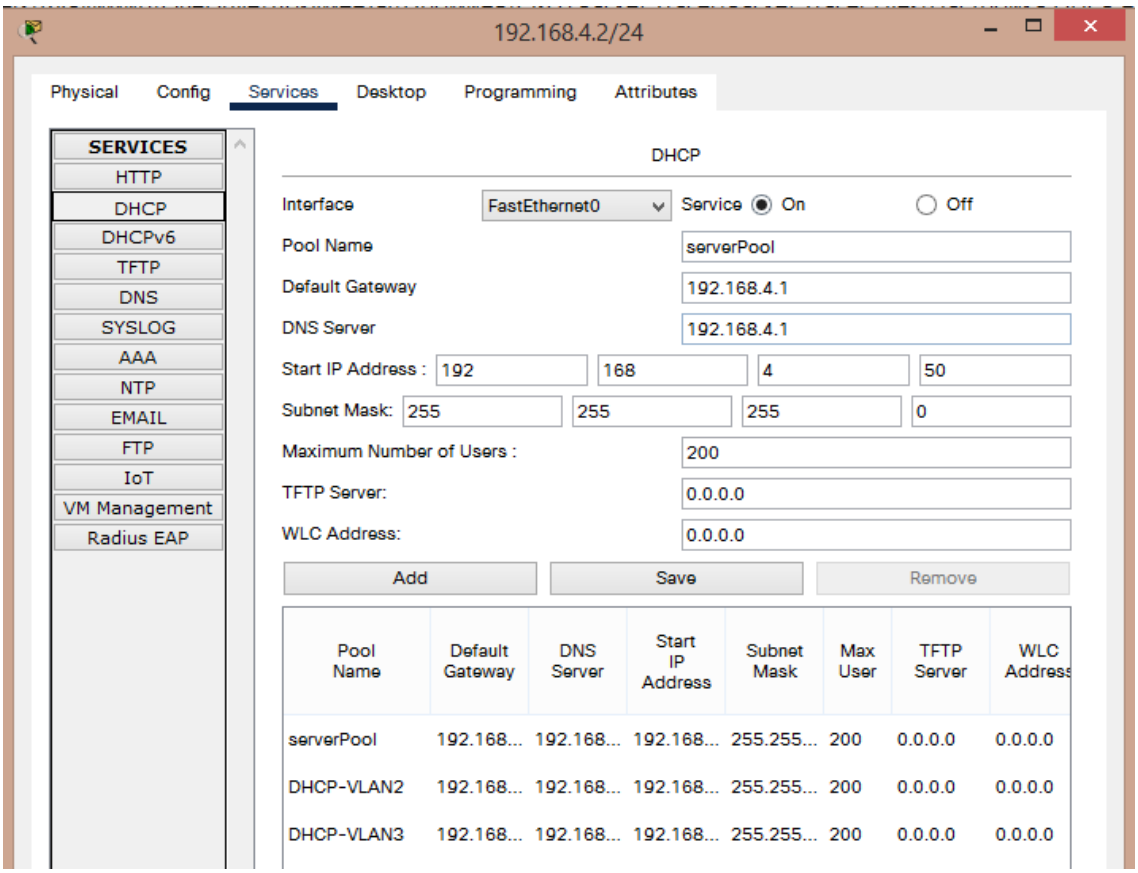

Рис. 5.10. Настроювання DHCP на сервері

У настройках мережних адаптерів комп'ютерів встановимо отримання мережних настройок за допомогою DHCP (див. рис. 5.5).

DHCP Relay настроювання роутера

DHCP Relay (Dynamic Host Configuration Protocol Relay) – це мережний пристрій або служба, яка дає змогу пересилати запити DHCP-клієнтів на DHCP-сервер, що знаходиться в іншій мережі. Зазвичай DHCP-сервер і клієнти знаходяться в різних підмережах, і безпосередній зв'язок між ними може бути неможливим через різні сегменти мережі. DHCP Relay розв'язує цю проблему.

Іншими словами, це ретранслятор, який відловлює пакети **DHCPDISCOVER** і перенаправляє їх DHCP-серверу, за рахунок цього можна зменшити кількість DHCP-серверів.

Настроїмо цей ретранслятор на роутері.

Router(config)*#int fa0/0.2*
Router(config-if)*#ip helper-address 192.168.4.2*
Router(config-if)*#exit*
Router(config)*#int fa0/0.3*

***Router(config-if)**#ip helper-address 192.168.4.2*
***Router(config-if)**#exit*
***Router(config)**#do wr*

Перевіримо отримані комп'ютерами DHCP-настройки за допомогою команди ipconfig (рис. 5.11), як це робили раніше.

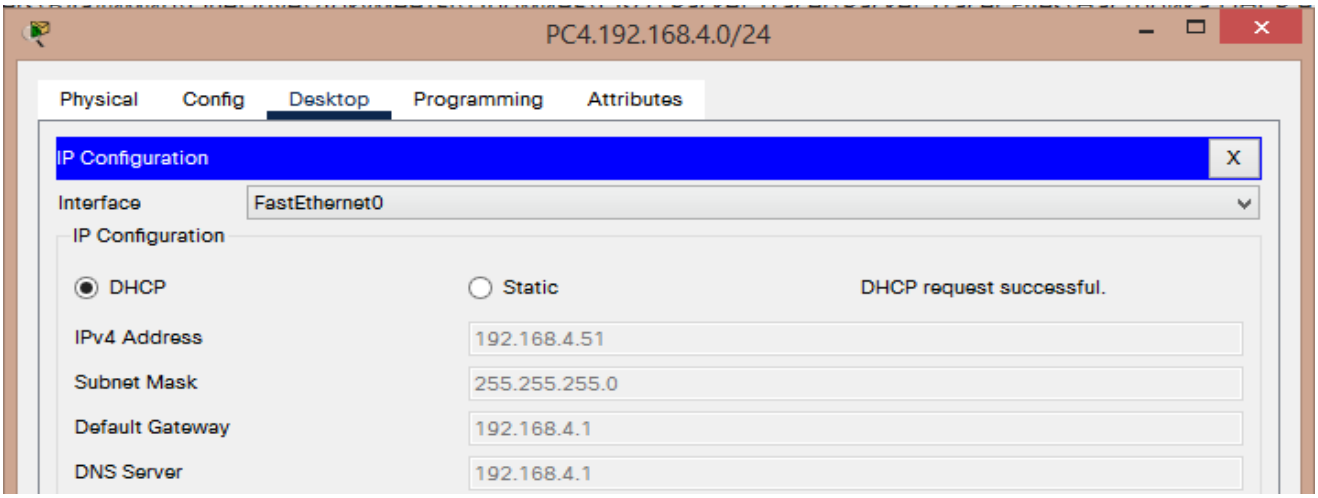

Рис. 5.11. Отримані комп'ютерами DHCP-настройки

Перевіримо працездатність мережі та доступність комп'ютерів за допомогою команди **ping** (рис. 5.12).

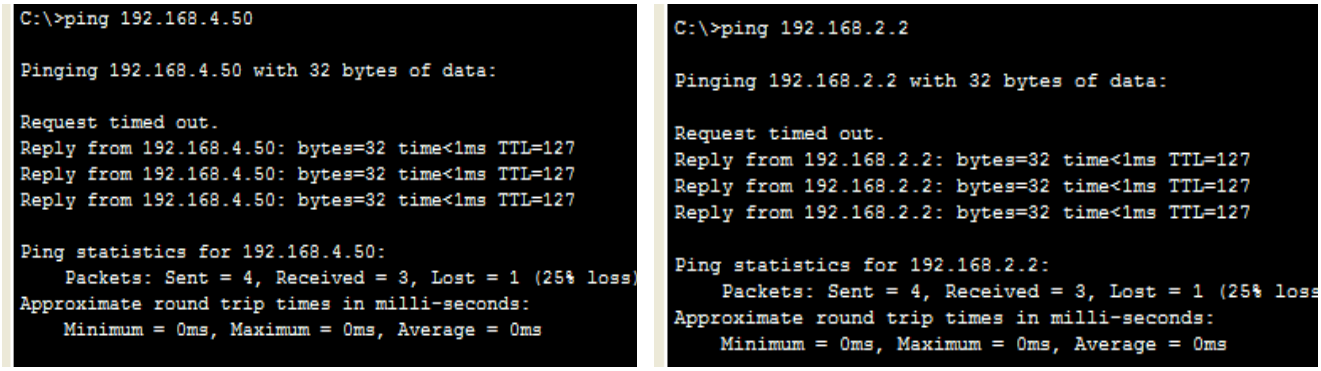

Рис. 5.12. Команда **ping**

Отже, перевірка дала позитивний результат, з чого можна зробити висновок, що встановлена служба DHCP працює коректно і мережа працездатна.

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.

2. Побудуйте наступну схему у Cisco Paket Tracer (див. рис. 5.3).
3. Проведіть настроювання пристроїв мережі згідно зі своїм варіантом (табл. 5.1–5.3) та порядком, описаним у лабораторній роботі № 4. Настроювання проводити, користуючись вкладкою CLI.
4. Настройте та ввімкніть службу DHCP на роутері.
5. Настройте мережні адаптери кінцевих пристроїв у режимі автоматичного отримання настройок.
6. Виведіть на екран настройки мережних адаптерів хостів.
7. Виведіть на екран отримані IP-адреси хостів засобами командного рядка роутера.
8. Перевірте доступність комп'ютерів у мережі за допомогою команди **ping**.
9. Побудуйте схему мережі з окремим DHCP-сервером (див. рис. 5.9), присвоївши DHCP-серверу адресу, що йде безпосередньо за адресою роутера (x.x.x.2).
10. Настройте DHCP-сервер згідно зі своїм варіантом (табл. 5.4). Кількість користувачів установіть такою, що дорівнює 20.
11. Вимкніть DHCP-службу на роутері.
12. Настройте на роутері ретранслятор **DHCP RELAY**.
13. Настройте мережні адаптери кінцевих пристроїв у режимі автоматичного отримання настройок.
14. Виведіть на екран отримані IP-адреси хостів засобами командного рядка роутера.
15. Перевірте доступність комп'ютерів у мережі за допомогою команди **ping**.

Вимоги до звіту

Звіт з лабораторної роботи має містити:
1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 5.1

IP-адреси підмереж

Номер варіанта	Адреси підмереж		
	PC2 перша підмережа	PC3 друга підмережа	PC4 третя підмережа
1, 11	192.168.2.0	192.168.12.0	192.168.22.0
2, 12	192.168.3.0	192.168.13.0	192.168.23.0
3, 13	192.168.4.0	192.168.14.0	192.168.24.0
4, 14	192.168.5.0	192.168.15.0	192.168.25.0
5, 15	192.168.6.0	192.168.16.0	192.168.26.0
6, 16	192.168.7.0	192.168.17.0	192.168.27.0
7, 17	192.168.8.0	192.168.18.0	192.168.28.0
8, 18	192.168.9.0	192.168.19.0	192.168.29.0
9, 19	192.168.10.0	192.168.20.0	192.168.30.0
10, 20	192.168.11.0	192.168.21.0	192.168.31.0

Таблиця 5.2

IP-адреси шлюзів

Номер варіанта	Адреси підмереж		
	PC2 перша підмережа	PC3 друга підмережа	PC4 третя підмережа
1, 11	192.168.2.1	192.168.12.1	192.168.22.1
2, 12	192.168.3.1	192.168.13.1	192.168.23.1
3, 13	192.168.4.1	192.168.14.1	192.168.24.1
4, 14	192.168.5.1	192.168.15.1	192.168.25.1
5, 15	192.168.6.1	192.168.16.1	192.168.26.1
6, 16	192.168.7.1	192.168.17.1	192.168.27.1
7, 17	192.168.8.1	192.168.18.1	192.168.28.1
8, 18	192.168.9.1	192.168.19.1	192.168.29.1
9, 19	192.168.10.1	192.168.20.1	192.168.30.1
10, 20	192.168.11.1	192.168.21.1	192.168.31.1

Таблиця 5.3

Номери VLAN

Номер варіанта	Перша підмережа	Друга підмережа	Третя підмережа
1, 11	vlan 2	vlan 3	vlan 4
2, 12	vlan 5	vlan 6	vlan 7

Закінчення табл. 5.3

Номер варіанта	Перша підмережа	Друга підмережа	Третя підмережа
3, 13	vlan 8	vlan 9	vlan 10
4, 14	vlan 11	vlan 12	vlan 13
5, 15	vlan 14	vlan 15	vlan 16
6, 16	vlan 17	vlan 18	vlan 19
7, 17	vlan 20	vlan 21	vlan 22
8, 18	vlan 23	vlan 24	vlan 25
9, 19	vlan 26	vlan 27	vlan 28
10, 20	vlan 29	vlan 30	vlan 31

Таблиця 5.4

Стартові IP-адреси пулів адрес

Номер варіанта	Стартові-IP адреси пулів адрес у підмережах		
	PC2 перша підмережа	PC3 друга підмережа	PC4 третя підмережа
1, 11	192.168.2.10	192.168.12.20	192.168.22.30
2, 12	192.168.3.11	192.168.13.21	192.168.23.31
3, 13	192.168.4.12	192.168.14.22	192.168.24.32
4, 14	192.168.5.13	192.168.15.23	192.168.25.33
5, 15	192.168.6.14	192.168.16.24	192.168.26.34
6, 16	192.168.7.15	192.168.17.25	192.168.27.35
7, 17	192.168.8.16	192.168.18.26	192.168.28.36
8, 18	192.168.9.17	192.168.19.27	192.168.29.37
9, 19	192.168.10.18	192.168.20.28	192.168.30.38
10, 20	192.168.11.19	192.168.21.29	192.168.31.39

Контрольні запитання

1. До якого рівня моделі OSI належить протокол DHCP?
2. За що відповідає поле OP у заголовку протоколу DHCP?
3. Що означає повідомлення **DHCPOFFER**?
4. Хто є відправником повідомлення **DHCPDISCOVER**?
5. Що означає термін оренди у протоколі DHCP?
6. Яку інформацію несуть опції у протоколі DHCP?
7. Які функції виконує агент ретрансляції у роботі протоколу DHCP?

Лабораторна робота № 6

НАСТРОЮВАННЯ NAT НА РОУТЕРІ В ЛОКАЛЬНІЙ МЕРЕЖІ

Мета роботи: вивчити процес настроювання NAT на роутері в локальній мережі та необхідні для цього команди на обладнанні Cisco.

Теоретичні відомості

NAT (Network Address Translation) – це технологія, що дає змогу змінювати IP-адреси в пакетах, які передаються через маршрутизатор або інший мережний пристрій. Це особливо корисно для підключення внутрішньої мережі з приватними IP-адресами до Інтернету, де використовуються публічні IP-адреси. Існує кілька видів NAT, які використовуються в різних сценаріях.

Види NAT

Статичний NAT – перетворення «сірого» IP на білий, приклад прокидання порту в локальну мережу, наприклад RDP.

Динамічний NAT – перетворення «сірого» IP на одну з IP-адрес групи білих IP-адрес.

Перевантажений NAT або, як його ще називають, PAT (port adress translation), перетворення кількох «сірих» IP на «білий» через надання їм різних портів.

Списки контролю доступу ACL (Access Control List)

Списки керування доступом є частиною комплексної системи безпеки мережі. З їх допомогою можна заборонити/дозволити певним хостам доступ до ресурсів мережі. Наприклад, у корпоративній мережі адміністратори можуть одним користувачам заборонити доступ до Інтернету, а іншим, навпаки, дозволити.

Заборонити/дозволити доступ можна на основі IP-адрес, портів та задіяних протоколів. За цим принципом працюють списки керування доступом ACL (Access Control List).

Іншим прикладом використання списків доступу є заборона пакетів протоколу **ICMP**, що надходять на маршрутизатор. Як відомо, за допомогою **ICMP** працюють утиліти **Ping**, **Traceroute/Tracert**. За допомогою цих утиліт можна просканувати мережу, а це небажано з погляду політики безпеки кожної мережі.

Списки доступу дають змогу фільтрувати трафік на вході та виході інтерфейсу маршрутизатора.

Коли ACL настроєні на вході інтерфейсу, то трафік фільтрується безпосередньо перед процесом маршрутизації (рис. 6.1).

Коли ACL настроєні на виході інтерфейсу, то трафік фільтрується відразу після процесу маршрутизації (рис. 6.2).

Списки доступу містять набір інструкцій, які порти та адреси блокувати, а які, навпаки, дозволити. Цих інструкцій може бути від декількох одиниць до десятків.

Після надходження трафіку перевірка списку доступу починається зверху вниз, тобто з першої інструкції. Як тільки буде знайдено збіг, перевірка припиниться і буде виконано дію, вказану в інструкції (заблокувати або пропустити).

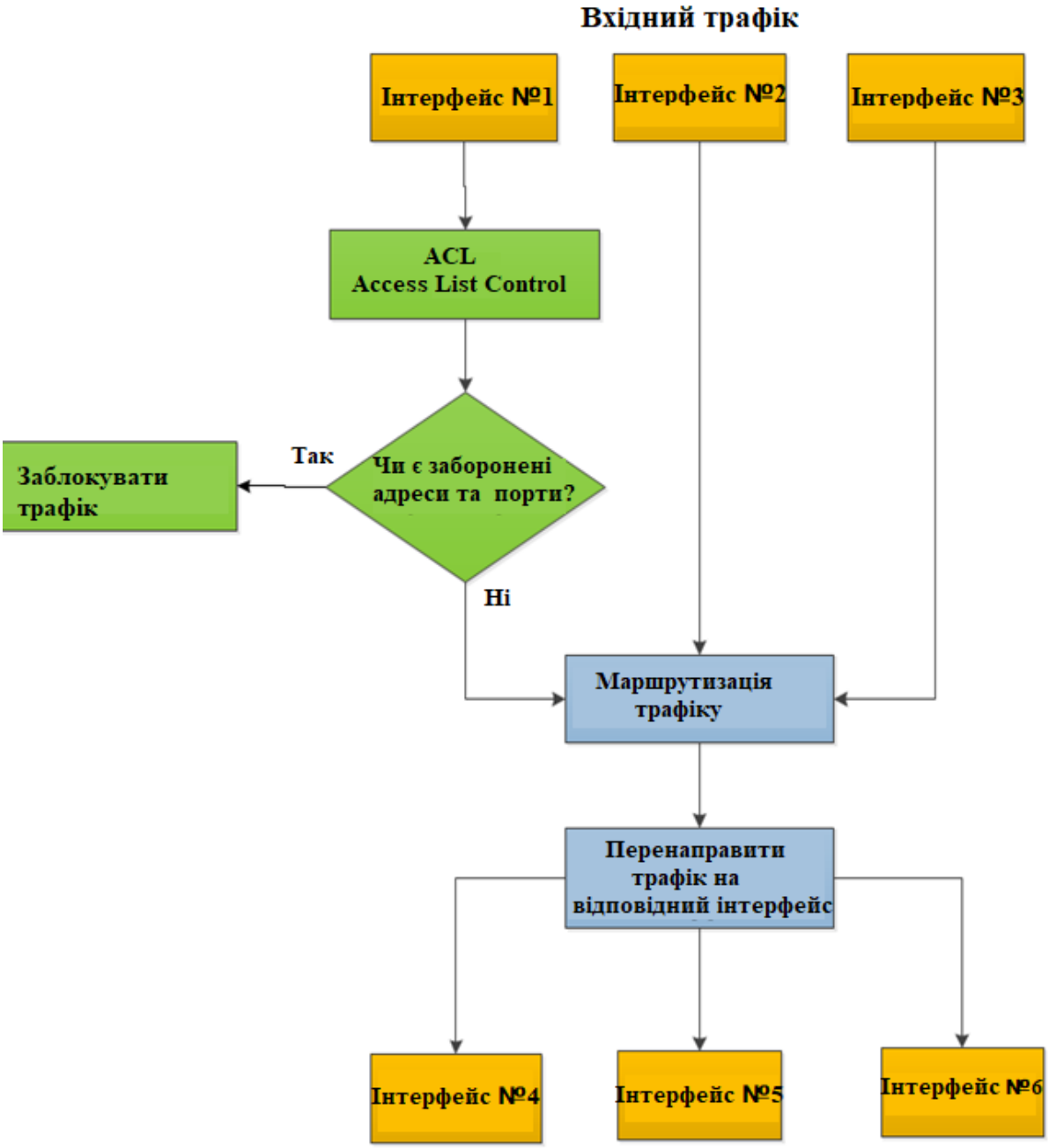

Рис. 6.1. Фільтрація трафіку на вході в роутер

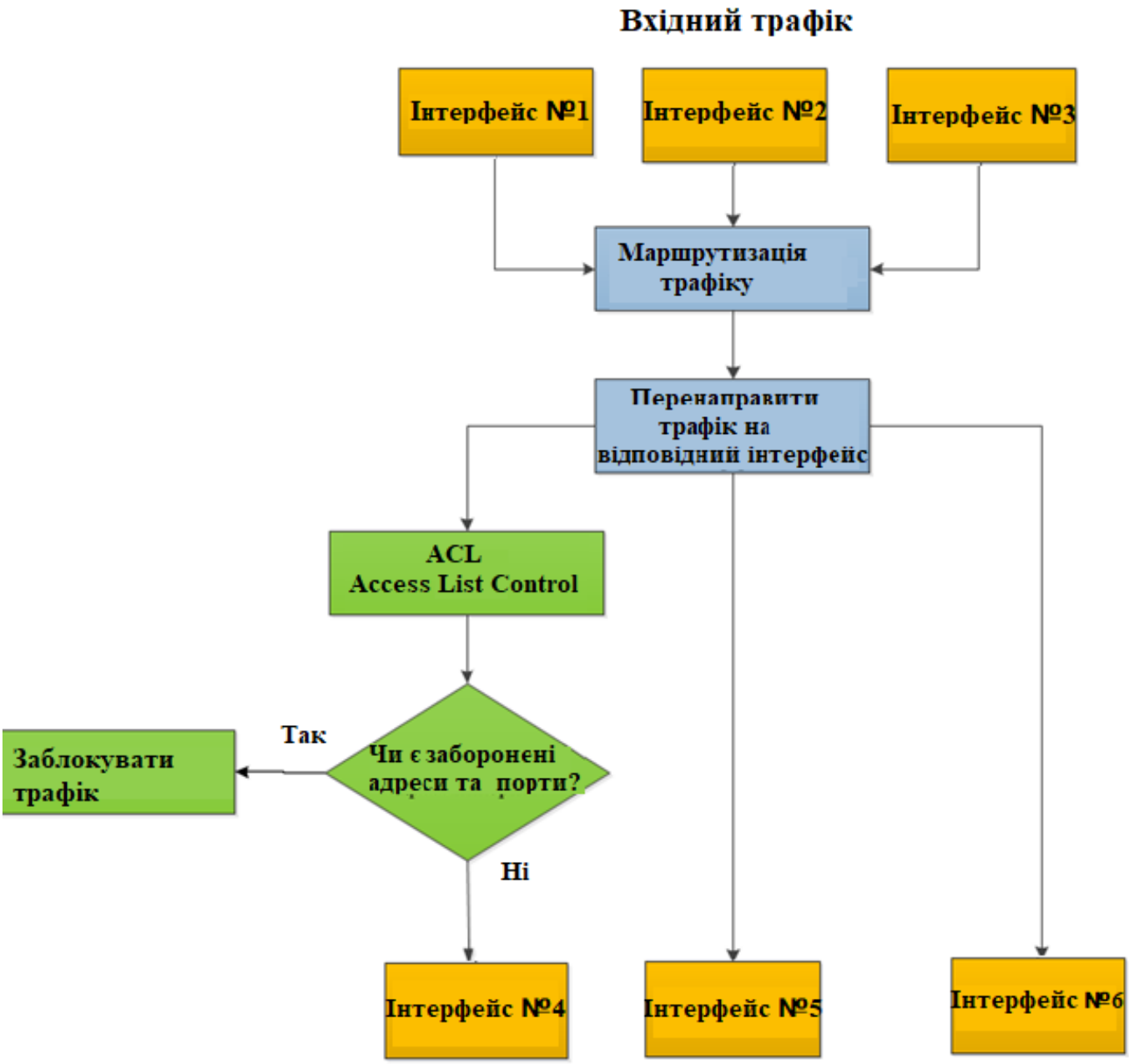

Рис. 6.2. Фільтрація трафіку на виході з роутера

Унизу списку завжди є неявна інструкція з блокування всього трафіку. Ця інструкція автоматично додається системою. У настройках її не видно, але потрібно знати, що вона є.

Види ACL

Cisco IOS підтримує три типи ACL:

- стандартні списки;
- розширені списки;
- іменовані списки.

За допомогою стандартних списків можна перевіряти лише IP-адресу відправника.

За допомогою розширених списків можна фільтрувати пакети на основі адрес, портів і протоколів одержувача та відправника.

Іменовані списки є тими ж стандартними та розширеними ACL, проте надають більш гнучкі можливості для редагування.

Настроювання ACL

Стандартний список

Інструкція задається такою командою:

Router(config)# access-list номер permit | deny IP_адреса_відправника інвертована_маска (wildcard mask)

Наприклад, так:

Router(config)# access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# access-list 1 deny any

Номер списку набуває значення від 1 до 99. Цифри означають не пріоритет або впорядкованість, а номер списку. Потім йде команда permit (дозволити) або deny (заборонити). За допомогою **інвертованої маски (wildcard mask)** можна визначити діапазон адрес, на які поширюватиметься заборона/дозвіл.

Першою командою забороняємо мережу 192.168.1.0/24, а другою – дозволяємо мережу 10.1.0.0/16.

Таких команд (інструкцій) можна додавати скільки завгодно. Як було зазначено раніше, робота завжди починається з найпершої команди і далі йде вниз за списком. Наприкінці списку завжди є неявна команда, що забороняє весь інший трафік, слід враховувати це при плануванні списків доступу. При додаванні нової команди до списку вона завжди додається до кінця списку.

Робота інвертованої маски ґрунтується на такому принципі.

На тих бітових позиціях інвертованої маски у двійковому вигляді, де встановлено 0, IP-адреса пристрою має збігатися з адресою, вказаною в настройках ACL.

На тих бітових позиціях інвертованої маски у двійковому вигляді, де встановлено 1, IP-адреса пристрою може не збігатися з адресою, вказаною в настройках ACL, тобто набувати будь-яких значень.

Розширений список доступу

Розширені списки доступу мають від 100 до 199 номерів.

Команди мають досить широкий набір опцій, тому наведемо найбільш загальний приклад команди:

Router(config)#access-list номер *permit* | *deny* протокол IP_адреса_відправника інвертована_маска порт_відправника IP_адреса_одержувача інвертована_маска порт_одержувача

Наприклад:

Router(config)#*access-list 100 permit tcp 192.168.1.0 0.0.0.255 eq 80 10.1.1.0 0.0.0.255 eq 443*

Ця команда дозволяє TCP-трафік від хостів з діапазоном 192.168.1.0/24 на хости з діапазоном 10.1.1.0/24. Причому порти відправника мають дорівнювати 80, а порти одержувача – 443. Якщо всі ці умови виконуються, то пакет пропускається, якщо ні, то переходить до наступної команди.

Router(config)#*access-list 100 deny tcp any host 172.16.1.5 gt 5000*

А ця команда забороняє весь TCP-трафік від будь-якого хоста на конкретний хост з адресою 172.16.1.5. Причому заборона діє за умови, що запити йдуть на порти отримувача від 5001 та вище.

Для перегляду настройок використовуються такі команди:

Router# *show running-config*
Router# *show ip access-lists*
Router# *show ip access-lists interface (назва_інтерфейсу)*

Іменовані списки

Іменовані списки нічим не відрізняються від стандартних та розширених списків, проте дають змогу гнучко редагувати новостворені списки.

Стандартні та розширені списки не можна редагувати. Наприклад, не можна всередину списку вставити команду або видалити її. Для цього потрібно спочатку деактивувати список на самому інтерфейсі, а потім його повністю видалити і настроїти заново.

За допомогою іменованого списку можна використовувати назви списків замість їх номерів. Усі введені команди нумеруються, що дає змогу легко додавати та видаляти команди.

Синтаксис команд

Стандартний список доступу

Router(config)#*access-list* <номер списку від 1 до 99> {permit | deny | remark} {address | any | host} [source-wildcard] [log]

- permit: дозволити
- deny: заборонити
- remark: коментар про список доступу
- address: забороняємо або дозволяємо мережу
- any: дозволяємо або забороняємо все
- host: дозволяємо або забороняємо хосту
- source-wildcard: WildCard маска мережі
- log: включаємо логування пакетів, що проходять через цей запис ACL

Розширений список доступу

Router(config)#access-list <номер списку від 100 до 199> {permit | deny | remark} protocol source [source-wildcard] [operator operand] [port <порт або назва протоколу> [established]

- protocol source: який протокол будемо дозволяти або закривати (ICMP, TCP, UDP, IP, OSPF тощо)
- deny – заборонити; permit – дозволити
- operator:
  A.B.C.D – адреса одержувача
  any – будь-який кінцевий хост
  eq – тільки пакети на цьому порту
  gt – лише пакети з великим номером порту
  host – єдиний кінцевий хост
  lt – лише пакети з нижчим номером порту
  neq – лише пакети не на цьому номері порту
  range – діапазон портів
- port: номер порту (TCP або UDP), можна вказати ім’я
- established: дозволяємо проходження TCP-сегментів, які є частиною вже створеної TCP-сесії

Алгоритм настроювання мережі

Цей алгоритм дає змогу настроїти NAT на роутері в локальній мережі і зв’язати локальну мережу з глобальною мережею завдяки настройкам роутера провайдера.

Настроювання роутерів

Розглянемо наведену у лабораторній роботі № 5 схему мережі малого офісу з настроєною внутрішньою маршрутизацією за допомогою субінтерфейсів та службою DHCP, розташованою на окремому сервері (рис. 6.3).

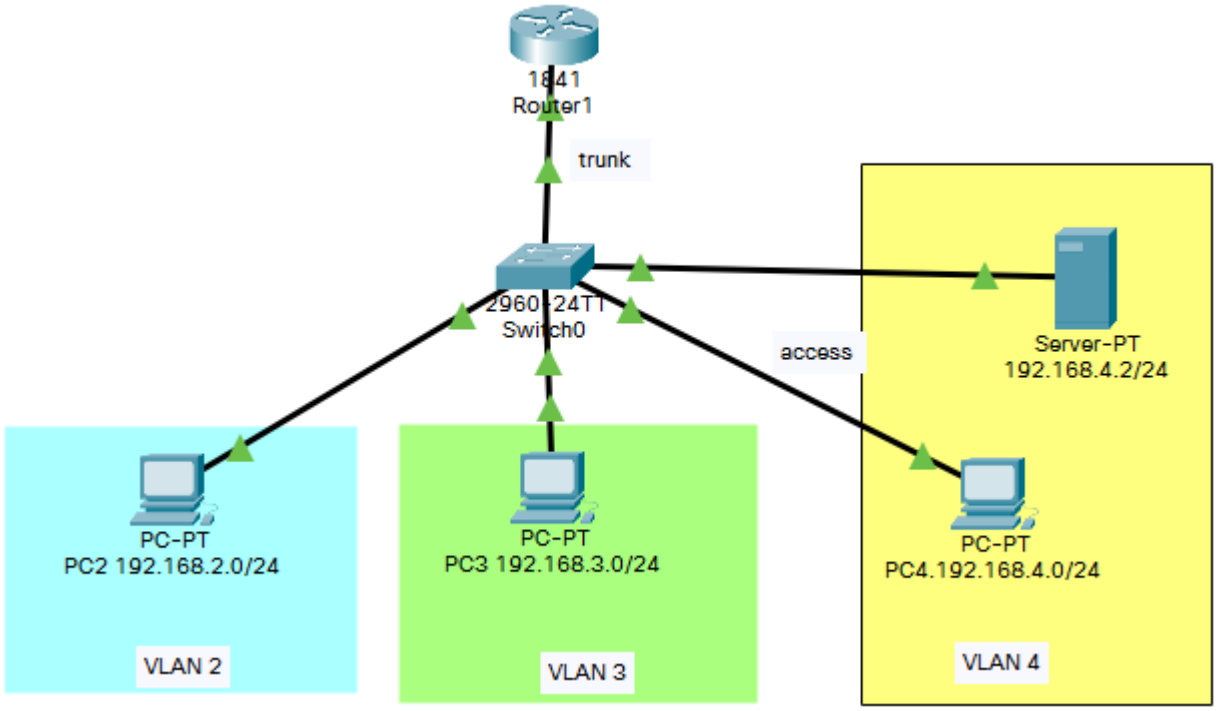

Рис. 6.3. Схема мережі

Розглянемо варіант під'єднання локальної мережі до **ISP** (Internet Service Provider) за схемою, показаною на рис. 6.4.

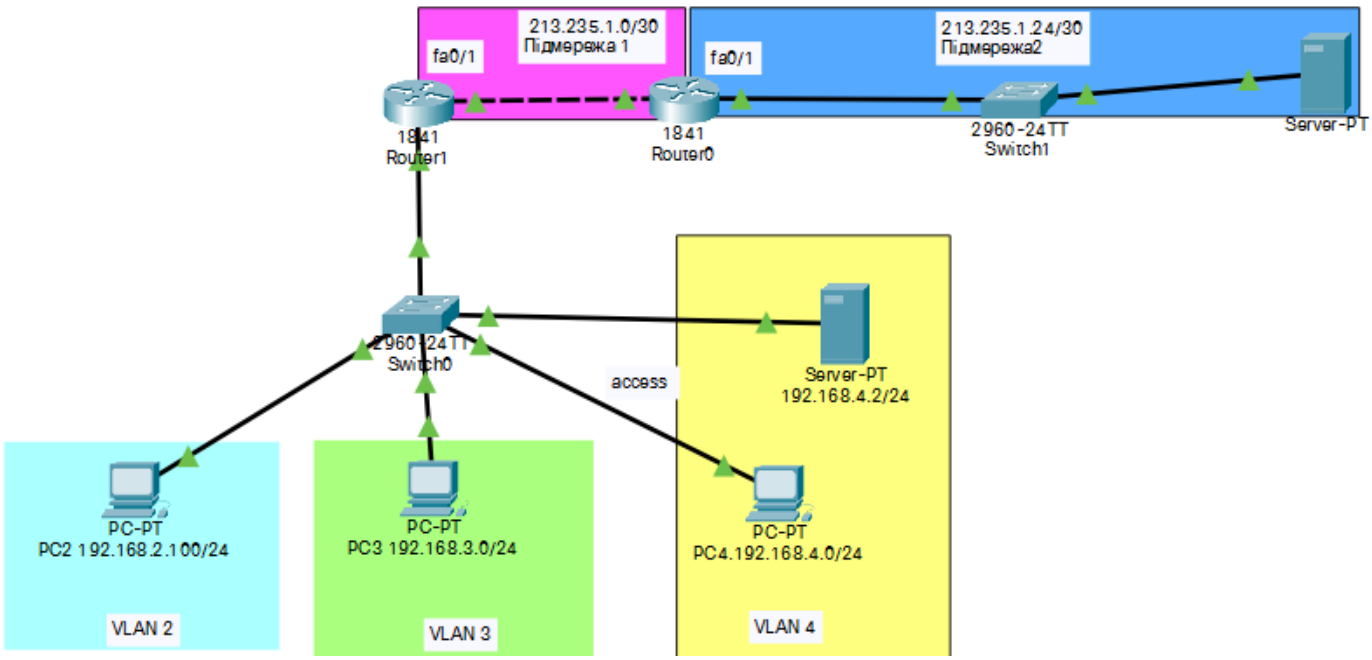

Рис. 6.4. Схема під'єднання до ISP

На роутері провайдера (Router 0) лівому порту (рис. 6.5) присвоєно «білу» IP-адресу 213.235.1.1/30.

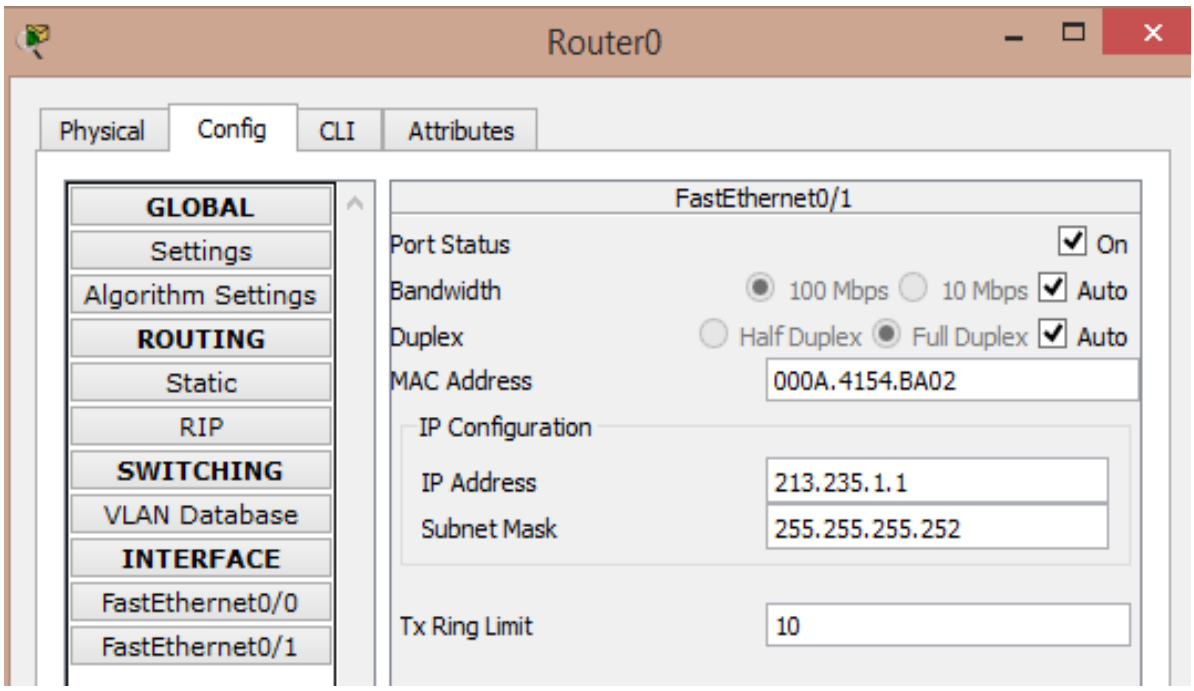

Рис. 6.5. Настроювання роутера провайдера (лівий інтерфейс з боку клієнта)

Зробимо настроювання інтерфейсів на сервері зовнішньої мережі, роутері провайдера та офісному роутері, користуючись вкладкою **Config** (рис. 6.6–6.8).

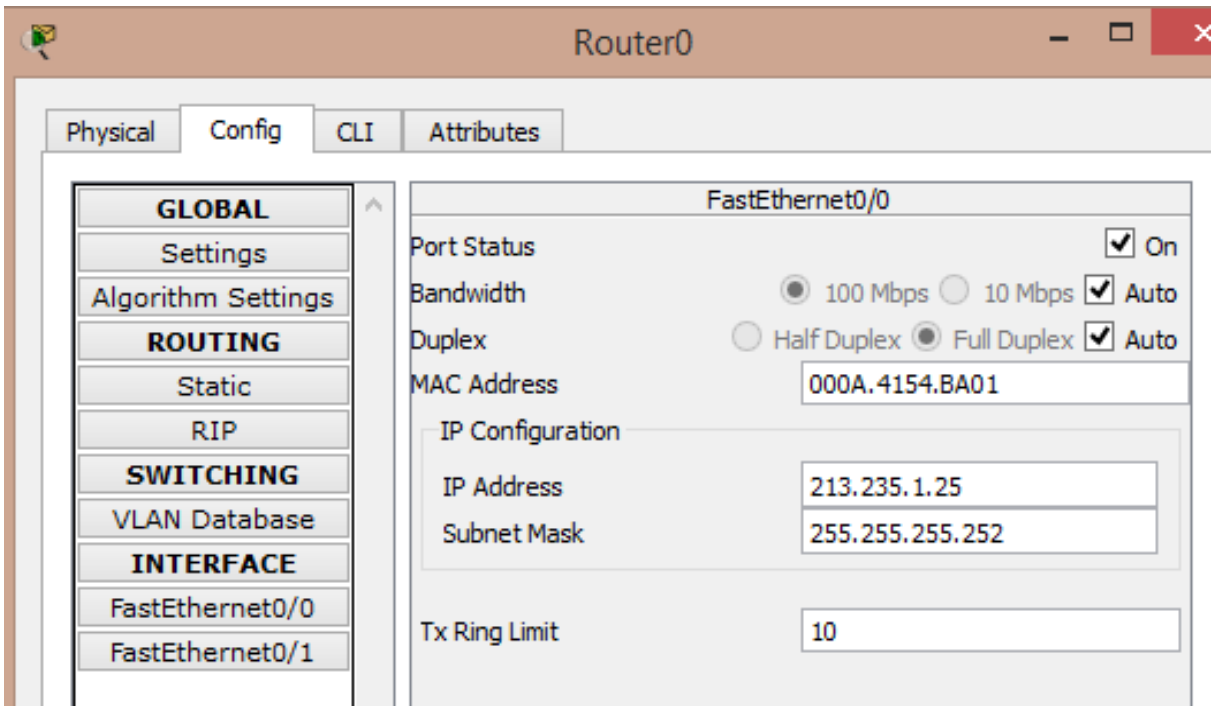

Рис. 6.6. Настроювання роутера провайдера з боку зовнішньої мережі

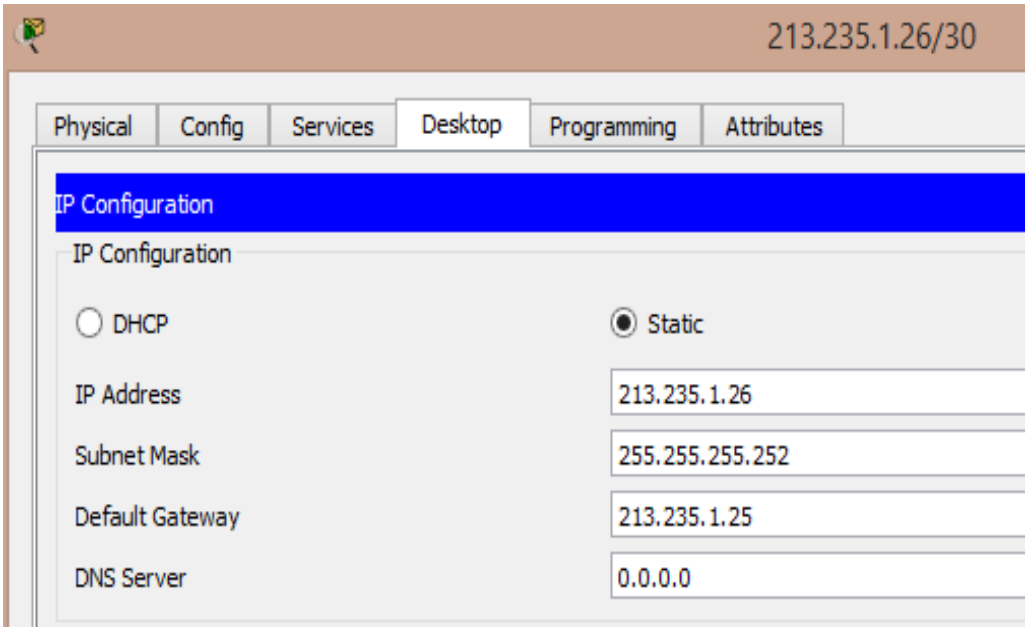

Рис. 6.7. Настроювання сервера зовнішньої мережі

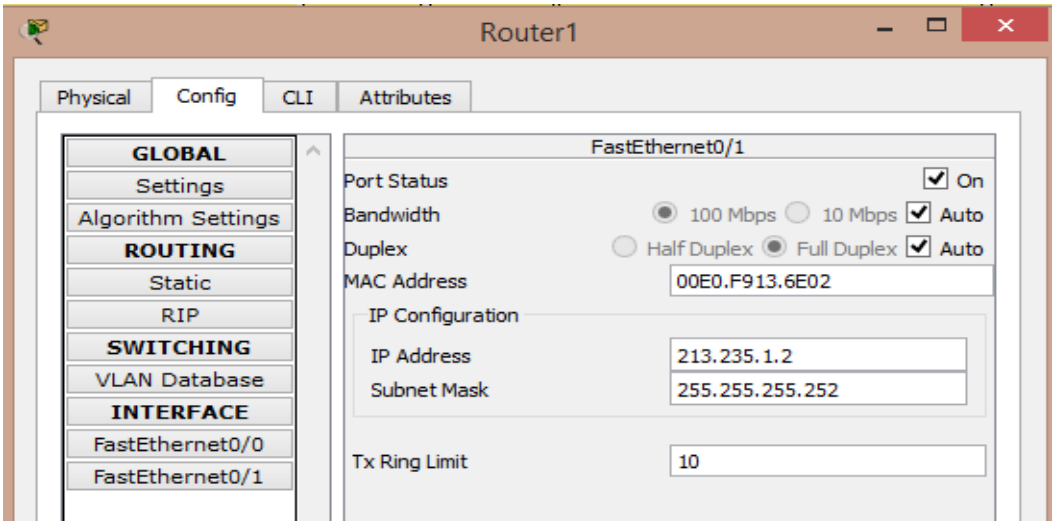

Рис. 6.8. Настроювання зовнішнього інтерфейсу роутера локальної мережі

Також ці настроювання можна виконати за допомогою стандартних команд Cisco IoS, наприклад, для Router1:

Router1>*enable*
Router1*#conf t*
Router1(config)*#int fa0/0*
Router1(config-if)*#ip address 213.235.1.2 255.255.255.252*
Router1(config-if)*#no shutdown*
Router1(config-if)*#exit*

Настроювання NAT

На роутері в локальній мережі потрібно задати, який інтерфейс **NAT**

будемо вважати зовнішнім, а який внутрішнім.

Зовнішнім буде той, де настроєна «біла» IP-адреса провайдера, внутрішнім – той, на якому настроєні Sub-інтерфейси для внутрішньої маршрутизації. На Router1 (див. рис. 6.4) внутрішнім інтерфейсом є **fastethernet0/0** (**fa0/0**), а зовнішнім – **fastethernet0/1** (**fa0/1**) відповідно.

Порядок настроювання інтерфейсів має такий вигляд:

Router1>*enable*
Router1*#conf t*
Router(config)*#int fa0/1*
Router1(config-if)*#ip nat outside*
Router1(config-if)*#exit*
Router(config)*#int fa0/0.2*
Router1(config-if)*#ip nat inside*
Router1(config-if)*#exit*
Router(config)*#int fa0/0.3*
Router1(config-if)*#ip nat inside*
Router1(config-if)*#exit*
Router(config)*#int fa0/0.4*
Router1(config-if)*#ip nat inside*
Router1(config-if)*#exit*

Далі настроїмо маршрутизацію за так званим нульовим маршрутом на адресу роутера провайдера (**Router0**):

Router(config)*#ip route 0.0.0.0 0.0.0.0 213.235.1.1*
Router(config)*#exit*
Router1*#wr*

Настроювання ACL

Створюємо іменований список доступу на ім'я MY_NAT і дозволяємо три пули IP-адрес:

Router*#*
Router(config)*#ip access-list standard MY_NAT*
Router(config-std-nacl)*#permit 192.168.2.0 0.0.0.255*
Router(config-std-nacl)*# permit 192.168.3.0 0.0.0.255*
Router(config-std-nacl)*# permit 192.168.4.0 0.0.0.255*
Router(config-std-nacl)*#end*

Далі вводимо ще одну команду, за допомогою якої трафік, що надійшов на fa0/1, можна маршрутизувати за правилом **перевантаженого NAT**.

Router(config)*#ip nat inside source list MY_NAT interface fa0/1 overload*

***Router(config)**# do wr*

Перевірка працездатності мережі

Пропінгуємо зовнішній сервер з одного з комп'ютерів локальної мережі (рис. 6.9).

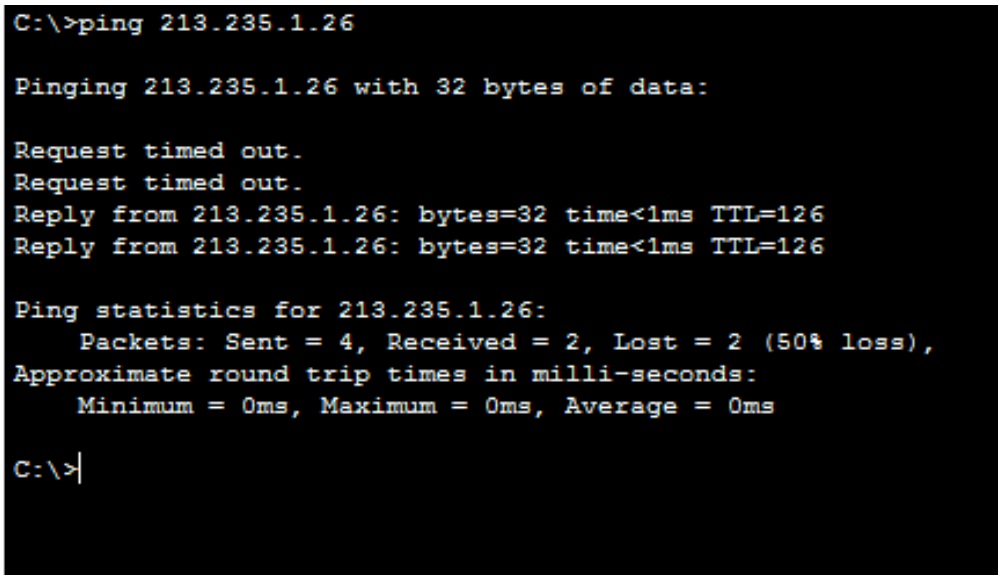

Рис. 6.9. Команда ping

Переглянемо трансляцію IP-адрес (рис. 6.10) за допомогою такої команди:

***Router**#show ip nat translation*

```
Router#sh ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 213.235.1.2:1     192.168.2.2:1      213.235.1.26:1     213.235.1.26:1
icmp 213.235.1.2:2     192.168.2.2:2      213.235.1.26:2     213.235.1.26:2
icmp 213.235.1.2:3     192.168.2.2:3      213.235.1.26:3     213.235.1.26:3
icmp 213.235.1.2:4     192.168.2.2:4      213.235.1.26:4     213.235.1.26:4
```

Рис. 6.10. Результати роботи команди

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.
2. Побудуйте у Cisco Paket Tracer таку схему, як показано на рис. 6.4, використавши схему, розроблену у лабораторній роботі № 5 (див. рис. 6.3) відповідно до свого варіанта.
3. Проведіть настроювання пристроїв мережі відповідно до свого варіанта (табл. 6.1) та порядку, описаного в роботі. Настроювання проводьте, користуючись вкладкою **config**, крім роутера локальної мережі.

4. Перевірте доступність комп’ютерів з боку сервера та сервера з боку комп’ютерів за допомогою команди **ping**.
5. Виведіть таблицю маршрутизації роутера локальної мережі.
6. Виведіть таблицю трансляції IP-адрес роутером (Router1) локальної мережі (див. рис. 6.4).
7. За допомогою команди **show access-list** виведіть створений вами ACL.

Вимоги до звіту

Звіт з лабораторної роботи повинен містити:
1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Номер варіанта та умови завдань.
4. Команди настроювання мережних пристроїв.
5. Скріншоти кроків виконання роботи.
6. Файл *.pkt (Cisco Packet Tracer) зі схемою виконаного завдання.
7. Висновки.

Варіанти завдань

Таблиця 6.1

IP-адреси підмереж та ім’я ACL

Номер варіанта	Адреси підмереж		Ім’я ACL
	перша підмережа	друга підмережа	
1, 11	213.235.1.0	213.235.1.40	London
2, 12	213.235.1.4	213.235.1.44	Paris
3, 13	213.235.1.8	213.235.1.48	Belgrade
4, 14	213.235.1.12	213.235.1.52	Berlin
5, 15	213.235.1.16	213.235.1.56	Bratislava
6, 16	213.235.1.20	213.235.1.60	Brussels
7, 17	213.235.1.24	213.235.1.64	Dublin
8, 18	213.235.1.28	213.235.1.68	Kiev
9, 19	213.235.1.32	213.235.1.72	Madrid
10, 20	213.235.1.36	213.235.1.76	Monaco

Контрольні запитання

1. Які ви знаєте види **NAT**?
2. Для чого використовуються списки контролю доступу?
3. Яку інформацію містять списки контролю доступу?
4. Які є види **ACL**?
5. Яка різниця між стандартним та розширеним списком доступу?
6. Які переваги надають іменовані списки доступу?

Лабораторна робота № 7

МЕРЕЖНІ НАСТРОЙКИ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА. ВИКОРИСТАННЯ МЕРЕЖНИХ УТИЛІТ СТЕКА ПРОТОКОЛІВ TCP/IP

Мета роботи: вивчити мережні утиліти ОС Windows, навчитися використовувати утиліти стека протоколів TCP/IP.

Теоретичні відомості

Сучасні операційні системи Windows мають вбудовані мережні утиліти, що забезпечують засоби для встановлення та ідентифікації мережних підключень комп'ютера. Мережні утиліти відіграють критичну роль в інструментарії адміністраторів мереж, фахівців з безпеки та всіх, хто працює в галузі інформаційних технологій. Вони дають змогу ефективно контролювати стан мереж, діагностувати проблеми та забезпечувати надійність мережної інфраструктури.

Утиліта hostname

Виводить ім'я локального хоста. Використовується без параметрів.

Приклад 1. Виведення на екран імені локального хоста за допомогою команди *hostname* (рис. 7.1).

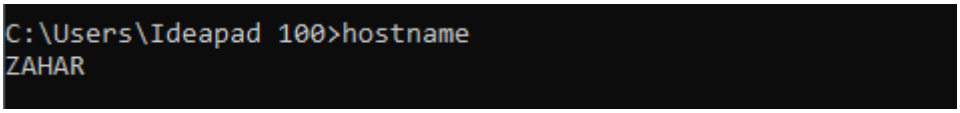

Рис. 7.1. Утиліта hostname

Утиліта ping

Утиліта ping (Packet Internet Groper) є одним із головних засобів, що використовуються для настроювання мереж і для примусового виклику відповіді конкретної машини. Ця утиліта дає змогу перевіряти роботу протоколів TCP/IP на віддалених машинах, адреси пристроїв у локальній мережі, адресу та маршрут для віддаленого мережного пристрою. У виконанні команди **ping** беруть участь система маршрутизації, схеми дозволу адрес та мережні шлюзи. Це утиліта низького рівня, яка не вимагає наявності серверних процесів на перевіряємій машині, тому успішний результат при проходженні запиту зовсім не означає, що виконуються будь-які сервісні програми високого рівня, а свідчить про те, що мережа знаходиться в робочому стані, живлення перевіряємої машини включено і машина не відмовила («не висить»).

Утиліта дає змогу перевірити:

– працездатність IP-з'єднання;

– правильність настройки протоколу TCP/IP на вузлі;

– працездатність маршрутизаторів;

– працездатність системи розпізнавання імен FQDN або NetBIOS;

– доступність і працездатність будь-якого мережного ресурсу.

Утиліта ***ping*** перевіряє з'єднання з віддаленим хостом шляхом відправки до цього хосту ехо-пакетів ICMP і прослуховування ехо-відповідей. ***Ping*** очікує кожен посланий пакет і виводить на екран кількість переданих і отриманих пакетів. Якщо зв'язок між хостами поганий, з повідомлень ***ping*** стане ясно, скільки пакетів втрачено.

За замовчуванням передається чотири ехо-пакети довжиною 32 байти. Утиліта ***ping*** дає змогу змінити розмір і кількість пакетів; вказати, чи слід записувати маршрут, який вона використовує; яку величину часу життя (TTL) встановлювати; чи можна фрагментувати пакет і т. ін. При отриманні відповіді в поле ***time*** (рис. 7.2) вказується, за який час (у мілісекундах) відправлений пакет доходить до віддаленого хоста і повертається назад. Оскільки значення за замовчуванням для очікування відгуку дорівнює 1 секунді, то всі значення цього поля будуть менше 1000 мілісекунд. Якщо надійшло повідомлення ***Request time out*** (перевищено інтервал очікування), то, можливо, якщо збільшити час очікування відповіді, пакет дійде до віддаленого хоста. Це можна зробити за допомогою ключа -**w**.

Ping можна використовувати для тестування як імені хоста (DNS або NetBIOS), так і його IP-адреси. Якщо команду ***ping*** з IP-адресою виконано успішно, а з ім'ям – невдало, це означає, що проблема виникла в розпізнаванні відповідності адреси та імені, а не під час встановлення зв'язку.

Синтаксис утиліти: ***ping*** *[-t] [-a] [-n <count>] [-l <length>] [-f] [-w <timeout>]*

У табл. 7.1 вкажемо основні і найбільш часто використовувані ключі утиліти ***ping*** і дамо їх короткий опис.

Таблиця 7.1

Ключі утиліти ping

Ключ	Опис
-t	Нескінченна (до натискання клавіш <Ctrl> + <Break>) відправка пакетів на вказаний вузол
-n <count>	Посилає кількість пакетів ECHO, вказану параметром count
-l <length>	Посилає пакети довжиною length байт (максимальна довжина 8192 байт)
-f	Посилає пакет зі встановленим прапором «Не фрагментувати». Цей пакет не буде фрагментуватися на маршрутизаторах по шляху свого проходження
-w <timeout>	Вказує час очікування (timeout) відповіді від віддаленого хоста в мілісекундах (за замовчуванням – 1 с)

Для перевірки того, що TCP/IP встановлено і правильно настроєно на локальному комп’ютері, в команді ***ping*** задається адреса *петлі зворотного зв'язку* (loopback address) **ping 127.0.0.1**.

Використання утиліти

Приклад 2. Використання утиліти **ping** з тестування інтерфейсу 127.0.0.1.

Адреса 127.0.0.1 – це особиста адреса будь-якого комп'ютера – **Loopback interface**. Таким чином, ця команда перевіряє проходження сигналу «на самого себе». Вона може бути виконана без наявності будь-якого мережного підключення. Ви повинні побачити приблизно такі рядки, які показано на рис. 7.2.

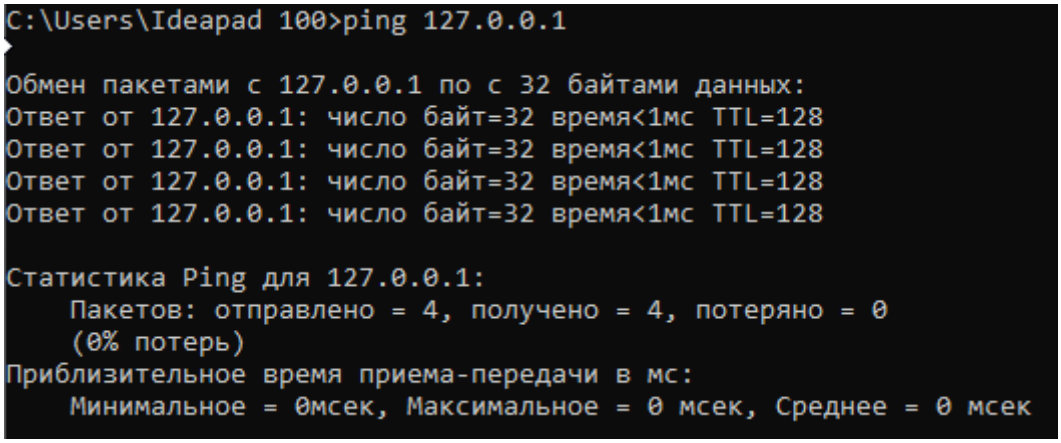

Рис. 7.2. Використання утиліти *ping* з **Loopback** інтерфейсом

Приклад 3. Заборона фрагментації пакета.

Серед додаткових опцій команда **ping** приймає прапор **-f** (рис. 7.3), який забороняє фрагментацію IP-пакета. Оскільки мережний рівень абстрагується від використовуваної технології канального рівня, то необхідний механізм, за допомогою якого можна передавати блоки даних довільної довжини через різні транспортні мережі з їх власними технологіями канального рівня, які мають різні обмеження на розмір кадру (MTU). Якщо пакет даних плюс службові заголовки перевищує розмір кадру, то пакет розбивається на фрагменти, які вже можуть бути передані в кадрах канального рівня. На кінцевому вузлі фрагменти збираються в єдиний пакет даних.

Друга опція команди – це прапор **-l**, після якого через пробіл вказується цифра – розмір буфера, який буде надсилатися на віддалений вузол в пакеті ICMP (див. рис. 7.3).

Якщо фрагментацію заборонено і розмір надсилаємого пакету завеликий для технології канального рівня, який використовує локальна мережа, то в операції буде відмовлено (див. рис. 7.3).

```
C:\Users\Ideapad 100>ping google.com -l 10000 -f

Обмен пакетами с google.com [142.250.203.206] с 10000 байтами данных:
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.
Требуется фрагментация пакета, но установлен запрещающий флаг.

Статистика Ping для 142.250.203.206:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)
```

Рис. 7.3. Використання опцій фрагментації та довжини пакета

Використовуючи спільно ключі **-l** і **-f**, можна з'ясувати максимальний розмір блока даних, поміщеного в IP-пакет, який інакше називається **MSS** (максимальний розмір сегмента). MSS буде дорівнювати довжині блока даних + довжині ICMP заголовка, який дорівнює 8 байт у випадку використання команди ***ping***. Розмір стандартного заголовка IP-пакета дорівнює 20 байт. Таким чином, MTU = «розмір буфера команди ping» 1500 + 20 + 8.

Приклад 4. Використання утиліти ***ping*** з різною кількістю ехо-запитів.

Якщо необхідно відправити певну кількість пакетів ECHO, то задайте параметр **-n** <count>, де параметр count дорівнює кількості запитів (рис. 7.4).

```
C:\Users\Ideapad 100>ping google.com -n 10

Обмен пакетами с google.com [142.250.203.206] с 32 байтами данных:
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117
Ответ от 142.250.203.206: число байт=32 время=15мс TTL=117

Статистика Ping для 142.250.203.206:
    Пакетов: отправлено = 10, получено = 10, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 15мсек, Максимальное = 15 мсек, Среднее = 15 мсек
```

Рис. 7.4. Використання опції -n

Якщо бажаєте створити нескінченний ряд запитів у часі, то використовуйте замість ключа **-n** ключ **-t** (рис. 7.5).

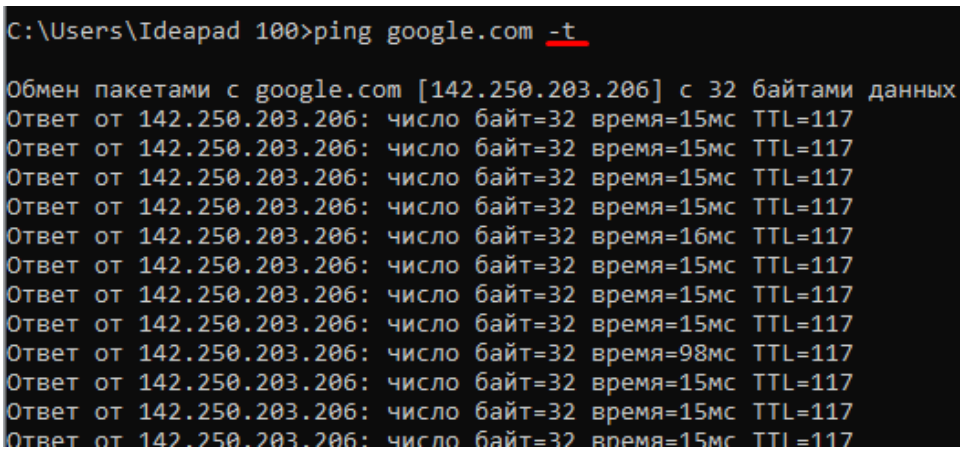

Рис. 7.5. Використання опції -t

Також утиліта ***ping*** дає змогу знайти IP-адресу хоста, коли звертаємось до нього за допомогою доменного імені. Наприклад, IP-адреса хоста з доменним ім'ям google.com – 142.250.203.206 (див. рис. 7.5).

Утиліта ipconfig

Цю утиліту використовують для відображення всіх поточних параметрів мережі TCP/IP і поновлення параметрів DHCP (Dynamic Host Configuration Protocol) і DNS (Domain Name System). При виклику команди ***ipconfig*** без параметрів виводяться IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера.

Синтаксис утиліти:

ipconfig [/all | / Renew [adapter] | / Release [adapter] | / Displaydns]

У табл. 7.2 вкажемо основні і найбільш часто використовувані ключі утиліти ***ipconfig*** і наведемо їх короткий опис.

Таблиця 7.2

Ключі утиліти **ipconfig**

Ключ	Опис
?	Показує довідку щодо команди
all	Відображає повну інформацію про настройки параметрів усіх адаптерів. Без цього ключа відображається тільки IP-адреса, маска і шлюз за замовчуванням
renew [adapter]	Оновлює параметри конфігурації DHCP для зазначеного мережного адаптера
release [adapter]	Звільняє виділену DHCP IP-адресу для зазначеного мережного адаптера
displaydns	Виводить інформацію про вміст локального кеша клієнта DNS, використовуваного для «розв'язання» доменних імен, тобто їх перетворення на IP-адреси

Таким чином, утиліта ***ipconfig*** (рис. 7.6) дає змогу з'ясувати, чи ініціалізована конфігурація і чи не дублюються IP-адреси:

– якщо конфігурація ініціалізована, то з'являється IP-адреса, маска, шлюз;

– якщо IP-адреси дублюються, то маска мережі буде 0.0.0.0;

– якщо при використанні DHCP комп'ютер не зміг отримати IP-адресу, то вона буде дорівнювати 0.0.0.0.

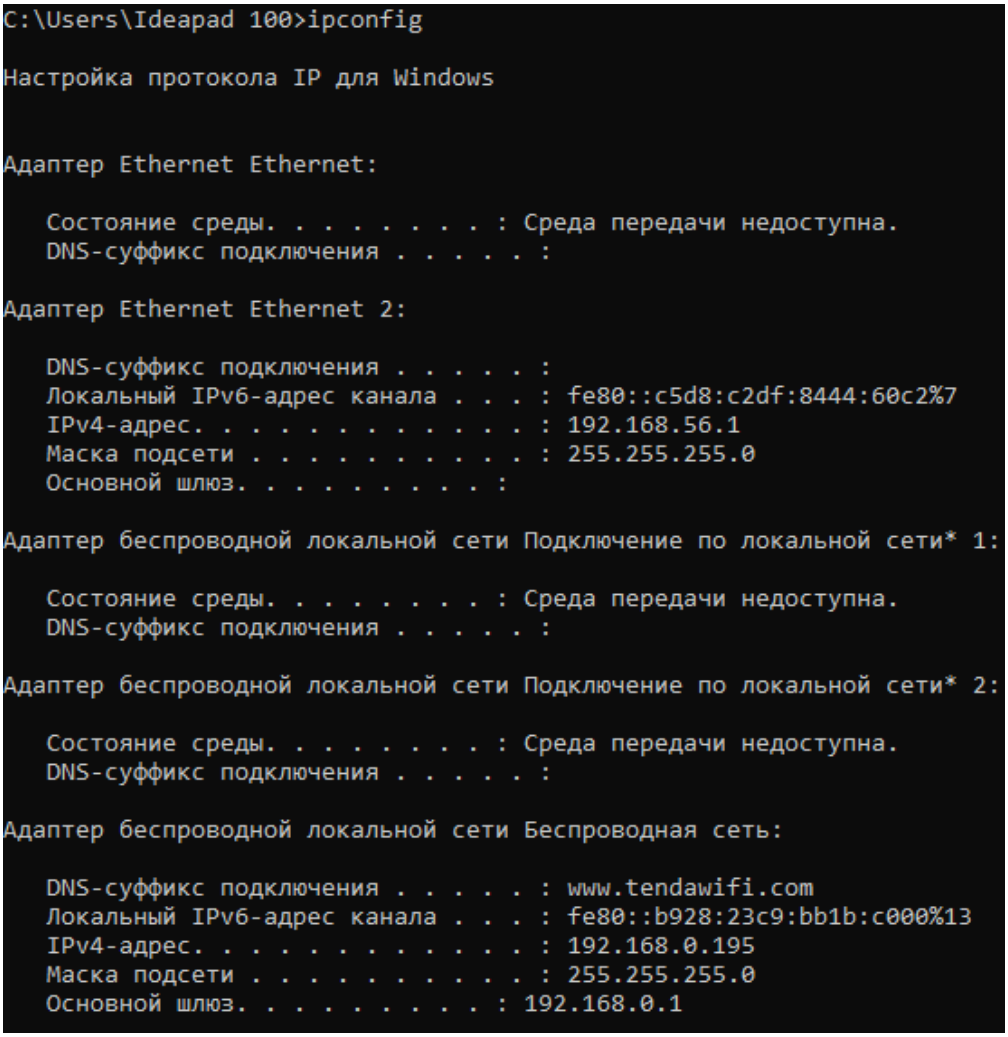

Рис. 7.6. Утіліта ipconfig без параметрів

Утиліта route

Утиліта ***route*** дає змогу переглядати маршрути проходження мережних пакетів при передачі інформації.

Синтаксис: route [-f] [-p] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

У табл. 7.3 наведено основні і найбільш часто використовувані ключі утиліти ***route*** і їх короткий опис.

Таблиця 7.3

Ключі утиліти route

Ключ	Опис
-f	Очищення таблиць маршрутів від записів усіх шлюзів. При зазначенні однієї з команд таблиці очищуються до виконання команди
-p	Очищення таблиць маршрутів від записів усіх шлюзів. При зазначенні однієї з команд таблиці очищуються до виконання команди
command	PRINT – виведення інформації про маршрут; ADD – додавання маршруту; DELETE – видалення маршруту; CHANGE – зміна маршруту
destination	Адреса вузла, якому передається пакет
MASK	Вказує, що наступний параметр інтерпретується як маска мережі: – netmask – значення маски підмережі для запису певного маршруту. Якщо цей параметр не заданий, за замовчуванням використовується значення 255.255.255.255; – gateway – шлюз; – interface – номер інтерфейсу для зазначеного маршруту
METRIC	Визначення метрики, тобто ціни маршрута до вузла, якому адресується пакет

У цілому процес IP-маршрутизації являє собою серії окремих операцій прямої або непрямої маршрутизації пакетів.

Кожен мережний вузол приймає рішення про маршрутизацію пакета на основі таблиці маршрутизації, яка зберігається в оперативній пам’яті вузла (комп’ютера). Таблиці маршрутизації існують не тільки у маршрутизаторів з декількома інтерфейсами, а й у робочих станцій, що під’єднуються до мережі через мережний адаптер.

Таблиця маршрутизації

Таблиця маршрутизації – це базова структура, яку використовують маршрутизатори для визначення найкращого шляху для пересилання пакетів між різними мережами. Вона містить записи про те, куди слід направляти пакети залежно від призначених IP-адрес.

Таблицю маршрутизації в системі Windows можна подивитися за допомогою команди ***route print***. Кожна таблиця маршрутизації містить набір записів, які можуть формуватися різними способами:

– записи, створені автоматично системою на основі конфігурації протоколу TCP/IP на кожному з мережних адаптерів;

– статичні записи, створені командою **route add** або в консолі служби Routing and Remote Access Service;

– динамічні записи, створені різними протоколами маршрутизації (RIP або OSPF).

Розглянемо два приклади: таблицю маршрутизації типової робочої станції, розташованої в локальній мережі компанії, і таблицю маршрутизації сервера, що має кілька мережних інтерфейсів.

Приклад. Таблиця маршрутизації робочої станції.

У цьому прикладі є робоча станція з системою Windows, з одним мережним адаптером і такими настройками протоколу IP: IP-адреса – 192.168.1.10, маска підмережі – 255.255.255.0, основний шлюз – 192.168.1.1. Введемо в командному рядку системи Windows команду ***route print*** (рис. 7.7).

```
C:\>route print

IPv4 таблица маршрута
===========================================================================
Список интерфейсов (Interface List)
0x1 ...........................          MS TCP Loopback interface
0x10002 ...00 c0 26 a1 6e 05 ......      Realtek   RTL8139   Family   PCI   Fast
Ethernet NIC
===========================================================================
===========================================================================
Активные маршруты (Active Routes):

Сетевой адрес     Маска сети       Адрес шлюза     Интерфейс       Метрика
(Network          (Netmask)        (Gateway)       (Interface)     (Metric)
Destination)
        0.0.0.0          0.0.0.0     192.168.1.1    192.168.1.10              1
      127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1              1
    192.168.1.0    255.255.255.0    192.168.1.10    192.168.1.10             20
   192.168.1.10  255.255.255.255       127.0.0.1       127.0.0.1             20
  192.168.1.255  255.255.255.255    192.168.1.10    192.168.1.10             20
      224.0.0.0        240.0.0.0    192.168.1.10    192.168.1.10             20
255.255.255.255  255.255.255.255    192.168.1.10    192.168.1.10              1
Основной шлюз (Default Gateway):      192.168.1.1
===========================================================================
Постоянные маршруты (Persistent Routes):
  Отсутствует (None)
```

Рис. 7.7. Результат роботи команди **route print** для комп’ютера

Зверху наведено список інтерфейсів, тобто список мережних адаптерів, встановлених у комп’ютері. Інтерфейс MS TCP **Loopback interface** присутній завжди і призначений для звернення вузла до самого себе. Інтерфейс Realtek RTL8139 Family PCI Fast Ethernet NIC – мережна карта. Закріплена за ним адреса 127.0.0.1.

Далі йде сама таблиця маршрутів. Кожен рядок таблиці – це маршрут для будь-якої IP-мережі. Її стовпці:

Мережна адреса – діапазон IP-адрес, досяжних за допомогою певного маршруту.

Маска мережі – маска підмережі, в яку відправляється пакет за допомогою певного маршруту.

Адреса шлюзу – IP-адреса вузла, на який пересилаються пакети, що відповідають певному маршруту.

Інтерфейс – позначення мережного інтерфейсу комп'ютера, на який пересилаються пакети, що відповідають певному маршруту.

Метрика – умовна вартість маршруту. Якщо для однієї і тієї ж мережі є кілька маршрутів, то вибирається маршрут з мінімальною вартістю. Зазвичай метрика – це кількість маршрутизаторів, які має пройти пакет, щоб потрапити в потрібну мережу.

Проаналізуємо деякі рядки таблиці.

Перший рядок таблиці відповідає значенню основного шлюзу в конфігурації TCP/IP мережного адаптера комп'ютера. Мережа з адресою «0.0.0.0» позначає «всі інші мережі, що не відповідають іншим рядкам цієї таблиці маршрутизації» – так званий «маршрут за замовчуванням», або «нульовий маршрут».

Другий рядок – маршрут для відправлення пакетів від вузла самому собі.

Третій рядок (мережа 192.168.1.0 з маскою 255.255.255.0) – маршрут для відправлення пакетів у локальній IP-мережі (тобто в тій мережі, де розташована ця робоча станція).

Останній рядок – широкомовна адреса для всіх вузлів локальної IP-мережі.

Останній рядок на рис. 7.8 – список постійних маршрутів робочої станції. Це статичні маршрути, створені командою **route add**. У цьому прикладі немає жодного такого статичного маршруту.

Приклад. Таблиця маршрутизації сервера.

Тепер розглянемо сервер з системою Windows 2003 Server, з трьома мережними адаптерами:

– адаптер 1 розташований у внутрішній мережі компанії (IP-адреса – 192.168.1.10, маска підмережі – 255.255.255.0);

– адаптер 2 розташований у зовнішній мережі інтернет-провайдера ISP-1 (IP-адреса – 213.10.11.2, маска підмережі – 255.255.255.248, найближчий інтерфейс у мережі провайдера – 213.10.11.1);

– адаптер 3 розташований у зовнішній мережі інтернет-провайдера ISP-2 (IP-адреса – 217.1.1.34, маска підмережі – 255.255.255.248, найближчий інтерфейс у мережі провайдера – 217.1.1.33).

IP-мережі провайдерів умовні, IP-адреси обрані лише для ілюстрації (хоча цілком можливий випадковий збіг з будь-якою існуючою мережею).

Крім того, на сервері встановлено Службу маршрутизації та віддаленого доступу для керування маршрутизацією пакетів між IP-мережами і доступу в мережу компанії через модемний пул.

У таблиці в списку інтерфейсів відображені три мережних адаптери різних моделей, адаптер зворотного зв'язку (MS TCP Loopback interface) і WAN (PPP/SLIP) Interface – інтерфейс для доступу в мережу через модемний пул.

Відзначимо особливості таблиці маршрутів сервера з декількома мережними інтерфейсами.

Перший рядок схожий на перший рядок у таблиці робочої станції. Вона також відповідає значенню основного шлюзу в конфігурації TCP/IP цієї станції. Зауважимо, що тільки на одному інтерфейсі можна задавати параметр «Основний шлюз». У цьому випадку цей параметр було встановлено на одному із зовнішніх інтерфейсів (це ж значення відображено і в кінці таблиці в рядку «Основний шлюз»).

Як і в робочій станції, для кожного інтерфейсу є маршрути як для unicast-пакетів, так і для широкомовних (broadcast) для кожної підмережі.

У цьому випадку команда ***route print*** надрукує таблицю маршрутизації, зображену на рис. 7.8.

```
C:\>route print

IPv4 таблица маршрута
===========================================================================
Список интерфейсов (Interface List)
0x1 ...........................          MS TCP Loopback interface
0x10002 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
0x10003 ...00 03 47 97 61 81 ...... Intel(R) 10/100 Network Adapter
0x10004 ...00 02 b3 a6 be 48 ...... Intel(R) PRO/100 Adapter
0x10005 ...00 d0 b7 b7 fd df ...... Intel 8255x-based PCI Ethernet Adapter
(10/100)
===========================================================================
===========================================================================
Активные маршруты (Active Routes):

Сетевой адрес     Маска сети       Адрес шлюза     Интерфейс       Метрика
(Network          (Netmask)        (Gateway)       (Interface)     (Metric)
Destination)
        0.0.0.0          0.0.0.0     213.10.11.1     213.10.11.2              20
   196.15.20.16    255.255.255.0      217.1.1.33      217.1.1.33               1
      127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1               1
    192.168.1.0    255.255.255.0     192.168.1.1     192.168.1.1              20
    192.168.1.1  255.255.255.255       127.0.0.1       127.0.0.1              20
  192.168.1.255  255.255.255.255     192.168.1.1     192.168.1.1              20
   192.168.10.1  255.255.255.255       127.0.0.1       127.0.0.1              50
    213.10.11.0  255.255.255.248     213.10.11.2     213.10.11.2              20
    213.10.11.2  255.255.255.255       127.0.0.1       127.0.0.1              20
  213.10.11.255  255.255.255.255     213.10.11.2     213.10.11.2              20
     217.1.1.32  255.255.255.248      217.1.1.33      217.1.1.33              20
     217.1.1.34  255.255.255.255       127.0.0.1       127.0.0.1              20
    217.1.1.255  255.255.255.255      217.1.1.34      217.1.1.34              20
      224.0.0.0        240.0.0.0     192.168.1.1     192.168.1.1              20
      224.0.0.0        240.0.0.0     213.10.11.2     213.10.11.2              20
      224.0.0.0        240.0.0.0      217.1.1.34      217.1.1.34              20
255.255.255.255  255.255.255.255     192.168.1.1     192.168.1.1               1
255.255.255.255  255.255.255.255     213.10.11.2     213.10.11.2               1
255.255.255.255  255.255.255.255      217.1.1.34      217.1.1.34               1
Основной шлюз (Default Gateway):     213.10.11.1
===========================================================================
Постоянные маршруты (Persistent Routes):
  Отсутствует (None)
```

Рис. 7.8. Результат роботи команди **route print** для сервера

Підтримка таблиць маршрутизації

Є два способи підтримки актуального стану таблиць маршрутизації: ручний і автоматичний.

Ручний спосіб підходить для невеликих мереж. У цьому випадку до

таблиці маршрутизації вручну заносять статичні записи для маршрутів. Записи створюють або командою **route add**, або в консолі служби маршрутизації і віддаленого доступу.

У великих мережах ручний спосіб стає занадто трудомістким і може спричинити помилки. Автоматична побудова і модифікація таблиць маршрутизації проводиться так званими «динамічними маршрутизаторами». Динамічні маршрутизатори відстежують зміни в топології мережі, вносять необхідні зміни в таблиці маршрутів і обмінюються цією інформацією з іншими маршрутизаторами, які працюють за тими ж протоколами маршрутизації. У Windows Server реалізована динамічна маршрутизація в службі маршрутизації і віддаленого доступу. У цій роботі реалізовані найбільш поширені протоколи маршрутизації – протокол **RIP** версій 1 і 2 та протокол **OSPF**.

Утиліта arp

Утиліта **arp** дає змогу отримати таблицю відповідності IP-адреси і MAC-адреси. Основне завдання протоколу ARP – трансляція IP-адрес на відповідні MAC-адреси. Для цього ARP-протокол використовує інформацію з ARP-таблиці (ARP-кеша). Якщо необхідний запис у таблиці не знайдено, то протокол ARP спрямовує широкомовний запит до всіх комп'ютерів локальної мережі, намагаючись знайти власника цієї IP-адреси. У кеші можуть міститися два типи записів: статичні і динамічні. Статичні записи вводяться вручну і зберігаються в кеші постійно. Динамічні записи поміщаються в кеш унаслідок виконання широкомовних запитів. Для них існує поняття часу життя. Якщо протягом певного часу (за замовчуванням 2 хв.) запис не був затребуваний, то він видаляється з кешу. Приклад використання утиліти показано на рис. 7.9.

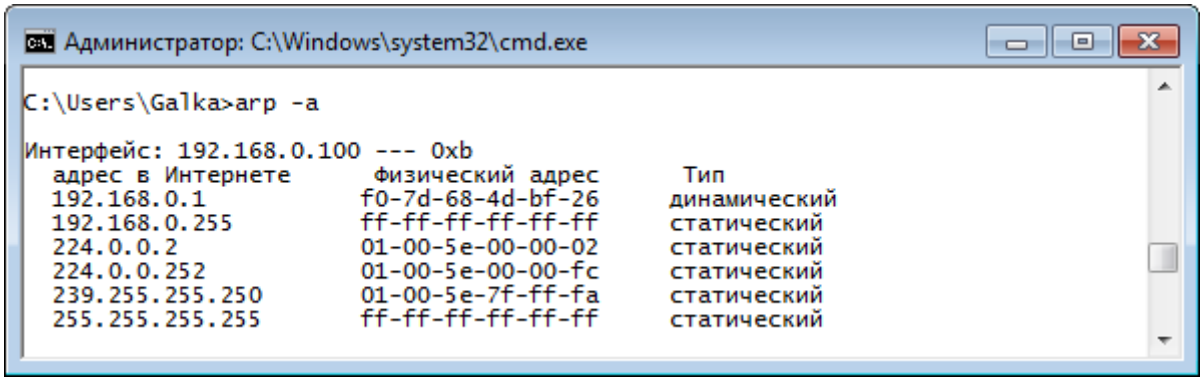

Рис. 7.9. Утиліта **arp**

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

У табл. 7.4 наведено основні і найбільш часто використовувані ключі утиліти **arp** та їх короткий опис.

Таблиця 7.4

Ключі утиліти **arp**

Ключ	Опис
-s	Занесення в кеш статичних записів
-d	Видалення з кешу записів для певної IP-адреси
-a	Перегляд вмісту кешу для всіх мережних адаптерів локального комп’ютера
inet_addr	Визначає IP-адресу
N if_addr	Відображає ARP-запис для заданого в if_addr мережного інтерфейсу

Утиліта netstat

Утиліта **netstat** дає змогу отримати статичну інформацію щодо деяких протоколів стека (TCP, UDP, IP, ICMP), а також виводить відомості про поточні мережні з’єднання. Особливо вона є корисною на брандмауерах, з її допомогою можна виявити порушення безпеки периметра мережі.

Синтаксис: netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

У табл. 7.5 вказані основні і найбільш часто використовувані ключі утиліти *netstat* і наведено їх короткий опис.

Таблиця 7.5

Ключі утиліти **netstat**

Ключ	Опис
-a	Відображення всіх активних з'єднань та портів, які прослуховуються на комп’ютері
-n	Відображення адрес і номерів портів у числовому форматі
-o	Відображення коду (ID) процесу кожного підключення
-r	Відображення вмісту локальної таблиці маршрутів

Якщо запустити команду ***netstat*** без параметрів, то можна отримати список активних TCP-з’єднань між локальним і віддаленими комп’ютерами. У колонці «стан» відображається статус TCP-з’єднання.

За замовчуванням ***netstat*** перетворює отримані IP-адреси на символьні імена DNS і номери портів на назви мережних служб. Це уповільнює роботу netstat, тому, якщо перетворення не потрібно, то можна вказати ключ **-n**.

Відображення списку активних підключень і портів, які прослуховуються

Команда **netstat** з ключем **-an** відображає в числовій формі список активних підключень і портів, які прослуховуються (рис. 7.10).

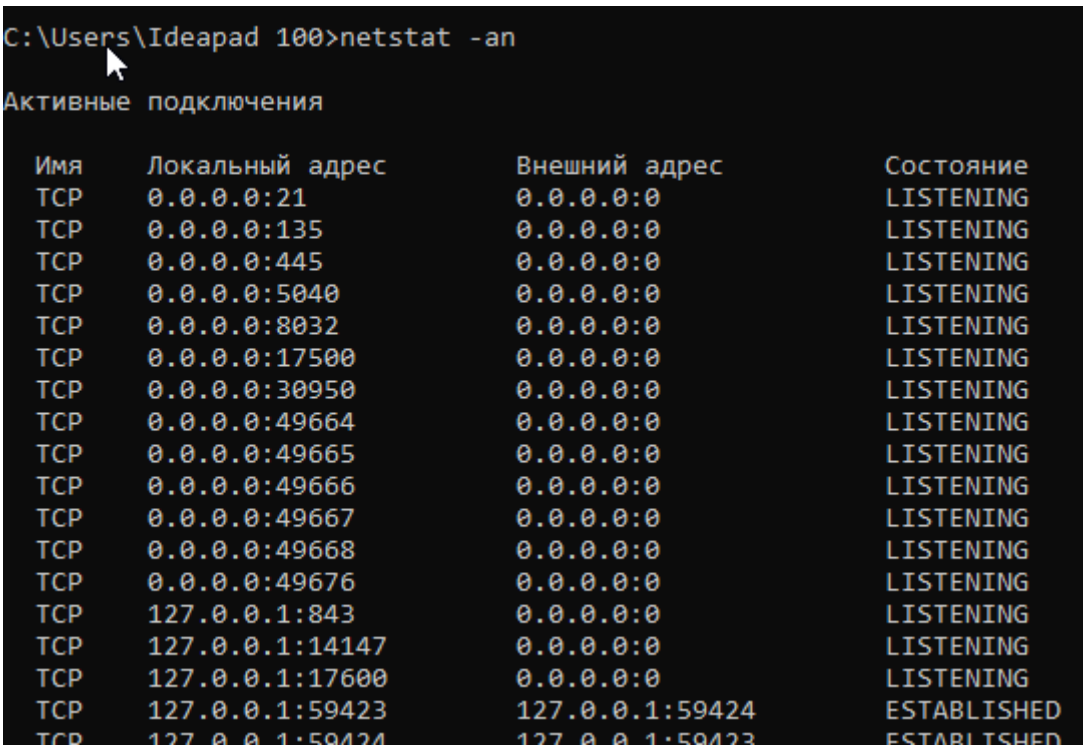

Рис. 7.10. Утиліта **netstat**

Утиліта Tracert

Визначає шлях до точки призначення за допомогою посилання в точку призначення повідомлень-запитів (ping) протоколу Internet Control Message Protocol (ICMP) з постійним збільшенням значень терміну життя (Time to Live, TTL). Виведений шлях – це список найближчих інтерфейсів маршрутизаторів, що знаходяться на шляху між вузлом джерела та точкою призначення. Близький інтерфейс є інтерфейсом маршрутизатора, який є найближчим до вузла відправника на шляху. Запущена без параметрів команда tracert виводить довідку.

Синтаксис: tracert [-d] [-h максимальна_кількість_стрибків] [-j список_вузлів] [-w інтервал] [ім’я_кінцевого_комп’ютера]

У табл. 7.6 наведено основні і найбільш часто використовувані ключі утиліти **tracert** і їх короткий опис.

Таблиця 7.6

Ключі утиліти **Tracert**

Ключ	Опис
-d	Без перетворення IP-адрес в імена вузлів
-h <макс.кількість>	Максимальна кількість стрибків при пошуку вузла
-w <таймаут>	Таймаут кожної відповіді в мілісекундах

Трасування маршруту

Приклад. *Команда* ***tracert****.* На рис. 7.11 наведено трасування маршруту до вузла google.com (якщо маєте у розпорядженні тільки одну IP-мережу, то вивчити роботу цієї команди буде неможливо).

```
C:\Users\Ideapad 100>tracert google.com

Трассировка маршрута к google.com [142.250.203.206]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     4 ms  192.168.0.1
  2     4 ms     1 ms     1 ms  gw-v239.cosmonova.net.ua [95.67.97.129]
  3     2 ms     1 ms     1 ms  jGrin.ua.cosmonova.net.ua [95.67.1.9]
  4     1 ms     3 ms     2 ms  jZh.ua.cosmonova.net.ua [95.67.1.8]
  5     3 ms     2 ms     7 ms  142.250.175.80
  6     5 ms     2 ms     2 ms  142.250.238.57
  7     2 ms    23 ms     2 ms  74.125.245.64
  8     3 ms     2 ms     2 ms  72.14.239.110
  9    43 ms    15 ms    18 ms  142.251.242.35
 10    17 ms    21 ms    17 ms  142.251.253.217
 11    15 ms    20 ms    17 ms  209.85.252.109
 12    17 ms    15 ms    15 ms  waw02s22-in-f14.1e100.net [142.250.203.206]

Трассировка завершена.
```

Рис. 7.11. Утиліта **tracert**

Як видно з рисунка 7.11, кількість стрибків до кінцевого сервера google.com (142.250.203.206) дорівнює 12.

Утиліта pathping

Надає інформацію про латентність мережі та втрати даних на проміжних вузлах між вихідним пунктом та пунктом призначення. Команда **Pathping** протягом деякого періоду часу надсилає численні повідомлення з ехо-запитом кожному маршрутизатору, що знаходиться між вихідним пунктом і пунктом призначення, а потім на підставі пакетів, отриманих від кожного з них, обчислює результати. Оскільки pathping показує коефіцієнт втрати пакетів кожного маршрутизатора або зв’язку, можна визначити маршрутизатори чи субмережі, що мають проблеми з мережею. Команда **Pathping** виконує еквівалентну команді **tracert** дію, ідентифікуючи маршрутизатори, що знаходяться на шляху. Потім вона періодично протягом заданого часу обмінюється пакетами з усіма маршрутизаторами і, залежно від кількості пакетів, отриманих від кожного маршрутизатора, обробляє статистику. Запущена без параметрів команда pathping виводить довідку.

Синтаксис: pathping [-n] [-h максимальна_кількість_переходів] [-g список_вузлів] [-p період] [-q кількість_запитів] [-w інтервал] [-T] [-R] [ім’я_кінцевого_комп’ютера]

На рис. 7.12 зображено роботу з утилітою **pathping**.

```
C:\Users\Ideapad 100>pathping google.com -q 10

Трассировка маршрута к google.com [142.250.203.206]
с максимальным числом переходов 30:
  0  ZAHAR.www.tendawifi.com [192.168.0.195]
  1  192.168.0.1
  2  gw-v239.cosmonova.net.ua [95.67.97.129]
  3  jGrin.ua.cosmonova.net.ua [95.67.1.9]
  4  jZh.ua.cosmonova.net.ua [95.67.1.8]
  5  142.250.175.80
  6  142.250.238.57
  7  74.125.245.64
  8  72.14.239.110
  9  142.251.242.35
 10  142.251.253.217
 11  209.85.252.109
 12  waw02s22-in-f14.1e100.net [142.250.203.206]

Подсчет статистики за: 30 сек. ...
           Исходный узел     Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                            ZAHAR.www.tendawifi.com [192.168.0.195]
                                 0/  10 =  0%   |
  1    1мс     0/  10 =  0%     0/  10 =  0%  192.168.0.1
                                 0/  10 =  0%   |
  2    1мс     0/  10 =  0%     0/  10 =  0%  gw-v239.cosmonova.net.ua [95.67.97.129]
                                 0/  10 =  0%   |
  3    4мс     0/  10 =  0%     0/  10 =  0%  jGrin.ua.cosmonova.net.ua [95.67.1.9]
                                 0/  10 =  0%   |
  4    3мс     0/  10 =  0%     0/  10 =  0%  jZh.ua.cosmonova.net.ua [95.67.1.8]
                                 0/  10 =  0%   |
  5    2мс     0/  10 =  0%     0/  10 =  0%  142.250.175.80
                                 0/  10 =  0%   |
  6    2мс     0/  10 =  0%     0/  10 =  0%  142.250.238.57
                                 0/  10 =  0%   |
  7    3мс     0/  10 =  0%     0/  10 =  0%  74.125.245.64
                                 0/  10 =  0%   |
  8    6мс     0/  10 =  0%     0/  10 =  0%  72.14.239.110
                                 0/  10 =  0%   |
  9   16мс     0/  10 =  0%     0/  10 =  0%  142.251.242.35
                                 0/  10 =  0%   |
 10   16мс     0/  10 =  0%     0/  10 =  0%  142.251.253.217
                                 0/  10 =  0%   |
 11   15мс     0/  10 =  0%     0/  10 =  0%  209.85.252.109
                                 0/  10 =  0%   |
 12   15мс     0/  10 =  0%     0/  10 =  0%  waw02s22-in-f14.1e100.net [142.250.203.206]
```

Рис. 7.12. Утиліта **pathping**

У табл. 7.7 наведено основні і найбільш часто використовувані ключі утиліти ***pathping*** і їх короткий опис.

Таблиця 7.7

Ключі утиліти **pathping**

Ключ	Опис
-n	Без перетворення IP-адрес на імена вузлів
-h <макс кількість>	Максимальна кількість стрибків при пошуку вузла
-q <кількість_запитів>	Кількість запитів при кожному стрибку
-w <таймаут>	Таймаут кожної відповіді в мілісекундах

Утиліта nslookup

Утиліта *nslookup* призначена для діагностики служби DNS, в найпростішому випадку – для виконання запитів до DNS-серверів на перетворення доменних імен на IP-адреси.

Синтаксис: nslookup хост [сервер]

Параметри утиліти

Хост – DNS-ім’я хоста, яке має бути перетворено на IP-адресу.

Сервер – адреси DNS-сервера, який буде використовуватися для перетворення імені. Якщо цей параметр опущений, то будуть послідовно використані адреси DNS-серверів з параметрів настройки протоколу TCP/IP.

Приклад роботи з утилітою

У найпростішому випадку утиліта *nslookup* має такий вигляд (рис. 7.13).

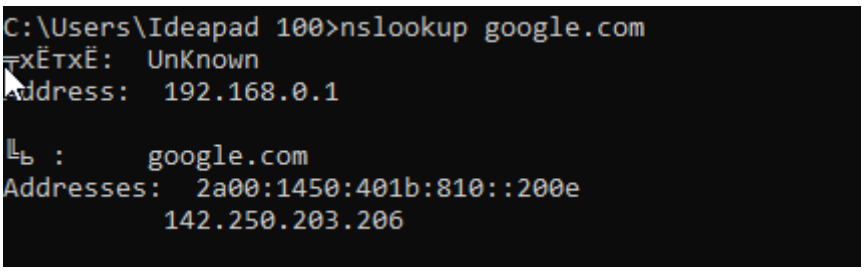

Рис. 7.13. Утиліта *nslookup*

Завдання для виконання лабораторної роботи

1. Вивчіть теоретичну частину.

2. Самостійно виконайте наведені приклади, використовуючи мережні можливості операційної системи *Windows* і утиліт стека протоколів TCP/IP. Під час роботи з утилітами всі команди слід виконувати в командному інтерпретаторі. Для його запуску натисніть кнопку «Пуск» і виберіть розділ «Виконати...». У рядку введення вкажіть ім’я команди: **cmd** і натисніть кнопку OK. Відкриється вікно інтерпретатора. Команди вводяться з клавіатури, завершуються введенням Enter.

3. Засобами ОС Windows визначте:

– загальні відомості про систему;
– IP-адресу, маску підмережі;
– ім’я комп’ютера, робочої групи.

4. Визначте ім’я локального хоста.

5. Виконайте команду ping 127.0.0.1 і перевірте правильність установки TCP/IP.

6. Перевірте доступність по мережі будь-якого сусіднього комп’ютера.

7. Експериментально з’ясуйте максимальний розмір кадру канального рівня (MTU). Для цього посилайте пакети різної довжини при встановленому

прапорі заборони фрагментації. Як віддалений вузол можна вибрати адресу шлюзу або адресу будь-якого сусіднього комп’ютера. Почніть з початкового значення розміру буфера 1500.

8. Виконайте команду *ipconfig* і запишіть інформацію про IP-адреси, маски мережі і шлюзи за замовчуванням для мережного адаптера.

9. Виконайте команду *ipcofig /all* і запишіть інформацію про апаратну адресу мережної карти, списку DNS-серверів мережного підключення.

10. Отримайте таблицю маршрутизації локального комп’ютера.

11. Отримайте таблицю ARP локального комп’ютера.

12. Отримайте список активних TCP-з'єднань локального комп’ютера.

13. Отримайте список активних TCP-з'єднань локального комп’ютера без перетворення IP-адрес на символьні імена DNS.

Контрольні запитання

1. Які вбудовані мережні утиліти системи Windows ви знаєте?
2. На базі якого протоколу побудована утиліта ping?
3. Що таке Loopback interface?
4. Який ключ використовується для виведення повної інформації про мережні інтерфейси вузла за допомогою команди Ipconfig?
5. Яка команда використовується для виведення таблиці маршрутизації вузла?
6. Для чого використовується фрагментація пакетів?
7. Яку інформацію надає користувачу ARP-таблиця?
8. Які утиліти поєднує в собі утиліта pathping?

Вимоги до звіту

Звіт з лабораторної роботи має містити:

1. Титульний аркуш.
2. Відповіді на контрольні запитання.
3. Скріншоти кроків виконання роботи.
4. Висновки.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Буров, Є. В. Комп’ютерні мережі : підручник / Є. В. Буров. – Львів : Магнолія 2006, 2013. – 264 с.

2. Николайчук, Я. М. Проектування спеціалізованих комп’ютерних систем : навч. посіб. / Я. М. Николайчук, Н. Я. Возна, Р. І. Пітух. – Тернопіль : ТзОВ «Терно-Граф», 2010. – 394 с.

3. Кравчук, С. О. Основи комп’ютерної техніки: компоненти, системи, мережі : навч. посіб. / С. О. Кравчук, В. О. Шанін. – Київ : Політехніка, 2005. – 344 с.

4. Олексюк, В. П. Організація комп’ютерної локальної мережі / В. П. Олексюк, Н. В. Балик, А. Н. Балик. – Тернопіль : Підручники та посібники, 2006. – 80 с.

5. Ткаченко, В. А. Комп’ютерні мережі та телекомунікації : навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків : НТУ ХПІ, 2011. – 224 с.

6. Internet of Things for Industry and Human Application. In Volumes 1–3. Vol. 1. Fundamentals and Technologies / V. S. Kharchenko (ed.). – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 605 p.

Навчальне видання

Захаренко Володимир Олександрович
Носиков Олександр Сергійович

КОМП’ЮТЕРНІ МЕРЕЖІ

Редактор Н. В. Мазепа

Зв. план, 2025
Підписано до видання 30.12.2025
Ум. друк. арк. 5,2. Обл.-вид. арк. 5,88. Електронний ресурс

Видавець і виготовлювач
Національний аерокосмічний університет
«Харківський авіаційний інститут»
61070, Харків-70, вул. Вадима Манька, 17
https://khai.edu

Свідоцтво про внесення суб’єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції сер. ДК № 391 від 30.03.2001