МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет
науки і технологій**

Кафедра «Електронні
обчислювальні машини»

В авторській редакції

КОМП'ЮТЕРНІ МЕРЕЖІ

(ЧАСТИНА 1)

Навчально-методичні рекомендації
до лабораторних робіт

Електронне видання

ДНІПРО
2023

УДК 004.7
К 63

Упорядники:
І. В. Жуковицький, О. П. Заєць, В. В. Дзюба

Електронне видання

Схвалено Групою забезпечення якості освітньої програми
123 «Комп’ютерна інженерія»
Протокол № 1 від 06.10.2023

Схвалено Групою забезпечення якості освітньої програми
125 «Кібербезпека»
Протокол № 1 від 06.10.2023

К 63 Комп'ютерні мережі : навчально-методичні рекомендації до лабораторних робіт / упоряд. : І. В. Жуковицький, О. П. Заєць, В. В. Дзюба ; Укр. держ. ун-т науки і технологій. – Електрон. вид. – Дніпро : УДУНТ, 2023. – Ч. 1. – 48 с.

Навчально-методичні рекомендації призначені для використання студентами безвідривної форми навчання спеціальностей 123 «Комп'ютерна інженерія» та 125 «Кібербезпека та безпека інформації» під час виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» в першому модулі курсу.

Навчально-методичні рекомендації містять основні теоретичні положення для засвоєння матеріалу, інструкції до виконання лабораторних робіт, вимоги до аналізу результатів та оформлення робіт, контрольні питання.

ЗМІСТ

Вступ 4

Лабораторна робота №1. Дослідження мережевої топології «зірка» засобами програми Cisco Packet Tracer 5

Лабораторна робота №2. Дослідження роботи протоколу arp засобами програми Cisco Packet Tracer 21

Лабораторна робота №3. Інсталяція налаштування та експерименти з віртуальною машиною Ubuntu 27

Лабораторна робота № 4. Дослідження методу використання масок та префіксів для визначення ipv4-адрес мереж та хостів 40

Додаток 1. Формат команди ping 47

Додаток 2. Опції команди tcpdump 47

Список літератури 49

ВСТУП

Дисципліна «Комп'ютерні мережі» відноситься до обов’язкової компоненти (ОК14) освітньо-професійної програми (ОП) «Комп'ютерна інженерія» першого (бакалаврського) рівня вищої освіти та до обов’язкової компоненти (ОК15) освітньо-професійної програми (ОП) «Кібербезпека» першого (бакалаврського) рівня вищої освіти.

Дане навчально-методичне видання сприяє здобуттю майбутніми фахівцями наступних результатів навчання (вміння, згідно робочих програм з цієї дисципліні за обома освітніми програмами):

- пояснювати роботу основних мережевих протоколів;
- налаштовувати систему мережевих адрес;
- досліджувати роботу мережевих протоколів;
- аналізувати мережевий трафік.

В даному навчально-методичному виданні надані вказівки до виконання 4 лабораторних робіт, які заплановані для виконання в першому модулі курсу. Частка лабораторних робіт виконується на програмному симуляторі Cisco Packet Tracer для моделювання комп'ютерних мереж (університет є філією академії компанії Cisco і має право використовувати цю програму).

Інша частка лабораторних робіт виконується в середовищі ОС Ubuntu (ОС, що вільно розповсюджується) з використанням віртуальних машин, що дає змогу на одній машині створювати мережу з декількох віртуальних машин і проводити, таким чином, дослідження мережі на одній реальній машині. Це особливо актуально в умовах можливої (в межах окремого часу) дистанційної форми навчання.

В методичних вказівках до кожної лабораторної роботи наведено відповідні теоретичні відомості, послідовність виконання роботи, індивідуальне завдання щодо цієї роботи (за варіантами), зміст звіту, контрольні питання.

Все необхідне для виконання лабораторних робіт програмне забезпечення викладено в системі дистанційного навчання «Лідер» університету в курсі «Комп'ютерні мережі».

Лабораторна робота № 1

ДОСЛІДЖЕННЯ МЕРЕЖЕВОЇ ТОПОЛОГІЇ «ЗІРКА» ЗАСОБАМИ ПРОГРАМИ CISCO PACKET TRACER

Мета роботи. Ознайомитися з програмою Cisco Packet Tracer для моделювання комп'ютерних мереж. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички по базовим настройках мережевих пристроїв. Засобами програми Cisco Packet Tracer дослідити мережі з топологією «Зірка» з концентратором і комутатором.

1.1 Знайомство з програмою Cisco Packet Tracer

Даний симулятор дозволяє проектувати свої власні мережі, вивчати і використовувати такі мережеві пристрої, як комутатори другого і третього рівнів, робочі станції, визначати типи зв'язків між ними і з'єднувати їх. Конфігурація обраних пристроїв можлива за допомогою термінального доступу або командного рядка. Далі можливо моделювання роботи створеної мережі.

Для запуску Cisco Packet Tracer необхідно викликати виконуваний файл. В даному курсі це PacketTracer5.exe (в подальшому можуть використовуватися інші версії). Загальний вигляд інтерфейсу (головного вікна) показаний на рис. 1.1.

У головному вікні зазвичай присутні наступні елементи:

1) Робоча область (Workspace) – область, в якій відбувається будівля мережі, проводяться спостереження за симуляцією і проглядається різна інформація і статистика.

2) Головне меню (Menu Bar) – панель, яка містить меню File, Edit, Options, View, Tools, Extensions, Help.

3) Графічне меню (Main Tool Bar) – містить графічні зображення ярликів для доступу до команд меню File, Edit, View і Tools, а також кнопку Network Information.

4) Панель інструментів (Common Tools Bar) – Панель, яка забезпечує доступ до найбільш часто використовуваних інструментів програми.

Інструмент **Select (Вибрати)**  (можна активувати клавішею Esc) використовується для виділення одного або більше об'єктів для подальшого їх переміщення, копіювання або видалення.

Інструмент **Move Layout (Перемістити шар)**  (клавіша M) використається для прокрутки великих проектів мереж.

Інструмент **Place Note (Зробити позначку)**  (клавіша N) додає текст в робочій області проекту.

Інструмент **Delete (Видалити)**  (клавіша Del) видаляє виділений об'єкт або групу об'єктів.

Інструмент **Inspect (Перевірка)**  (клавіша I) дозволяє, в залежності від типу пристрою, переглядати вміст таблиць (ARP, NAT, таблиці маршрутизації тощо).

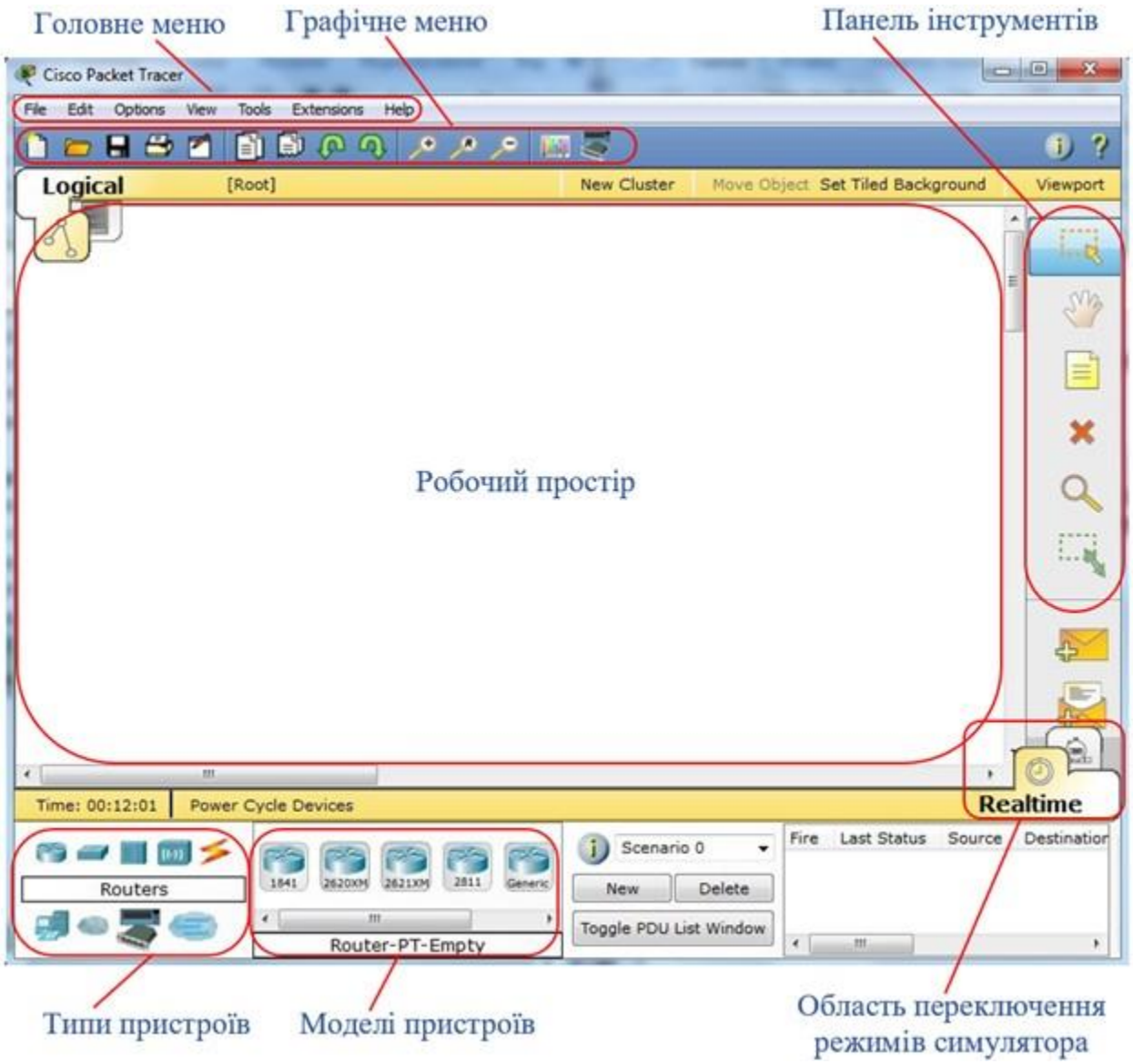


Рисунок 1.1 – Загальний вигляд інтерфейсу (головного вікна) Cisco Packet Tracer

5) Панель обладнання (Network Component Box). Це область, в якій вибираються пристрої та лінії зв'язку для розміщення їх на робочому просторі. Дана панель містить в своїй лівій частині (область **Device-Type Selection** – **типи пристроїв**) доступні типи пристроїв і зв'язків в Packet Tracer. При наведенні на кожен з типів пристроїв в прямокутнику, що знаходиться в центрі між ними, буде відображатися його назва. При натисканні покажчика миші на типі обладнання в правій частині панелі (область **Device-Specific Selection – моделі пристроїв**), відобразіться набір конкретних моделей цього типу обладнання, доступних в Cisco Packet Tracer.

Типи обладнання представлені на рис. 1.2.

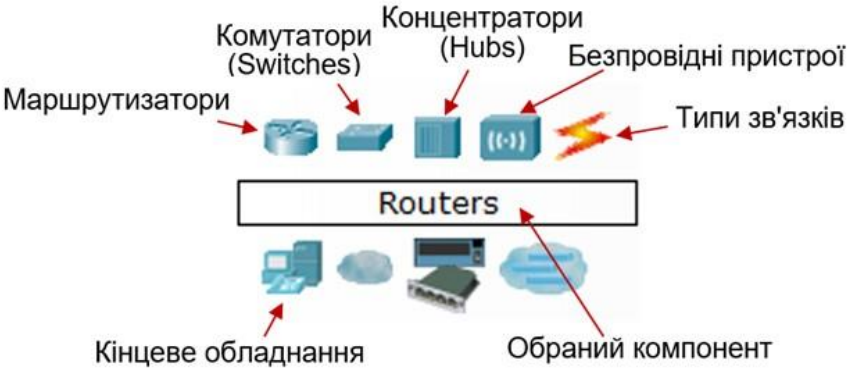


Рисунок 1.2 – Панель обладнання (область Device-Type Selection)

Маршрутизатори (routers) – пристрої, які пересилають пакунки між різними сегментами мережі на підставі алгоритмів маршрутизації.

Комутатори (switches) і **концентратори (habs)** – пристрої, призначені для об'єднання декількох вузлів в межах одного або декількох фізичних сегментів мережі.

Бездротові пристрої в програмі представлені бездротовим маршрутизатором і трьома точками доступу.

Серед **кінцевого обладнання** присутні ПК, ноутбук, сервер, принтер, телефони і так далі.

Типи з'єднання включають набір ліній зв'язку за допомогою яких створюються з'єднання вузлів мережі в єдину топологію і при цьому кожен тип кабелю може бути з'єднаний лише з певними типами інтерфейсів пристроїв (рис. 1.3).

Рисунок 1.3 – Типи ліній зв'язку

Автоматичний тип – при даному типі з'єднання Packet Tracer автоматично вибирає найбільш кращі тип з'єднання для обраних пристроїв.

Консоль (Console) – консольні з'єднання. Консольне з'єднання може бути виконано між ПК і маршрутизатором або комутатором.

Мідний прямий (Copper Straight-through) – цей тип кабелю є стандартною середовищем передачі Ethernet для з'єднання пристроїв, які функціонує на різних рівнях OSI (наприклад, комутатор і PC).

Мідний кросовер (Copper Cross-Over) – цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI (наприклад, комутаторів між собою).

Послідовний DCE і **послідовний DTE** – з'єднання через послідовні порти. Для налагодження таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристрою. Сторону DCE можна визначити по маленькій іконці "годинник" поруч з портом.

6) Realtime / Simulation Bar (Область перемикання режимів симулятора) – За допомогою закладок цієї панелі можна переключатися між режимом Realtime і режимом Simulation. Вона також містить кнопки Add Simple PDU (Додати простий PDU, клавіша P) і Add Complex PDU (Додати комплексний PDU, клавіша C), що призначені для емуляції відправки пакета з подальшим відстеженням його маршруту і даних всередині пакету.

1.2 Загальні принципи побудови комп'ютерних мереж

У комп'ютерній мережі ряд кінцевих пристроїв (комп'ютери, принтери тощо, часто називаються «хости») пов'язані між собою лініями зв'язку, найчастіше з використанням спеціального комунікаційного обладнання: комутаторів (switchs), концентраторів (hubs), маршрутизаторів (routers) тощо. Точки підключення ліній зв'язку до кінцевого або комунікаційного обладнання називаються **портами** (для дротових мереж – це роз'єм). Порти кожного пристрою мають номери (зазвичай починаючи з нуля). З поняттям «порт» пов'язане поняття «мережевий інтерфейс» (далі просто «інтерфейс»). Інтерфейс – це сукупність апаратного і програмного забезпечення, яке через порт забезпечує взаємодію обладнання (кінцевого або комутаційного) з мережею з використанням спеціального мережевого протоколу (Ethernet, Fast Ethernet, Poit to Poin Protocol – PPP і ін.). У програмному забезпеченні в позначенні порту, крім його номера, використовується умовне позначення протоколу, який працює через цей порт, наприклад eth0 – 0-й порт, що працює по протоколу Ethernet, fa1 – 1-й порт, який працює по протоколу Fast Ethernet, S2 – 2-й порт, який працює по послідовному (Serial) протоколу. Кожен порт має унікальну 48-бітну фізичну адресу – MAC-адресу (від англ. *Media Access Control* – нагляд за доступом до середовища).

Організація взаємодії комп'ютерів в мережі Інтернет реалізується протоколом IP (Internet Protocol). В даний час основною версією є 4-я версія цього протоколу. Розвивається 6-я версія. Для адресації мереж і мережевих пристроїв в IP-мережі використовуються IP-адреси. В 4-й версії протоколу – це 32-розрядні числа, які найчастіше записуються у вигляді X.X.X.X, де X – однобайтне число від 0 до 255. У записі адреси часто присутня маска, про яку буде сказано в наступних лабораторних роботах.

1.3 Побудова мережі в Cisco Packet Tracer

Покажемо побудову мережі на прикладі простої мережі з двох комп'ютерів і комутатора, з'єднаних між собою кабелем типу Copper Straight-through.

Для виставлення пристрою в робочий простір програми необхідно обрати пристрій з області Device-Type Selection (типи пристроїв) панелі обладнання, а потім з панелі Device-Specific Selection (моделі пристрою) обрати модель пристрою. Після цього потрібно натиснути ліву кнопку миші в полі робочого простору програми (Workspace) або перемістити мишкою обрану модель пристрою з панелі Device-Specific Selection в робочий простір.

Також можна перемістити пристрій прямо з області Device-Type Selection, але при цьому буде обрана модель пристрою за умовчанням.

Вибір пристроїв для нашого прикладу показано на рис. 1.4, 1.5.

Додані вузли ми зв'яжемо з допомогою ліній зв'язків. Для цього необхідно вибрати (клацнути лівою клавішею миші) піктограму «Тип з'єднання» з панелі Network Component Box (рис. 1.2). Назва типу (Connection) з'явиться в центрі області типів з'єднань, а в області Device-Specific Selection ми побачимо всі можливі типи з'єднань між пристроями. Виберемо «мідний прямий» (Copper Straight-through)  , котрий зазвичай використовується для зв'язку комп'ютера з комутатором в технології Ethernet.

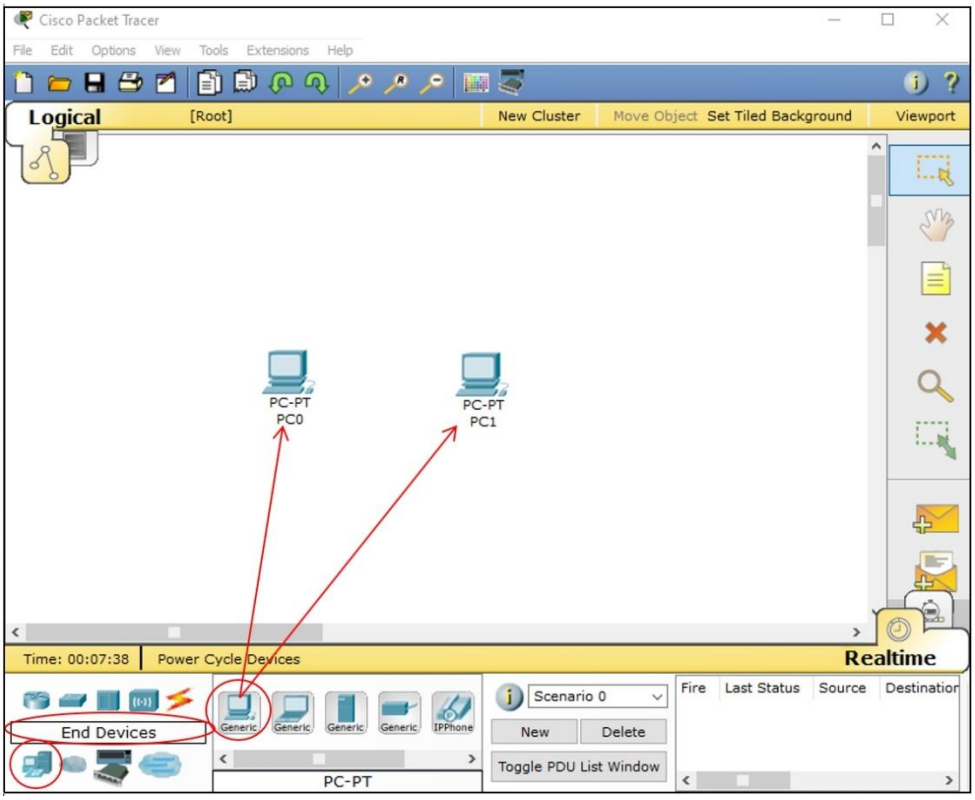


Рисунок 1.4 – Формування на робочому просторі двох моделей комп'ютерів

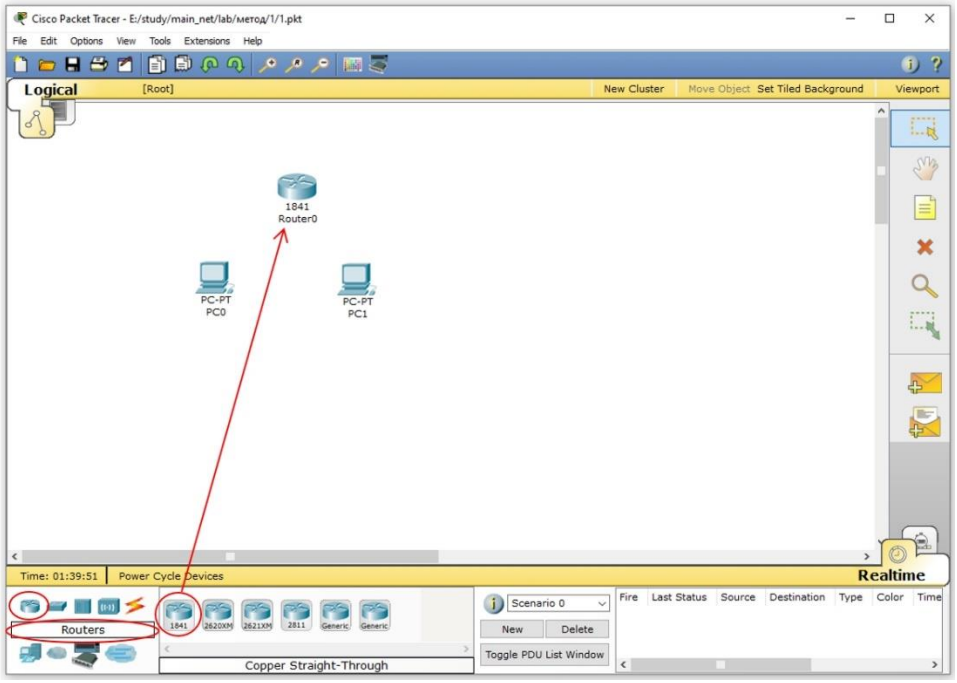


Рисунок 1.5 – Формування на робочому полі моделі комутатора

Після вибору (клацання мишею) вид значка зміниться на  , а покажчик миші (в робочому просторі) зміниться на курсор «connection» (має вигляд роз'єму). Клацнемо на першому пристрої (комутатор) і виберемо з списку інтерфейсів даного пристрою що випав (рис. 1.6) відповідний інтерфейс (наприклад, FastEthernet0/1), до котрого потрібно підключити кабель з'єднання. Далі перемістимо курсор до другого пристрою (PC0). За курсором буде тягнутися лінія зв'язку. Клацнемо на другому пристрої і виконаємо аналогічну операцію вибору інтерфейсу (рис. 1.7). Між пристроями з'явиться кабельне з'єднання (рис. 1.8), а індикатори на кожному кінці покажуть статус з'єднання (зелений колір – порт включений, червоний – вимкнений).

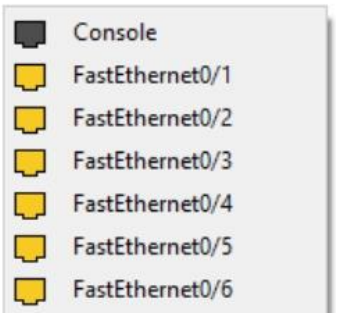


Рисунок 1.6 – Список інтерфейсів комутатора 2950-24

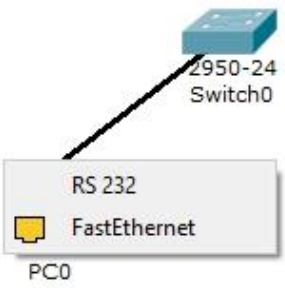


Рисунок 1.7 – Список інтерфейсів робочої станції

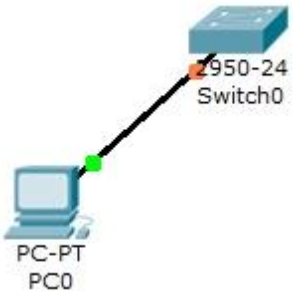


Рисунок 1.8 – Зв'язок комутатора 2950-24 з робочою станцією

Аналогічно з'єднаємо комутатор (вибравши на ньому інтерфейс FastEthernet0/2) з робочою станцією PC1. Загальний вигляд створеної мережі в робочому просторі Cisco Packet Tracer показаний на рис. 1.9.

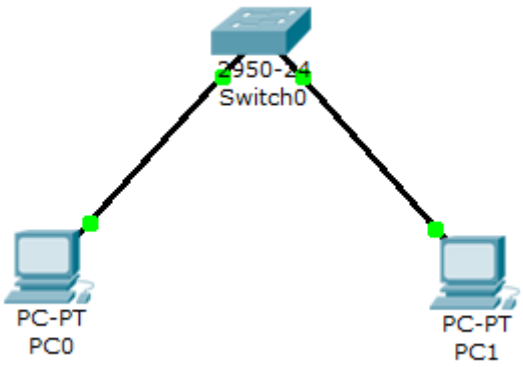


Рисунок 1.9. Загальний вигляд створеної мережі в робочій області Cisco Packet Tracer

Створену схему мережі можна зберегти у вигляді картинки з розширенням *.png, використовуючи пункти меню File -> Print ... -> Print to file...

1.4 Налаштування мережі в Cisco Packet Tracer

Для нашої найпростішої мережі налаштування буде полягати в призначенні IP-адрес для обраних інтерфейсів робочих станцій (у комутатора IP-адреси відсутні) і включенні обраних інтерфейсів (там, де вони вимкнені). Слід врахувати, що фізичні адреси (MAC-адреси) присутні на будь-яких інтерфейсах будь-яких мережевих пристроїв і в моделях пристроїв Cisco Packet Tracer формуються автоматично.

Для налаштування пристрою на робочому просторі потрібно клацнути на ньому лівою клавішею миші. Після цього з'являється вікно конфігурації з декількома закладками. Нас в даній лабораторній роботі буде цікавити лише закладка Config.

Зробимо клацання на комутаторі. З'являється вікно конфігурації комутатора. Вибираємо закладку Config (рис. 1.10). У списку елементів налаштування (в лівій частині вікна) вибираємо FastEthernet0/1. Перевіряємо, що опція Port Status в активному стані (перемикач On відзначений). Аналогічно перевіряємо стан цього перемикача для інтерфейсу FastEthernet0/2.

На рис. 1.11 показано вікно настройки інтерфейсу FastEthernet робочої станції PC0. Тут також потрібно включити перемикач On опції Port Status. У вікні показаний також MAC-адресу порту цього інтерфейсу (заданий автоматично в процесі створення моделі PC0).

Потрібно виконати конфігурацію (налаштування) IP-адреси. В курсі лабораторних робіт ми будемо працювати з версією IPv4, тобто з 32-розрядною IP-адресою. У даній лабораторній роботі ми будемо працювати з IP-адресами (для інтерфейсів робочих станцій) в діапазоні 192.168.0.1 – 192.168.0.254 і

єдиної для всіх адрес маскою – 255.255.255.0 (приклад показаний на рис. 1.12). Дана маска для зазначеного діапазону буде вводитись автоматично після введення IP-адреси і установки курсору в вікно Subnet Mask.

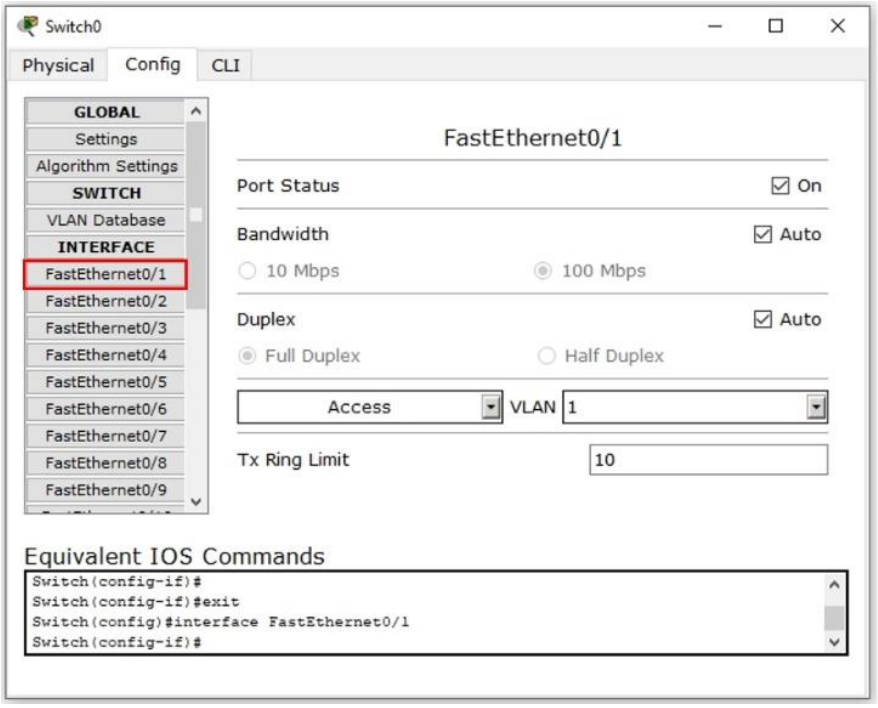


Рисунок 1.10 – Закладка Config вікна настройки комутатора 2950-24. Обрано налаштування інтерфейсу FastEthernet0/1

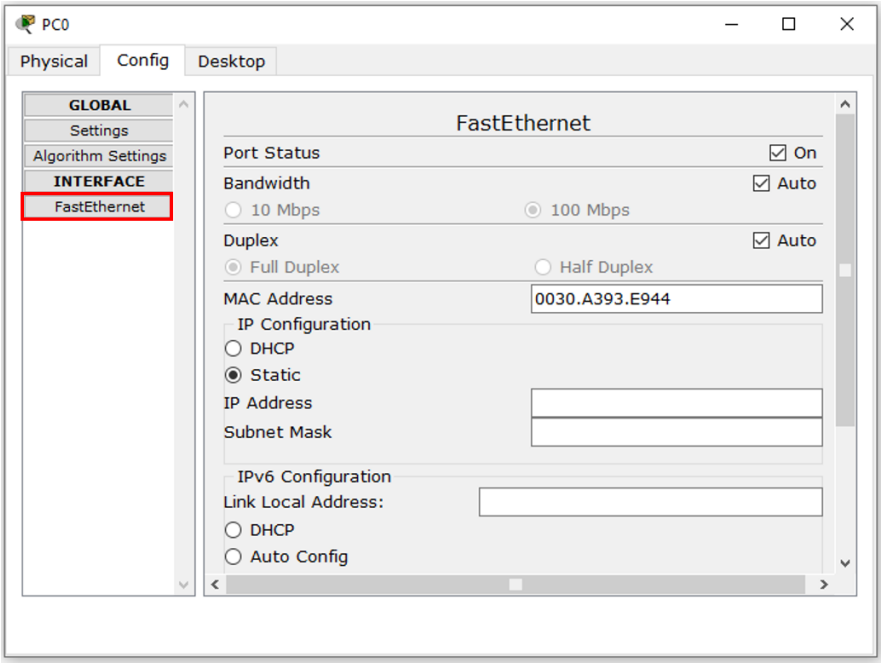


Рисунок 1.11 – Закладка Config вікна настройки робочої станції PC0. Встановлено значення інтерфейсу FastEthernet

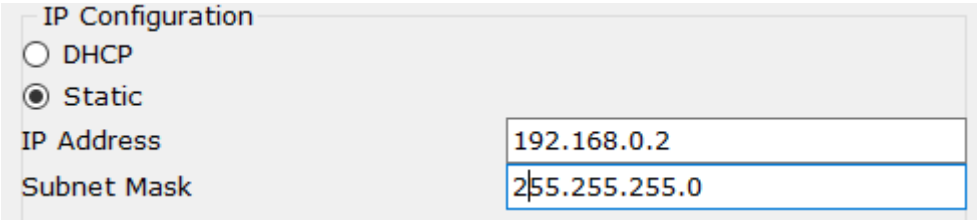


Рисунок 1.12 – Приклад конфігурації IP-адреси на робочій станції PC0.

Аналогічно конфігурується IP-адреса (зрозуміло, інша з заданого діапазону) і на PC1.

Звичайно ж в реальної мережі налаштування IP-адрес відбувається із використанням спеціального програмного забезпечення. В Cisco Packet Tracer також є можливість емуляції роботи з таким програмним забезпеченням.

Після створення мережі її (з усіма параметрами) можна зберегти, вибравши пункт меню File -> Save або File -> Save As ... або іконку Save на панелі Main Tool Bar. Файл збереженої топології має розширення *.pkt.

1.5 Тестування мережі в Cisco Packet Tracer

І в реальній мережі, і в Cisco Packet Tracer основним інструментом тестування мережі є спеціальна програма Ping (формат та список опцій цієї команди наданий в додатку 1). Вона запускається з командного рядка будь-якої мережевої операційної системи (Windows, Linux тощо). Ця програма посилає спеціальне повідомлення за вказаною в параметрах виклику програми Ping IP-адресою. Якщо вузол з такою IP-адресою в мережі є і він активний, то, отримавши такий запит, він зобов'язаний послати відповідь пристрою, що вислав цей запит. Протокол такого обміну передбачає, що IP-адреса пристрою, який вислав запит, знаходиться в самому запиті, точніше в заголовку IP-пакета, куди запит поміщений. За наявності відповіді і часу його затримки можна судити про наявність в мережі пристрою з заданою IP-адресою, його станом (активний!), пропускної спроможності каналів мережі (за часом затримки відповіді), надійності роботи мережі (по співвідношенню кількості запитів і відповідей).

Cisco Packet Tracer дає нам можливість емулювати роботу з командним рядком на кінцевих пристроях (комп'ютерах), а також емулювати роботу в середовищі спеціальної операційної системи IOS (Internetwork Operating System) компанії Cisco, встановленої у всіх маршрутизаторах і комутаторах цієї компанії.

У даній лабораторній роботі розглядається робота програми (команди) Ping, яка запускається з командного рядка комп'ютера.

Протестуємо зв'язок з командного рядка робочої станції PC1. У вікні конфігурації PC1 відкриємо закладку Desktop (робочий стіл), див. рис. 1.13. Клацнемо на іконці Command Prompt (негайна команда) і потрапимо в емулятор командного рядка. У рядку емулятора введемо команду ping 192.168.0.2 (тут

192.168.02 – IP-адреса робочої станції PC0, зв'язок з якою ми перевіряємо). Якщо всі налаштування зроблені правильно прийде відповідь (рис. 1.14).

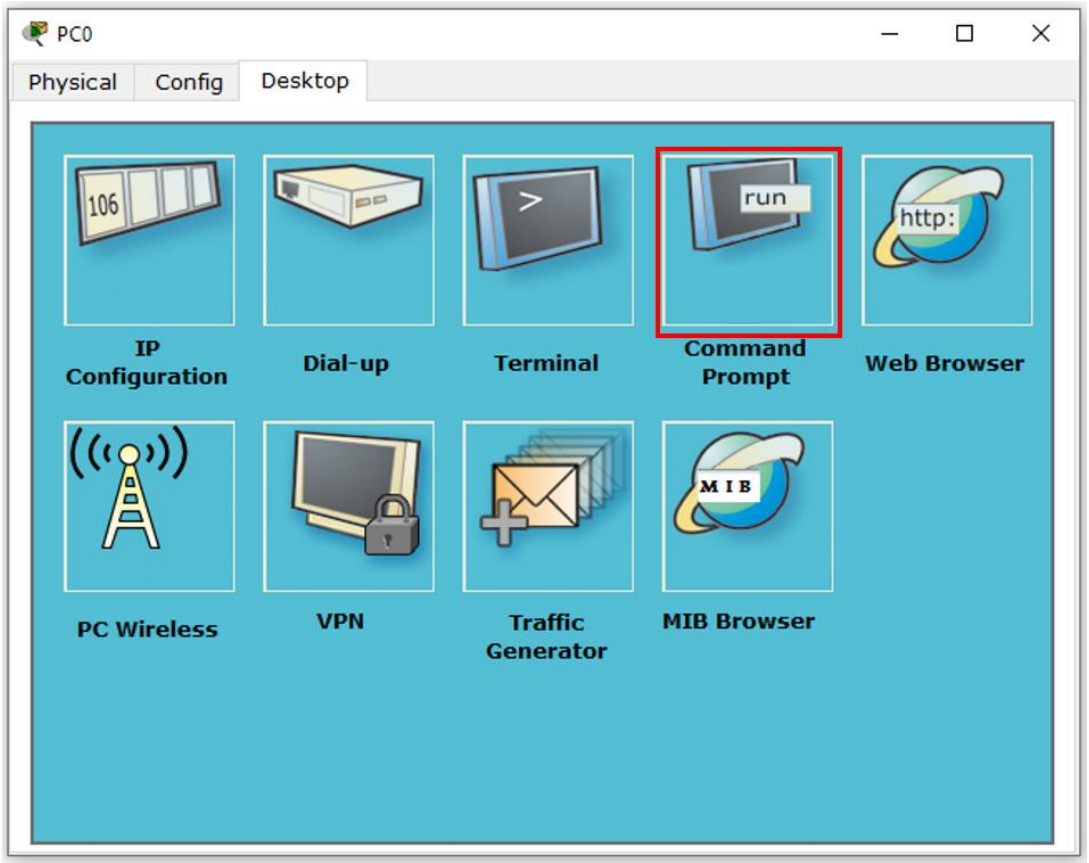


Рисунок 1.13 – Закладка Desktop вікна настройки PC0

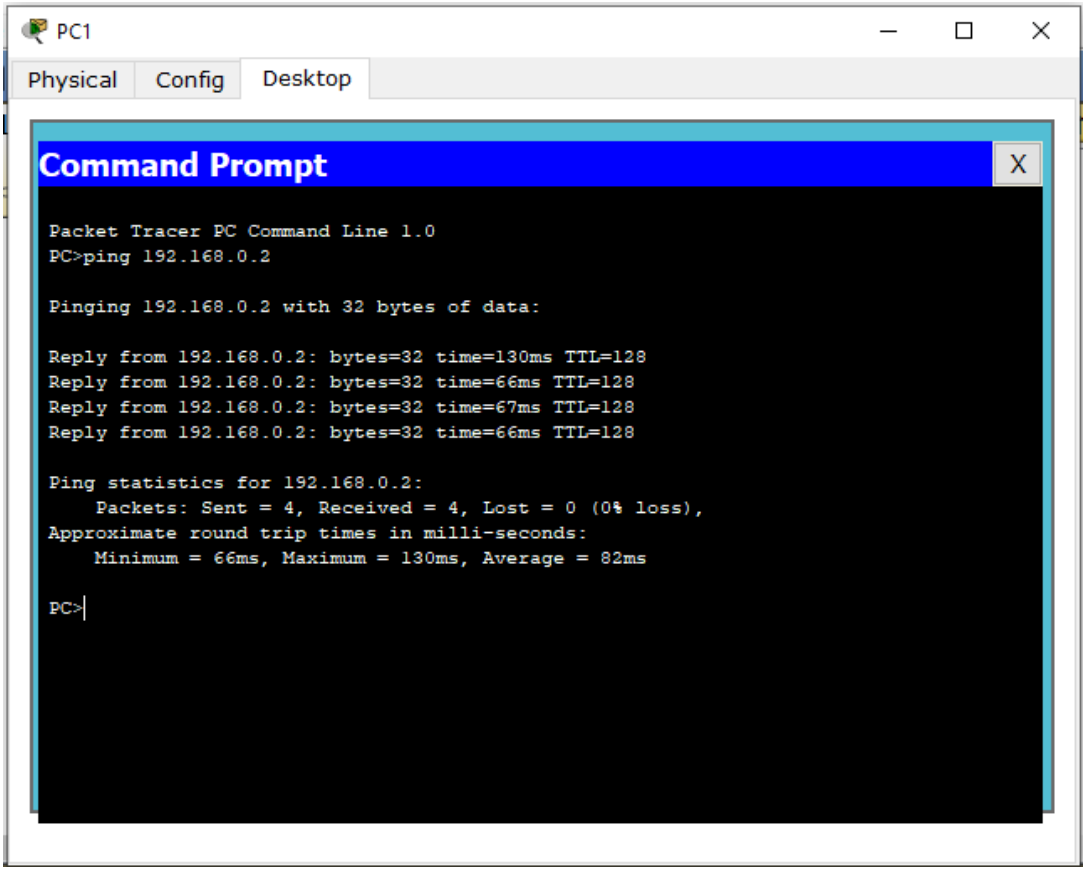


Рисунок 1.14 – Результат виконання команди ping

З отриманих повідомлень команди ping ми бачимо:

- пінгування відбувалося 32-байтними повідомленнями;
- було послано 4 повідомлення, отримано 4 відповіді, втрачених пакетів – 0 (0% втрат);
- мінімальна затримка відповіді – 66 мс, максимальна – 130 мс, середнє значення затримки – 82 мс.

1.6 Режим симуляції Cisco Packet Tracer

Cisco Packet Tracer містить режим симуляції роботи мережі, в якому можна імітувати мережеві події. Перейти в режим симуляції можна комбінацією клавіш **Shift+S** або, клацнувши мишею на іконці симуляції в правому нижньому кутку робочого простору (рис. 1.15).

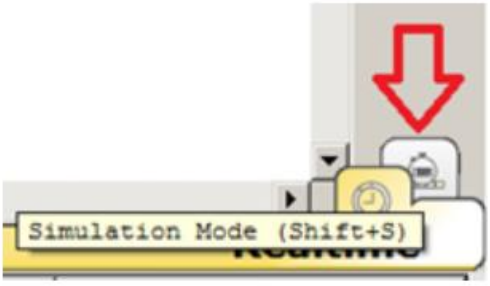


Рисунок 1.15 – Іконка включення режиму симуляції

Після включення режиму симуляції з'являється панель режиму симуляції. У нижній частині цієї панелі показані мережеві протоколи, роботу яких можна переглядати в цьому режимі (рис. 1.16).

Рисунок 1.16 – Область вибору мережевих протоколів на панелі режиму симуляції

У нашій роботі ми будемо переглядати роботу програми Ping, яка використовує протокол ICMP (Internet Control Message Protocol) – мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки та інші виключні ситуації, що виникли при передачі даних. Для налаштування режиму перегляду роботи виключно протоколу ICMP натисніть на кнопку Edit Filters (редагувати фільтри) і виключіть всі мережеві протоколи, крім ICMP (рис. 1.17).

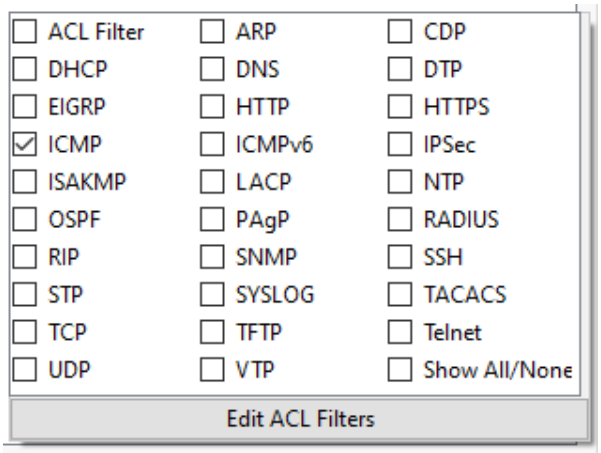


Рисунок 1.17 – Вікно редактора фільтра протоколів

Управління симуляцією виконується в області Play Control панелі симуляції (рис. 1.18).

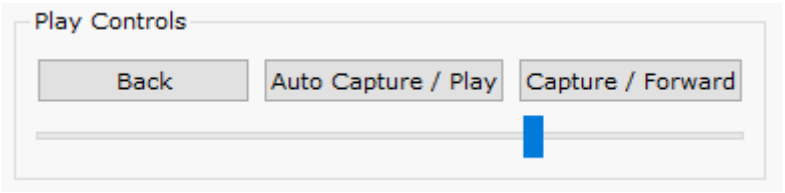


Рисунок 1.18 – Інструменти управління симуляцією

Запустити покроково просування пакета в мережі можна, натиснувши на кнопку Capture/Forward (Вперед).

Кнопка Back (Назад) повертає симуляцію на крок назад.

Якщо натиснути на кнопку Auto Capture/Play (відтворення), то ми побачимо весь цикл проходження пакета по мережі.

Під кнопками управління симуляцією розташований регулятор швидкості симуляції в режимі відтворення

У вікні Event List (Список подій) панелі симуляції ми можемо бачити кроки результату симуляції.

У створеній (рис. 1.9) і налаштованій мережі виконаємо пінгування комп'ютера 192.168.0.2 (PC1) з комп'ютера 192.168.0.1 (PC0) в режимі симуляції.

1) Ввійдемо в режим симуляції.

2) Ввійдемо в режим командного рядка робочої станції PC0 і запустимо команду ping 192.168.0.2

У робочому вікні біля зображення PC0 утворився пакет (конвертик), який чекає початку руху його по мережі, а в вікні списку подій постало повідомлення про перший крок виконання програми (рис. 1.19).

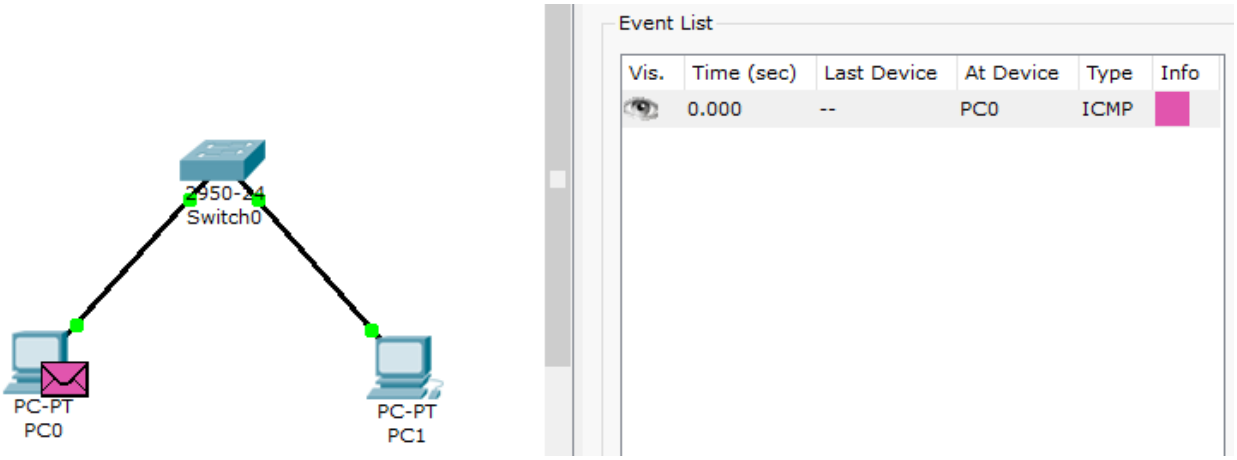


Рисунок 1.19 – Перший крок виконання програми Ping в режимі симуляції

Виконуючи покрокове пінгування, ми побачимо, що тільки на 5 кроці конвертик повернеться до PC0 з відповідним повідомленням і у вікні Desctop PC0 з'явиться рядок про цю подію. Таким чином (покроково або запустивши режим відтворення) можна відстежити всі кроки роботи програми Ping.

1.7 Індивідуальне завдання

1) За допомогою програмного симулятора Cisco Packet Tracer побудувати мережу з топологією Зірка на базі концентратора (рис. 1.20).

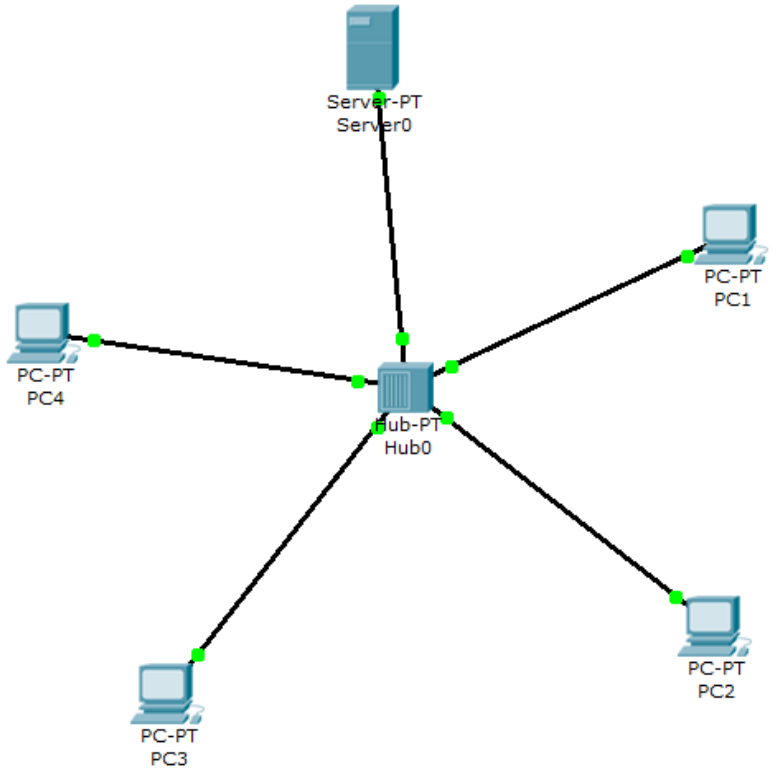


Рисунок 1.20 – Мережа з топологією Зірка на базі концентратора в робочому вікні програми Cisco Packet Tracer

2) Призначити вузлам мережі (кінцеве обладнання) IP-адреси і маску (табл. 1.1) відповідно до номера варіанта «x» (номер видає викладач):

Таблиця 1.1

IP-адреси і маски кінцеве обладнання відповідно до номера варіанта «x»

Кінцеве обладнання	IP-адреса	Маска
Server 0	192.168.x.10	255.255.255.0
PC1	192.168.x.1	255.255.255.0
PC2	192.168.x.2	255.255.255.0
PC3	192.168.x.3	255.255.255.0
PC4	192.168.x.4	255.255.255.0

Наприклад, для варіанта x = 37 IP-адреса PC1 буде 192.168.37.1

3) Використовуючи інструмент створення заміток Place Note (клавіша N), записати біля кожного пристрою його IP-адресу, а вгорі робочої області створити заголовок проекту «Дослідження топології Зірка» (рис. 1.21).

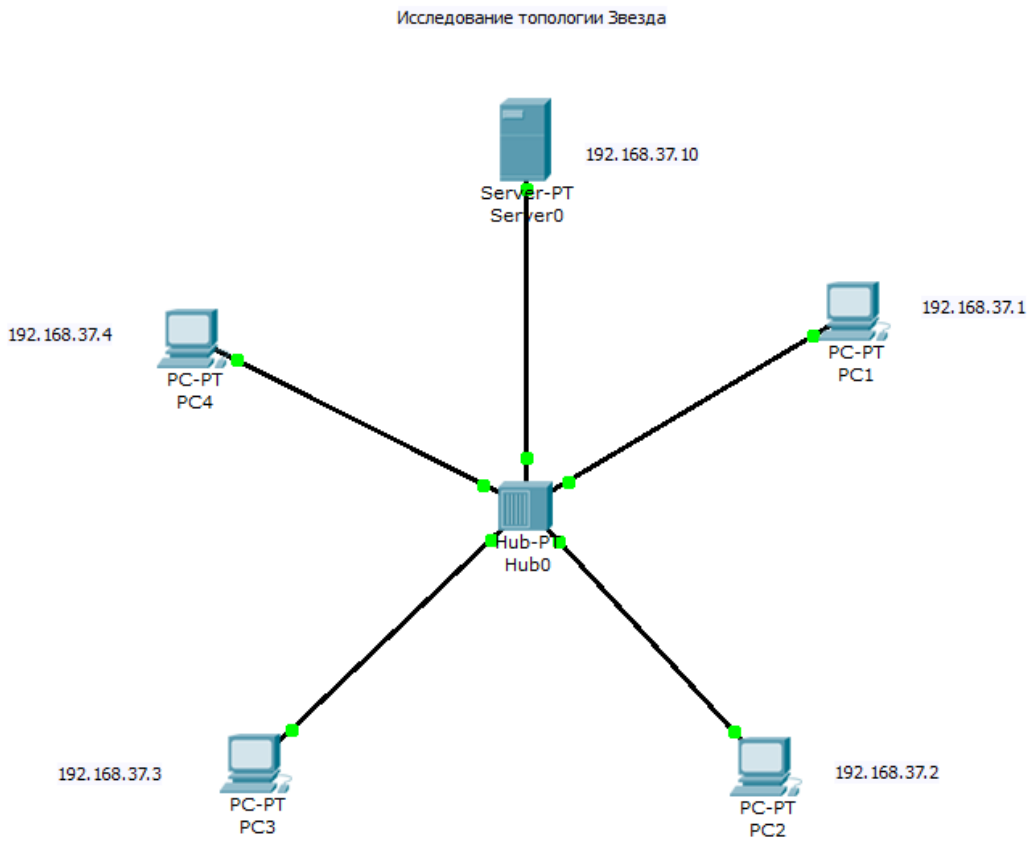


Рисунок 1.21 – Формування написів на рисунку мережі в робочій області

4) Зберегти створену мережу в файл у Вашому особистому каталозі.

5) Перейти в режим симуляції і виконати пінгування (в покроковому режимі і в режимі відтворення) будь-якої робочої станції з сервера. Поясніть процес пінгування. Врахуйте, що «пташка» на пакету, що прийшов до кінцевого пристрою, означає те, що пристрій опрацював цей пакет, а хрестик на пакеті означає, що вузол відкинув (знищив без обробки) пакет, що прийшов.

6) Замініть центральний вузол мережі – концентратор – іншим вузлом – комутатором. Збережіть цей варіант мережі.

7) Повторити дію п.5) при роботі в мережі з комутатором. Поясніть відміну процесу пінгування в мережі з комутатором від процесу пінгування в мережі з концентратором.

1.8 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з загальними принципами побудови комп'ютерних мереж (п.1.2, матеріали в системі «Лідер»).

2) Запустіть на комп'ютері програму PacketTracer5.

3) Ознайомтеся з інтерфейсом і загальними принципами побудови і моделювання мереж в програмі Cisco Packet Tracer, виконуючи дії, зазначені в пп. 1.1, 1.3-1.6.

4) Виконайте індивідуальне завдання п.1.7 за варіантом, виданим викладачем.

5) Оформіть звіт по роботі.

6) Пред'явіть звіт викладачеві і дайте відповідь на контрольні питання.

1.9 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Звіт повинен містити:

- назву роботи;
- мету роботи;
- загальний вигляд інтерфейсу (головного вікна Cisco Packet Tracer з позначками його основних елементів);
- скріншот побудованої по заданому варіанту мережі з топологією «Зірка» з центральним вузлом комутатором;
- скріншот побудованої по заданому варіанту мережі з топологією «Зірка» з центральним вузлом концентратором;
- скріншот результатів пінгування однією з робочих станцій з сервера у вікні Desktop сервера в мережі з топологією «Зірка» з центральним вузлом концентратором;
- скріншот результатів пінгування однією з робочих станцій з сервера у вікні Desktop сервера в мережі з топологією «Зірка» з центральним вузлом комутатором;
- скріншот списку подій результату пінгування в режимі симуляції в мережі з топологією «Зірка» з центральним вузлом комутатором;
- скріншот списку подій результату пінгування в режимі симуляції в мережі з топологією «Зірка» з центральним вузлом концентратором.

1.10 Контрольні питання

1. Які типи мережевих пристроїв і з'єднань можна використовувати в Cisco Packet Tracer?
2. Яким способом можна перейти до командного рядка пристрою.
3. Як додати в топологію мережі і налаштувати новий пристрій в програмі Cisco Packet Tracer?
4. Як зберегти сконфігуровану мережу в файлі? Яке розширення у цього файлу?
5. Чим відрізняється режим симуляції від режиму реального часу?
6. Яка команда може бути використана для тестування мережі? Папараметри цієї команди?
7. Поясніть результат пінгування вузла мережі.
8. Чим відрізняється пінгування в мережі з топологією «Зірка» з концентратором в центрі від цієї ж операцією в мережі з комутатором в центрі?

Лабораторна робота №2

ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ARP ЗАСОБАМИ ПРОГРАМИ CISCO PACKET TRACER

Мета роботи. Ознайомитись з роботою протоколу ARP. Дослідити алгоритм роботи цього протоколу у мережі з топологією Зірка засобами програми Cisco Packet Tracer.

2.1 Загальні відомості про протокол ARP

У мережах TCP/IP робота організована на кількох стандартних рівнях, які визначені стандартною моделлю взаємодії відкритих систем (Open System Interconnection, OSI). Ми в даній роботі розглядаємо рівні 1 – фізичний (канал зв'язку), 2 – канальний (на цьому рівні працює протокол Ethernet) і 3 – мережевої взаємодії (протокол IP). Саме дані протоколу Ethernet (кадр) передаються за фізичним каналом зв'язку і надходять у порт потрібного хоста за заданою MAC-адресою (локальною, фізичною адресою). Протокол IP містить свої дані разом із заголовком (пакет) у кадр протоколу Ethernet (рис. 2.1).

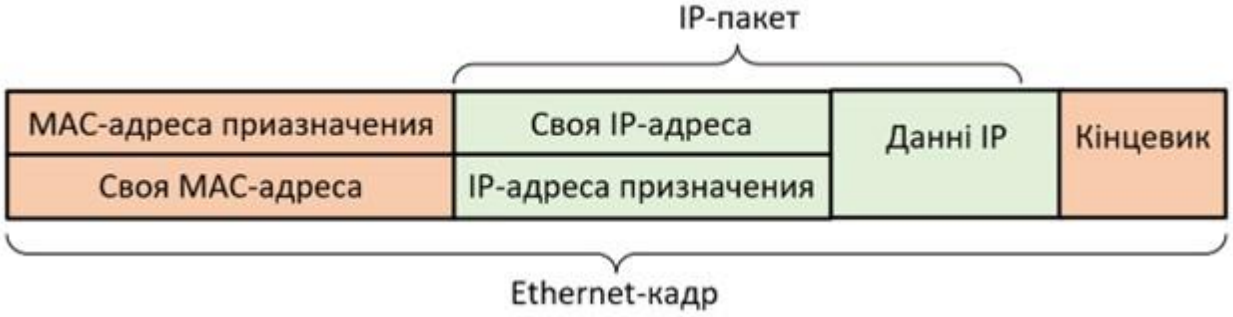


Рисунок 2.1 – Спрощена схема розміщення IP-пакету в кадрі Ethernet

Зазвичай, в результаті конфігурування мережі кожен інтерфейс хоста «знає» свою IP-адресу і свою локальну адресу, а також IP-адреси хостів своєї мережі. Проте фізичні адреси вузлів своєї мережі хосту зазвичай невідомі. Тим часом, для передачі будь-яких даних мережевий вузол повинен знати фізичну адресу одержувача для передачі IP-пакета.

Тим часом, жодної функціональної залежності між локальною (фізичною) адресою та її IP-адресою не існує, отже, єдиний спосіб встановлення відповідності – ведення таблиць. Для визначення локальної адреси за IP-адресою використовується протокол визначення адрес (Address Resolution Protocol, ARP).

Протокол ARP підтримує на кожному інтерфейсі мережного адаптера окрему ARP-таблицю (рис. 2.2), в якій в ході функціонування мережі накопичується інформація про відповідність між IP-адресами та MAC-адресами інших інтерфейсів даної мережі.

IP-адреса	MAC-адреса	Тип запису
195.36.210.12	12-43-F4-AB-5C-01	Динамічний/статичний

Рисунок 2.2 – Формат ARP-таблиці

Спочатку при включенні комп'ютера або маршрутизатора в мережу його ARP-таблиця порожня. Заповнення цієї таблиці може бути виконане засобами протоколу ARP або вручну адміністратором мережі.

Для роботи адміністратора з ARP-таблицею використовується програма (команда) arp. У цій лабораторній роботі розглядаються такі можливості цієї команди:

arp -a – перегляд таблиці;
arp -d – очищення таблиці.

Розглянемо роботу протоколу ARP у локальних мережах з широкомовленням, до яких належать мережі Ethernet. У таких мережах можна відправити кадр до всіх вузлів мережі, що знаходяться в одному логічному сегменті 3 рівня (він обмежений маршрутизатором).

Якщо вузлу необхідно відправити IP-пакет за будь-якою IP-адресою своєї IP-мережі (до іншої IP-мережі хост відправити пакет без послуг маршрутизатора не може), а в ARP-таблиці відсутній запис для цієї IP-адреси, то вузол формує широкомовне повідомлення – ARP-запит, вкладаючи його у кадр канального рівня (наприклад, у кадр Ethernet), у якому запитує фізичну адресу вузла призначення (рис. 2.3 п.1). Всі вузли мережі приймають цей запит і порівнюють вказану там IP-адресу з власною. У разі їх збігу вузол формує ARP-відповідь, в якому вказує свою IP-адресу і свою локальну адресу і відправляє його вже направлено, так як в ARP-запиті відправник вказує свою локальну адресу (рис. 2.3 п.2).

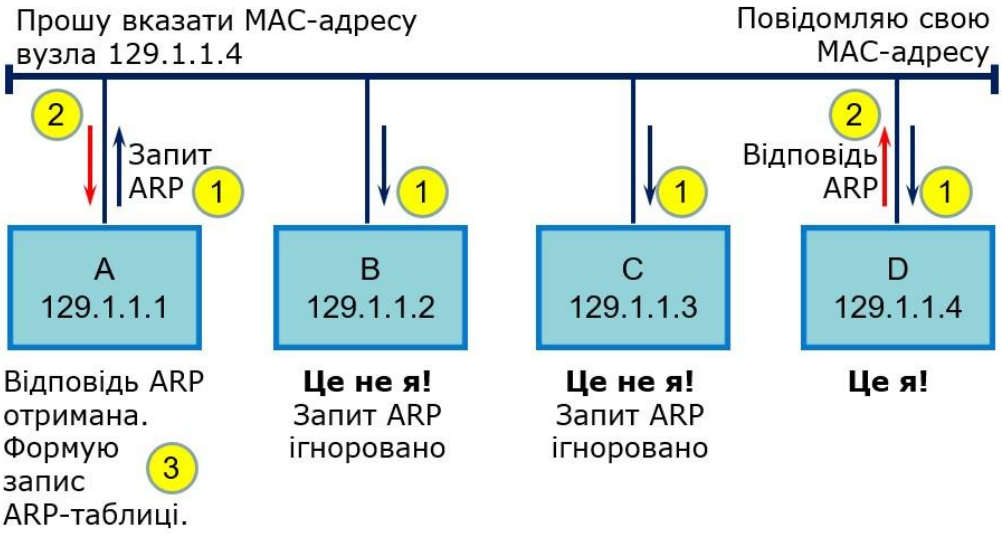


Рисунок 2.3 – Послідовність виконання ARP-запиту

Вузол, що отримав ARP-відповідь, записує в ARP-таблицю знайдену відповідність між IP-адресою і MAC-адресою вузла призначення (рис. 2.3 п.3) і в подальшому, протягом певного часу, не запитує його при повторних зверненнях до цього вузла. IP-пакет, який переносить дані для цільової машини, поміщається у кадр зі знайденою MAC-адресою і прямує до вузла призначення.

ARP-запити та відповіді використовують один і той самий формат пакета. На рис. 2.4, 2.5 показані формати (у полі даних кадру) протоколу ARP для передачі по мережі Ethernet.

Поле	Значення
«Тип мережі» канального рівня	1 (для Ethernet)
«Тип протокола» мережевого рівня	2048 (=0800_{16} для IP)
«Довжина локальної адреси»	6 (для Ethernet)
«Довжина мережевої адреси»	4 (для IP)
«Операція»	1 (для ARP-запиту)
«Локальна адреса відправника»	Апаратна адреса хоста, що відправив ARP-запит
«Мережева адреса відправника»	IP-адреса хоста, що відправив ARP-запит
«Локальна адреса отримувача»	000000000000
«Мережева адреса отримувача»	IP-адреса хоста отримувача

Рисунок 2.4 – Формат ARP-запиту передачі Ethernet

Поле	Значення
«Тип мережі» канального рівня	1 (для Ethernet)
«Тип протокола» мережевого рівня	2048 (=0800_{16} для IP)
«Довжина локальної адреси»	6 (для Ethernet)
«Довжина мережевої адреси»	4 (для IP)
«Операція»	2 (для ARP-відповіді)
«Локальна адреса відправника»	Апаратна адреса хоста, що відповідає (те, что було запитано)
«Мережева адреса відправника»	IP-адреса хоста, що відповідає
«Локальна адреса отримувача»	Аппаратна адреса хоста, що відправив ARP-запит
«Мережева адреса отримувача»	IP-адреса хоста, що відправив ARP-запит

Рисунок 2.5 – Формат ARP-відповіді для передачі через мережу Ethernet

2.2 Індивідуальне завдання

1) Запустіть програму Cisco Pacet Tracer.

2) Завантажте створену раніше мережу конфігурації Зірка з концентратором (хабом) як центральний вузол (рис. 1.22).

3) Під IP-адресами хостів запишіть їх MAC-адреси.

3) Зайдіть в режим командного рядка (Command prompt) будь-якого комп'ютера створеної мережі (клацніть на комп'ютері і в вікні, що з'явилось, виберіть вкладку Desctop, на якій вже виберіть режим Command prompt).

4) Очистіть ARP-таблицю командою arp -d.

5) Перевірте, що ARP-таблиця порожня, виконавши команду arp -a.

6) Пропінгуйте будь-який комп'ютер даної мережі, перевірте наявність зв'язку з цим комп'ютером за результатами пінгування.

7) Знову перегляньте ARP-таблицю командою arp -a. В ARP-таблиці з'явився запис. Проаналізуйте його.

8) Знову очистіть таблицю ARP.

9) Увімкніть режим симуляції Cisco Packet Tracer.

10) У списку фільтрів увімкніть лише протокол ARP.

11) Запустіть пінгування будь-якого комп'ютера мережі. Біля того комп'ютера, з якого проводиться пінгування, повинен з'явитися конвертик, а у вікні списку подій області симуляція рядок (див. рис. 1.20 л.р.1). Проаналізуйте його, а потім клацніть на кольоровому квадратику поля Info цього рядка. З'явиться вікно (рис.2.6), у якому буде дано докладна інформація про цей крок (у цьому прикладі пінгування робочої станції CT1 виробляється із сервера Server0 – приклад в лабораторній роботі 1, рис. 1.22).

Розглянемо це вікно докладніше.

Заголовок вікна "PDU information at Device: Server0" говорить про те, що в даному вікні надана інформація про дані, які використовуються (формуються, приймаються, передаються). Тут PDU (Protocol Data Unit) – узагальнена назва фрагмента даних на різних рівнях моделі OSI.

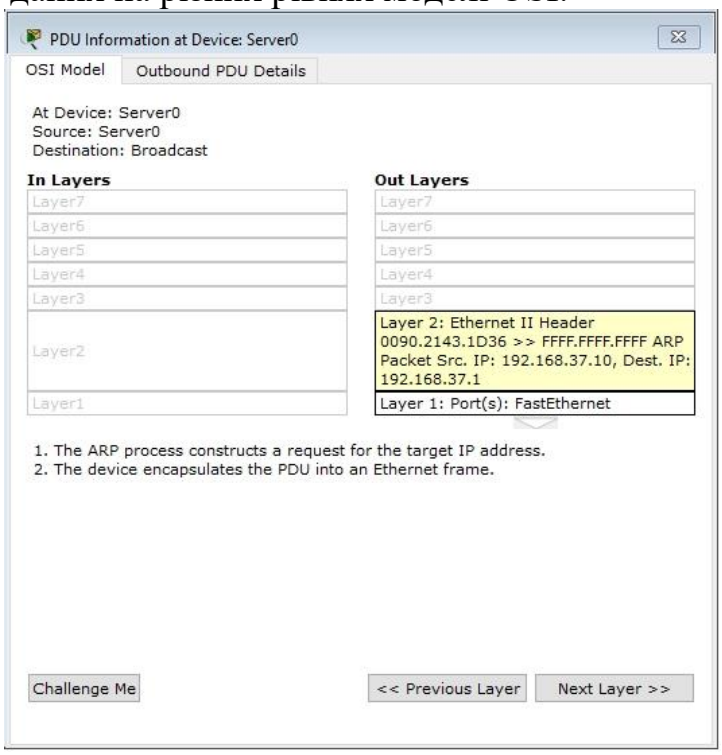


Рисунок 2.6 – Інформація про перший крок роботи протоколу ARP

У вікні дві закладки. Перша з них – OSI model (модель OSI, про яку ми вже говорили). На цій закладці ми бачимо два списки: In Layers та Out Layers. У кожному 7 полів від Layer 7 до Layer 1. Це 7 стандартних рівнів OSI для даних, які знаходяться в конверту, що прийшов (In Layer) і що відправлений (Out Layers).

У нашому випадку протокол ARP підготував до надсилання повідомлення на другому (канальному) рівні. Це Ethrnet-кадр, який з порту з MAC-адресою 0090.2143.1D36 (порт сервера) спрямований на широкомовну адресу (ознака широкомовної адреси – 1 у всіх бітах адреси). В якості поля даних кадру – ARP-повідомлення в якому в полі IP-адреси відправника (Src) – 192.168.37.10 – IP-адреса сервера, в якості IP-адреси одержувача (Dest) – 192.168.37.1 – IP-адреса робочої станції, яку пінгуємо.

Більш детальну інформацію про вміст кадру можна побачити на закладці «Outbound PDU Details» (рис. 2.7).

Тут докладно показано зміст кадру Ethernet. У полі даних цього кадру – повідомлення ARP, винесене окремо. Зіставте це повідомлення з форматом, наведеним на рис. 2.4.

12) Виконайте всі кроки пінгування. Проаналізуйте кожен крок, порівняйте з описом послідовності виконання ARP-запиту (рис.2.3). Подивіться зміст конвертика, який прийшов до джерела пінгування на останньому кроці.

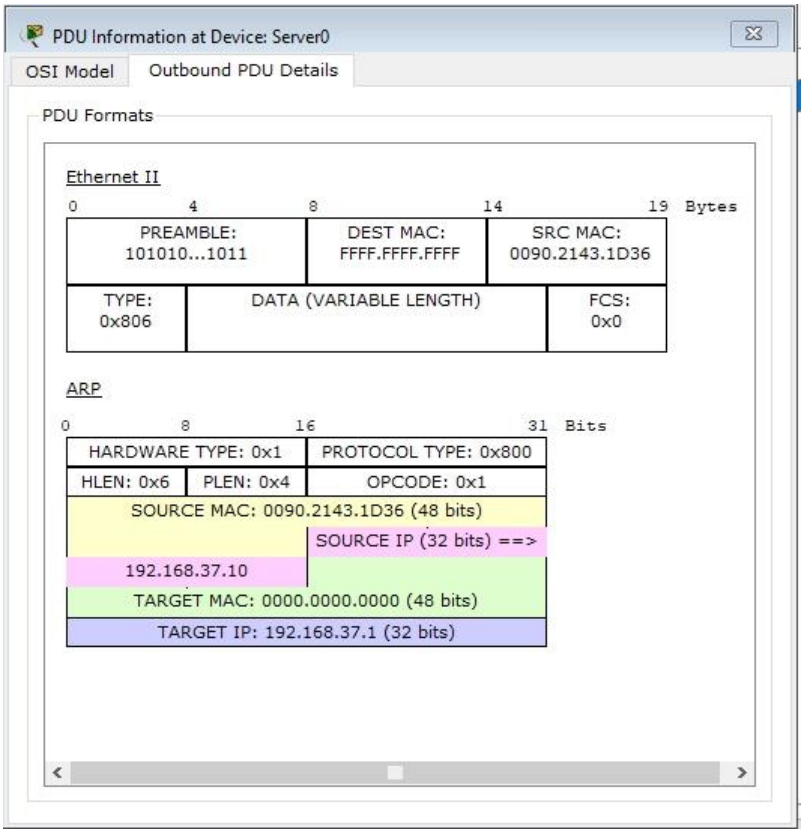


Рисунок 2.7 – Детальна інформація про вміст кадру в закладці Outbound PDU Details інформаційного вікна списку подій

2.3 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з загальними відомостями про протокол ARP (п. 2.1, матеріали системи «Лідер», рекомендована література).

2) Виконайте індивідуальне завдання п.2.2 за варіантом, виданим викладачем.

3) Оформіть звіт про роботу.

4) Подайте звіт викладачеві і дайте відповіді на контрольні питання.

2.4 Зміст звіту

Звіт складається в електронному форматі та роздруковується. Звіт повинен містити:

– назву роботи;

– мету роботи;

– номер Вашого варіанту;

– скріншот заданого варіанту мережі з топологією Зірка з центральним вузлом концентратором з підписаними IP- та MAC-адресами. Виділіть комп'ютер, з якого виконується пінгування (A) і комп'ютер, що пінгується (B);

– ARP-таблиця комп'ютера A після виконання пінгування;

– скріншот вікна в закладці OSI Model інформаційного вікна списку подій режиму симуляції з інформацією про перший крок роботи протоколу ARP (або фрагмента цього вікна з інформацією про кадр).

– скріншот вікна в закладці Outbound PDU Details інформаційного вікна списку подій режиму симуляції з детальною інформацією про вміст кадру першого кроку пінгування;

– скріншот вікна в закладці OSI Model інформаційного вікна списку подій режиму симуляцій з інформацією про останній крок роботи протоколу ARP (або фрагмента цього вікна з інформацією про кадр);

– скріншот вікна (або фрагмента вікна) в закладці Outbound PDU Details інформаційного вікна списку подій режиму симуляції з детальною інформацією про вміст кадру останнього кроку пінгування.

2.5 Контрольні питання

1. Призначення протоколу ARP?

2. Які поля є в ARP-таблиці?

3. Якою командою (і з якими параметрами) можна переглянути вміст ARP-таблиці?

4. Якою командою (і з якими параметрами) можна очистити вміст ARP-таблиці?

5. Чому у Вашому експерименті при виконанні команди Ping починав працювати протокол ARP?

6. Який протокол переносить повідомлення ARP?

7. Що таке PDU?

8. Що таке «широкомовне повідомлення»?

9. Послідовність роботи ARP-протоколу?

10. Зіставте вміст ARP-запиту та ARP-відповіді в скріншотах вмісту кадрів і в рис. 2.4, 2.5.

Лабораторна робота №3

Інсталяція, налаштування та експерименти з віртуальною машиною Ubuntu

Мета. Ознайомитись з принципами роботи та використання віртуальних машин. Створити віртуальну комп'ютерну мережу із двох віртуальних машин. Ознайомитись із роботою з терміналом віртуальної машини. Налаштувати IP-адресацію машин цієї мережі, провести експерименти по прослуховуванню налаштованої мережі.

3.1 Основні відомості щодо віртуальних машин

Для можливості індивідуального вивчення мережевих технологій можливе використання механізму віртуалізації. При цьому на одному фізичному комп'ютері встановлюється кілька віртуальних машин (ВМ), кожна зі своєю операційною системою (ОС), своїм віртуальним обладнанням. ВМ можуть працювати одночасно і паралельно. Кожна ВМ має власні віртуальні засоби комунікації – мережеві карти із відповідними портами, мережеві адреси тощо, які підтримуються ОС ВМ. Оскільки всі ВМ працюють під управлінням єдиної комп'ютерної програми (гіпервизора), то можливо забезпечити мережеву взаємодію між ВМ, встановленими на одному фізичному комп'ютері, тобто створити на одному комп'ютері віртуальну мережу.

В даному циклі лабораторних робіт в якості гіпервизора буде використовуватися комп'ютерна програма VMware Workstation v. 16.1, яка працює на основі спеціальних функцій сучасних 64-розрядних ЦП x86. В якості ОС, встановленої на ВМ, буде використовуватися дистрибутив Ubuntu 14.04.

3.2 Робота в ОС Ubuntu

ОС Ubuntu – це один з найбільш розповсюджених дистрибутивів Linux. В циклі лабораторних робіт з комп'ютерних мереж будуть використовуватись лише спеціальні мережеві програми, які вже інтегровані в цю ОС та використовуються як команди з набором параметрів. Ці команди будуть надаватися поступово по ходу виконання лабораторних робіт.

Запис результатів виконання команди може бути виведено у текстовий файл за наступним синтаксисом:

```
Команда_ з_параметрами > ім'я_файлу
```

За замовчанням в програмі VMware Workstations файли записуються в папку «Home» сховища віртуальної машини.

3.3 Послідовність виконання роботи

3.3.1 Інсталяція віртуальних машин

1) Завантажте дистрибутив програми «VMware Workstation» та образ дистрибутиву Linux (всі подальші дії будуть описані для дистрибутиву VMwareWorkstation v 16.1 та Ubuntu 14.04). Всі необхідні файли для створення ВМ знаходяться в розділі «лабораторні роботи» курсу «Комп'ютерні мережі» системи «Лідер».

2) Встановіть програму «VMware Workstation». Запустіть її (рис. 3.1).

3) Створіть віртуальну машину (натискаємо «Создать новую виртуальную машину»).

4) Виберіть тип конфігурації «Обычный» (рис. 3.2).

5) Виберіть перемикач «Файл образа установки (iso)» та вкажіть шлях до дистрибутиву Ubuntu, який будете інсталювати (рис.3.3).

6) Налаштуйте персоналізацію (рис.3.4). Для цього задайте назву ОС, ім’я користувача та пароль (всі ці данні можуть бути однакові для декількох віртуальних машин). **Обов’язково запам’ятайте пароль, він буде використовуватися для входу в систему!**

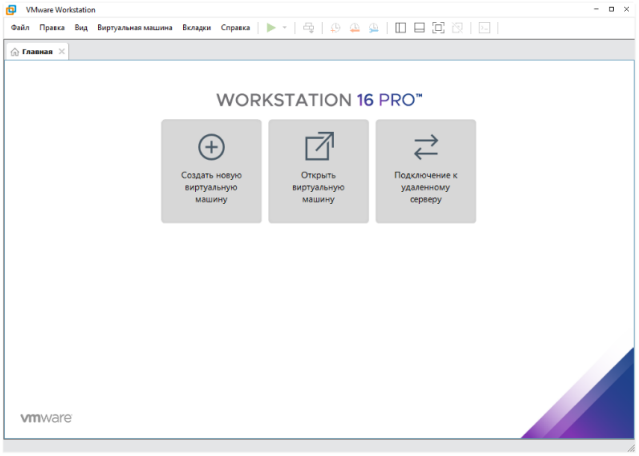


Рисунок 3.1 – Головне вікно програми VMware Workstation

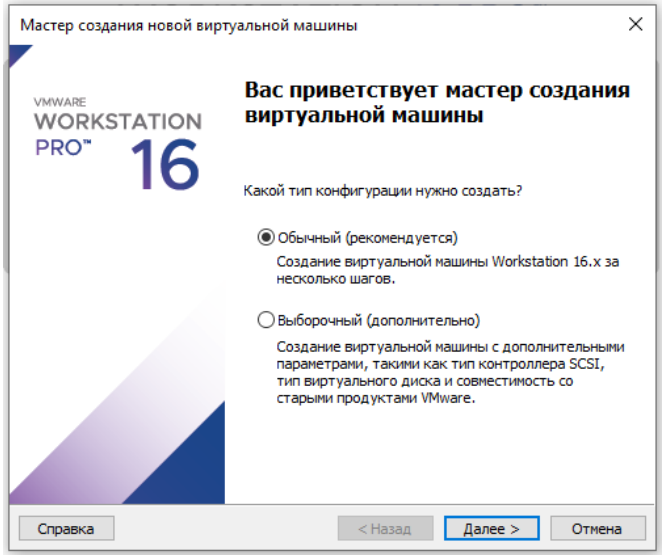


Рисунок 3.2 – Головне вікно майстра побудови віртуальної машини

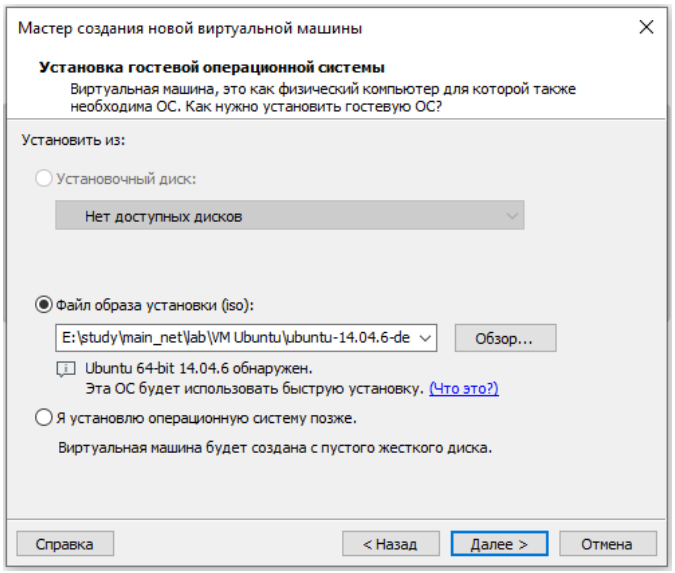


Рисунок 3.3 – Вибір файлу дистрибутиву ОС, яка буде встановлена на віртуальну машину

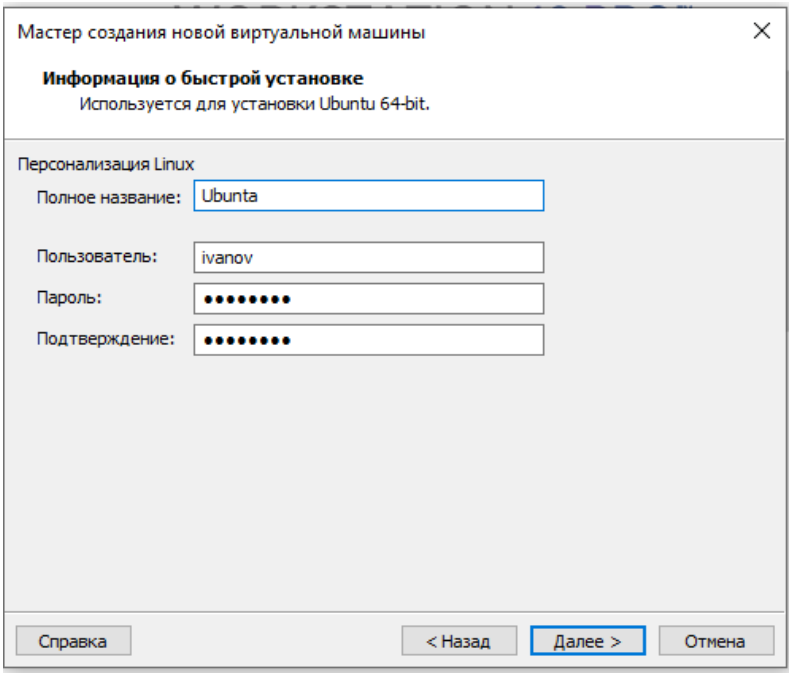


Рисунок 3.4 – вікно персоналізації

7) Вкажіть ім’я віртуальної машини та її місце зберігання на диску (рис. 3.5). Розташування ВМ повинно бути за замовчуванням (тобто, цю стрічку не треба змінювати), а ім’я користувача рекомендується обирати за правилом: «VM_<прізвище студента>_<номер машини>». Наприклад: VM_Ivanov_1.

Запом’ятайте (запишіть!) розташування Вашої віртуальної машини (у вікні «Розташування»).

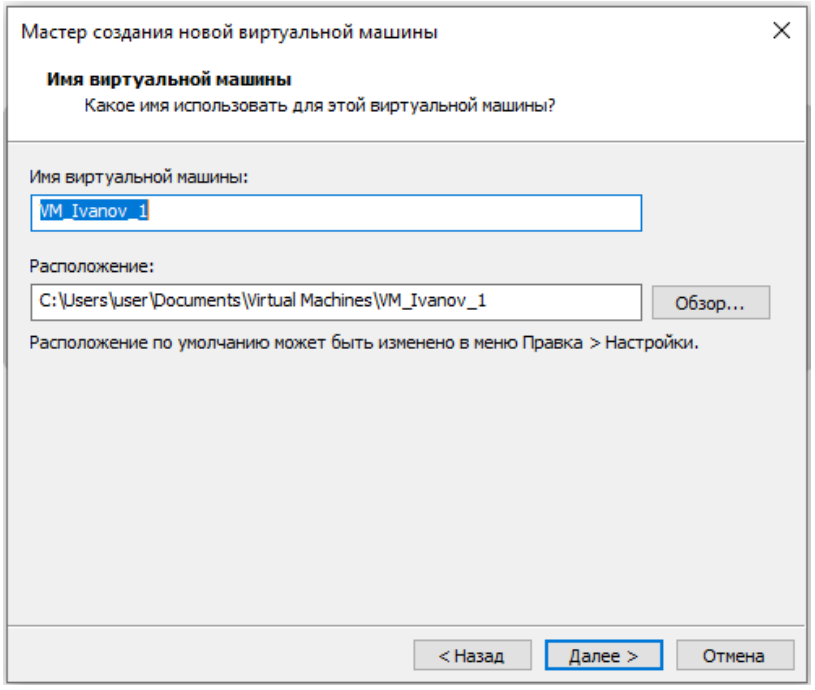


Рисунок 3.5 – Ім’я віртуальної машини (унікальне для кожної створеної ВМ) та її місце зберігання на жорсткому диску

8) Створіть віртуальний жорсткий диск для системи, яку будете встановлювати. Рекомендований розмір – 20 Гб. Оберіть «Сохранить виртуальный диск в одном файле» (рис. 3.6).

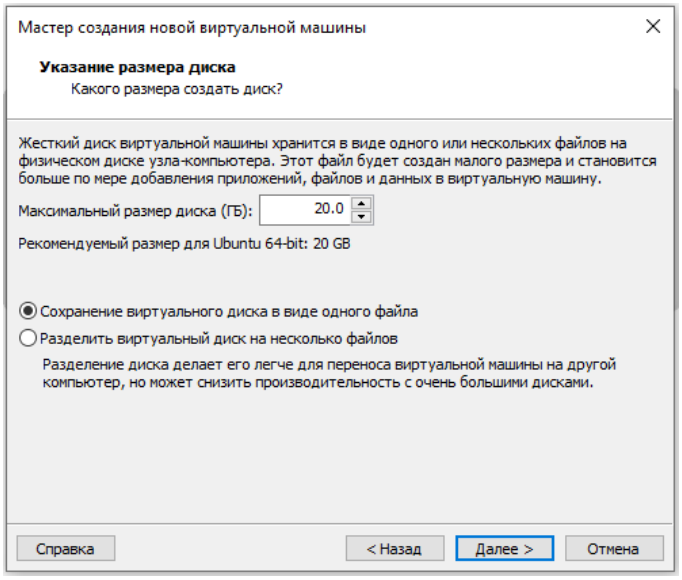


Рисунок 3.6 – Створення віртуального жорсткого диску ВМ

9) Перегляньте параметри віртуальної машини (рис. 2.7).

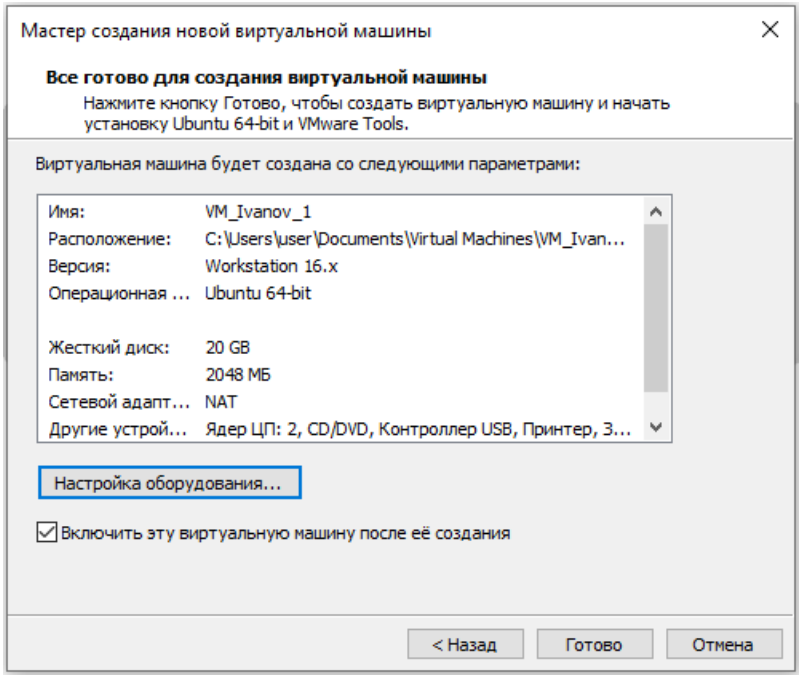


Рисунок 3.7 – Параметри створеної ВМ

В залежності від параметрів реальної машини створені параметри ВМ можуть бути змінені. Перш за все зменшено об’єм ОП. Для зміни параметрів натисніть «Настройка оборудования…» (рис. 3.7). Для зменшення об’єму ОП можливо використати повзунок чи вікно «Объём памяти для этой виртуальной машины».

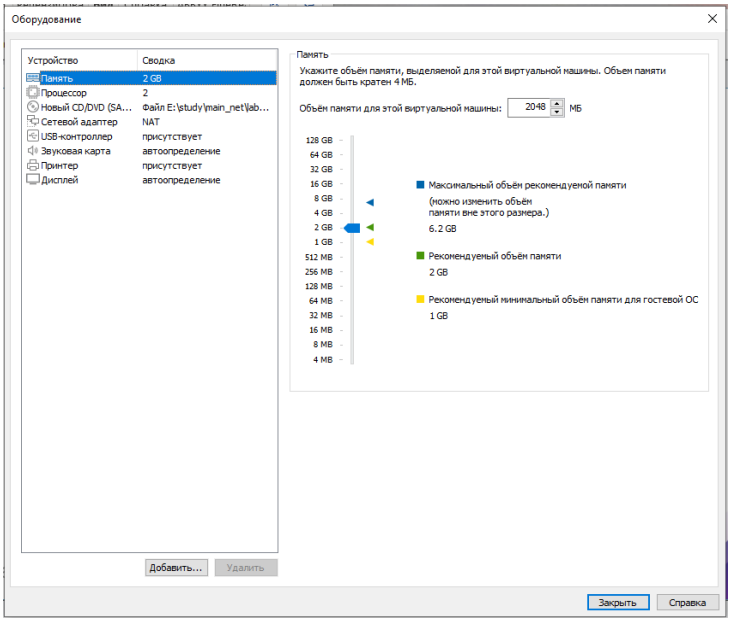


Рисунок 3.8 – Вікно налаштування параметрів ВМ

12) Вийдіть з вікна «Настройка оборудования…» (клавіша «Закрыть») та натисніть «Готово». Починається процес інсталяції віртуальної машини. По завершенню інсталяції з'являється форма з запрошенням до входу в ВМ після введення паролю (рис. 3.9). Зверніть увагу, що лівому верхньому куту форми ВМ присутня назва цієї ВМ, яку Ви указали при налагодженні інсталяції. Введіть пароль, який Ви вибрали в процесі підготовки до інсталяції (Ваш пароль).

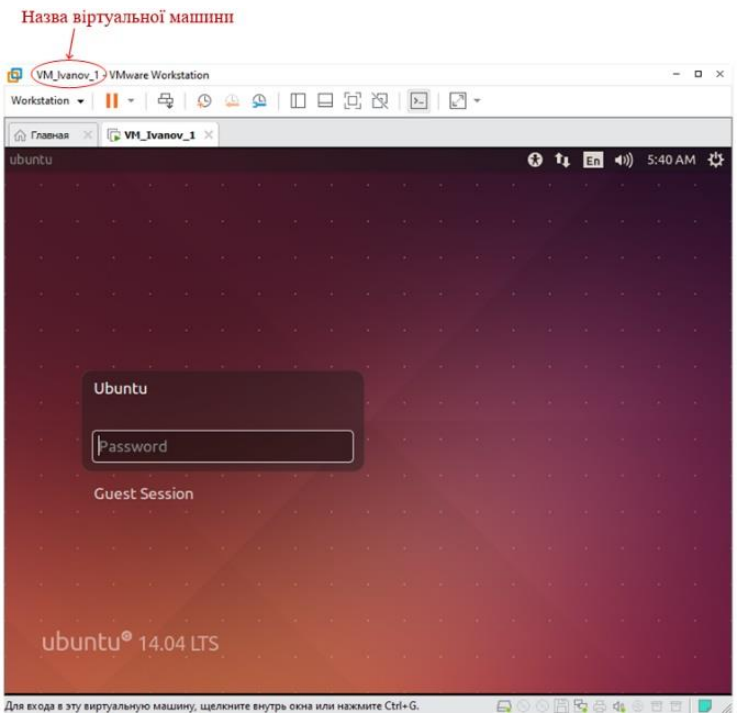


Рисунок 3.9 – Запрошення до входу в ВМ

Майте на увазі, що введення тексту в будь яке вікно ВМ потребує попереднього клацання покажчика миши в цьому вікні.

В деяких випадках може з'явитися повідомлення про помилку в процесі інсталяції. Інструкція про виправлення помилки

13) Після вдалого введення паролю з’являється головне вікно створеної ВМ – закладка VM_Ivanov_1 (рис.3.10).

17) Аналогічним чином створіть іншу віртуальну машину (VM_Ivanov_2).

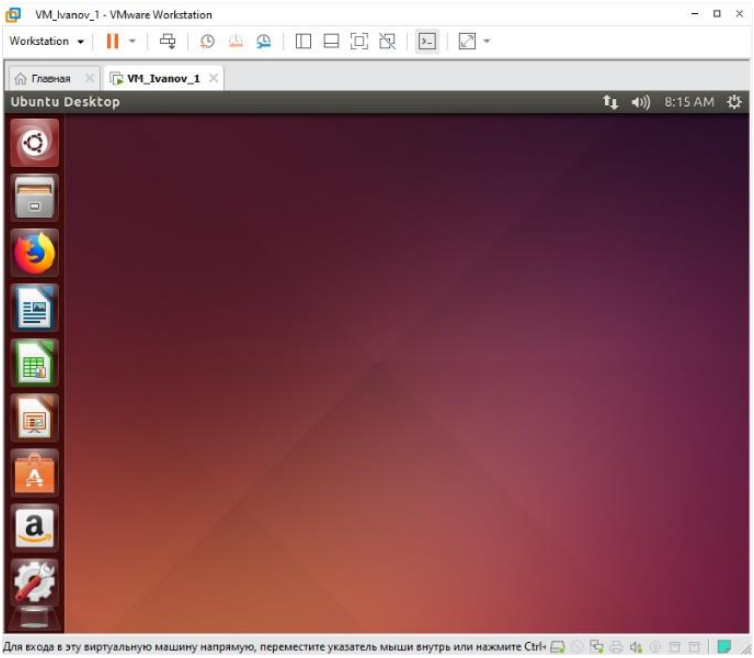


Рисунок 3.10 – Закладка з головним вікном створеної ВМ

Якщо в головному графічному меню натиснути на кнопку  «Отражение или скрытие библиотек», на формі з’явиться панель бібліотек створених ВМ (рис. 3.11).

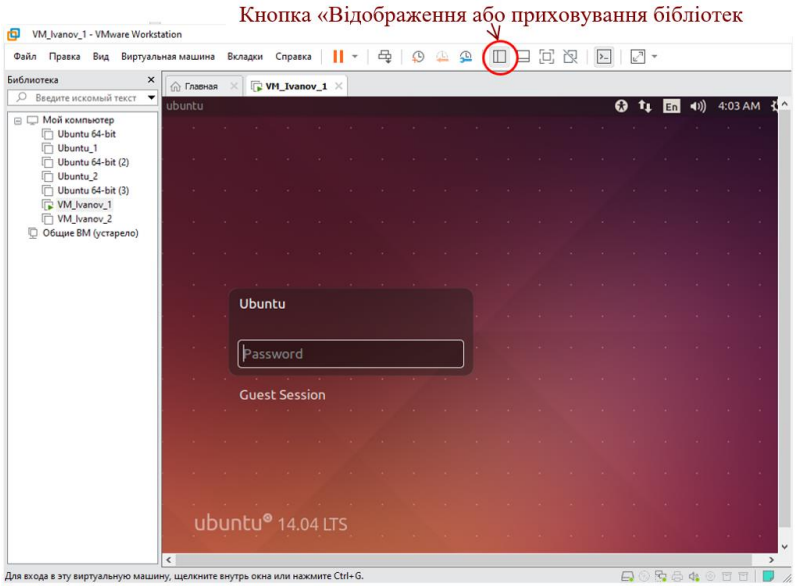


Рисунок 3.11 – Відображення панелі бібліотеки створених ВМ

18) Для того, щоб була можливість вивести на екран монітора одразу декілька ВМ (зручність перегляду взаємодії машин віртуальної мережі!) треба для запуска кожної ВМ зробити окремий ярлик програми VMware Workststions Pro на робочьому столі та у формі «Свойства» цього ярлику (клацнути правою кнопкою миши на ярлику та обрати «Свойства» у розгорнутому списку) в стрічці «Объект» (рис. 3.12) зробити наступні зміни:

<існуючий змість> -n “<розташування ВМ>\<ім’я ВМ>.vmx”

треба додати

Імя та роташування ВМ використовуйте ті, що Ви увели та записали при створенні ВМ (рис. 3.5).

Для прикладів цієї лабораторної роботи у стрічці «Объект» повинно бути:

"C:\Program Files (x86)\VMware\VMware Workstation\vmware.exe"

існуючий зміст

-n "c:\Users\user\Documents\Virtual Machines\VM_Ivanov_1\VM_Ivanov_1.vmx"

треба додати

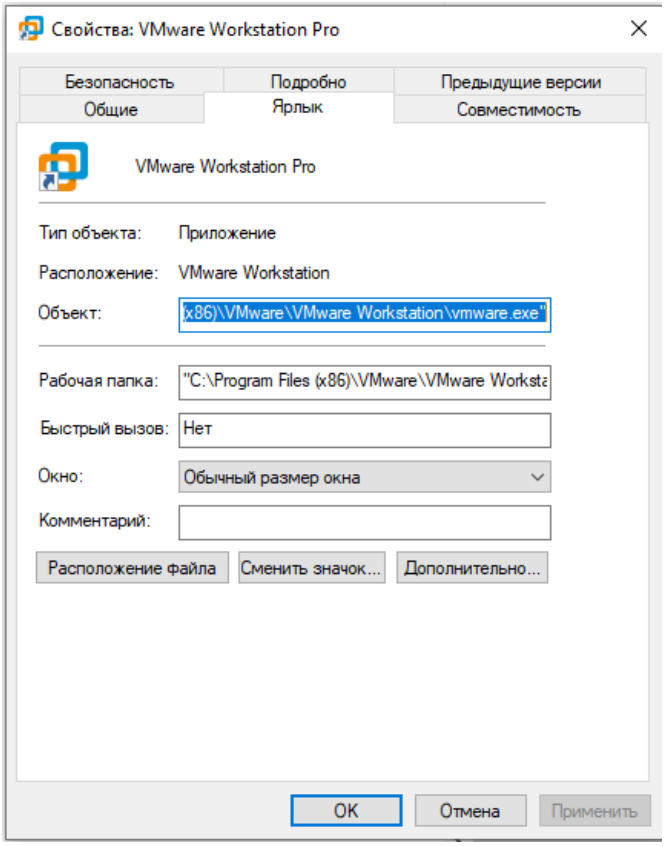


Рисунок 3.12 – Форма «Свойства» ярлика програми VMware Workststions Pro

Звісно, імена ярликів різних ВМ повинні бути різні. Рекомендовано надати їм імена ВМ

3.3.2 Робота з терміналом ВМ

1) Знайдіть термінал – додаток для діалогу користувача з операційною системою. Його можна знайти скориставшись пошуком. Натисніть на піктограму  «Search your computer and online sources» і введіть terminal (рис. 3.13).

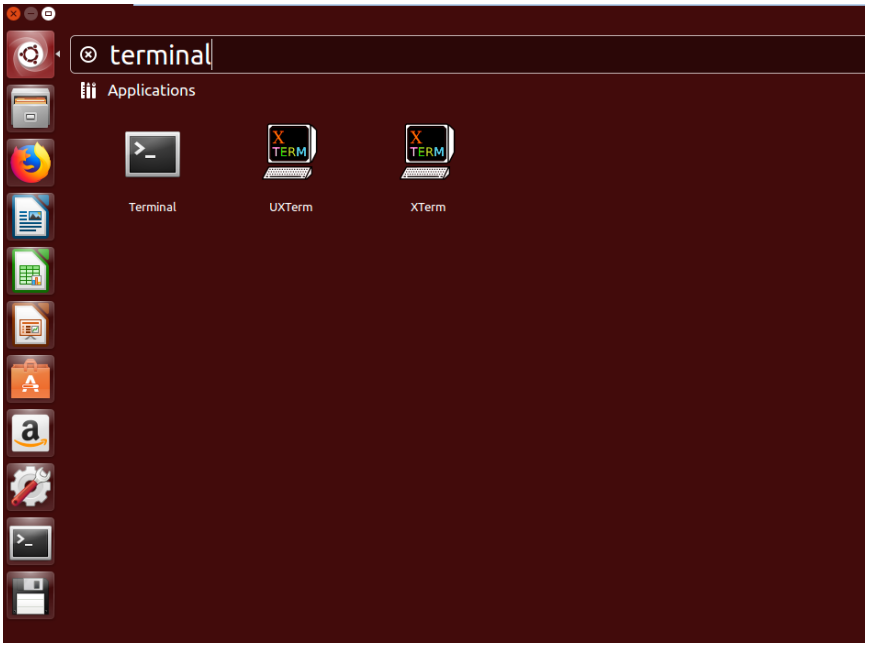


Рисунок 3.13 – Пошук терміналу серед системних утиліт Ubuntu

2) Відкрийте термінал на робочому столі. Для цього клацніть лівою клавішею миші на піктограмі термінала. На робочому столі з'являється вікно терміналу із запрошенням ввести пароль. Після введення паролю у вікні терміналу з'являється запрошення до введення команди користувача (рис. 3.14):

<користувач>@ubuntu: ~$

3.3.3 Налаштування інтерфейсів ВМ

1) Відкрийте термінал на хостах A та B (умовні назви двох створених віртуальних машин користувача ubuntu).

2) Перегляніть та збережіть (зробити скріншоти або запишіть у файл) інформацію про мережеві інтерфейси на обох хостах, щоб визначити які вони носять імена. Для цього використовується команда ifconfig (рис. 3.15).

Бачимо, що на обох хостах присутній інтерфейс eth0 – це інтерфейс мережевої ethernet-карти. Крім того присутній інтерфейс lo – це інтерфейс зворотного зв'язку. У відгуку команди вказано MAC-адресу ethernet-карти та IP4 та IP6 адреси хосту.

Результати роботи в терміналі зберігаємо (робимо скріншоти або записуємо у файл).

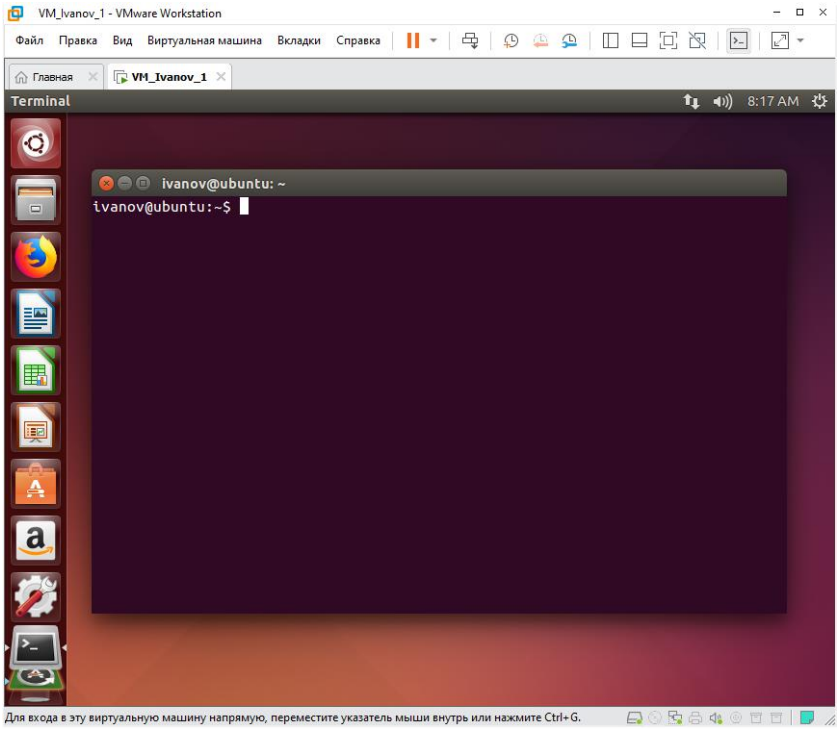


Рисунок 3.14 – Вікно терміналу на робочому столі ВМ Ubuntu

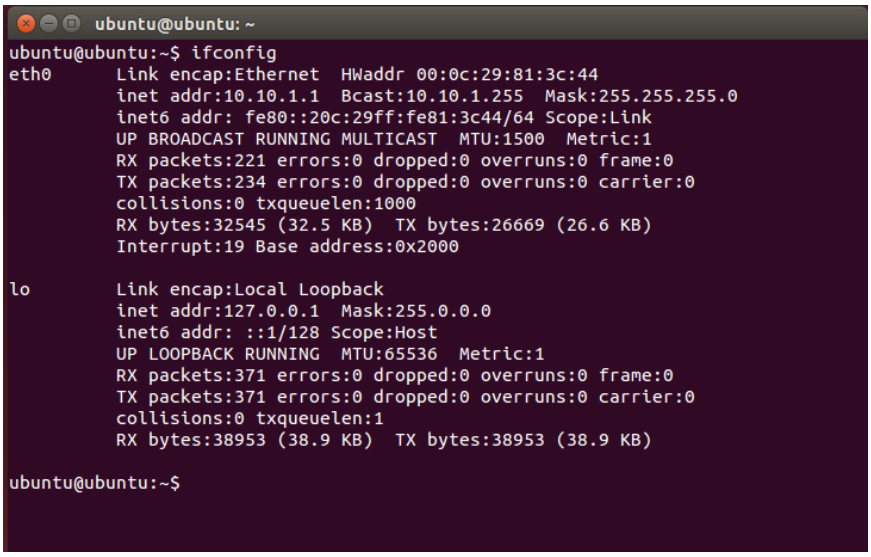


Рисунок 3.15 – Команда ifconfig показує існуючі на ВМ інтерфейси та їх характеристики

Для запису в файл використовуємо команду ifconfig > <ім’я файлу>, наприклад (при опису діалога програми з користувачем жирним шрифтом виділимо те, що вводить користувач):

ubuntu@ubuntu: ~$ **ifconfig > con.txt**

При цьому результати роботи команди будуть виведені не на екран , а в файл ifcofig.txt, що за замовчанням знаходиться в паці Home ВМ. Для доступу к цій папці натисніть клавішу  «files» (рис.3.16).

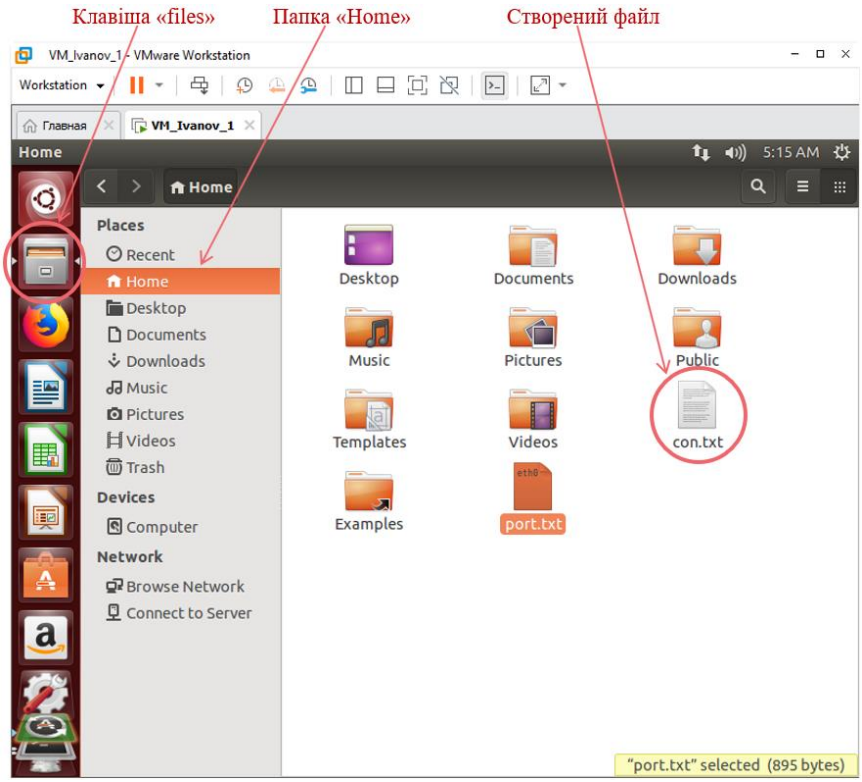


Рисунок 3.16 – Перегляд створеного файлу

Створений файл можливо скопіювати (клацнувши на файлі правою клавішею миші та обравши операцію «Copy») чи перетягнути в будь яку папку реальної машини.

3) На хості A встановіть адресу 10.x.1.1/24. «x» – це номер вашого варіанту роботи.

Змінити IP-адресу можливо командою:

ifconfig <інтерфейс> <IP-адреса>/<маска (у вигляді префикса)>

Важливо! Для виконання деяких команд (завдання адреси інтерфейсу, прослуховування мережі та ін.) потребується перехід у режим суперкористувача. Для цього необхідно ввести команду sudo перед командою, яку Ви хочете виконати, а після вводу команди ввести пароль адміна (Ваш пароль):

ubuntu@ubuntu: ~$ **sudo ifconfig eth0 10.x.1.1/24**

[sudo] password for ubuntu: xxxxxxx

(тут **xxxxxxx** пароль користувача, який на екрані не відображається).

4) На хості B встановіть адресу 10.x.1.2/24.

5) Перевірте зміну IP-адреси на хостах A і B командою ifconfig.

3.3.4 Експеримент по прослуховуванню мережі

Для прослуховування мережі існують спеціальні програми, які мають спільну назву «сніффери» («слухачі»). Слід зазначити, що прослуховування можливе лише на канальному рівні мережі. Один з розповсюджених сніферів – програма tcpdump. Опис цієї програми (команди) надано в додатку 2. В цьому експерименті будемо використовувати цю команду з параметрами, що рекомендовані.

1) На хості А запускаємо прослуховування мережі командою tcpdump:

ubuntu@ubuntu: ~$ **sudo tcpdump -n -i eth0 -v -X net 10.x.1.0/24**

3) Відкриваємо термінал хосту В. Передивляємось ARP-таблицю (команда arp -a) і запускаємо пінгування хосту А:

ubuntu@ubuntu: ~$ **ping -c3 10.x.1.1**

(x – номер Вашого варіанту, «-c3» – опція, що обмежує кількість пінг-запитів)

4) На терміналі хосту А зупиняємо прослуховування (Ctrl+C), передивляємось результати прослуховування. Фрагмент прикладу результатів прослуховування показаний на рис. 3.17.

Результати пінгування та прослуховування зберігаємо (робимо скріншоти або записуємо у файл).

5) На терміналі хосту В передивляємось ARP-таблицю. Зміст таблиці зберігаємо.

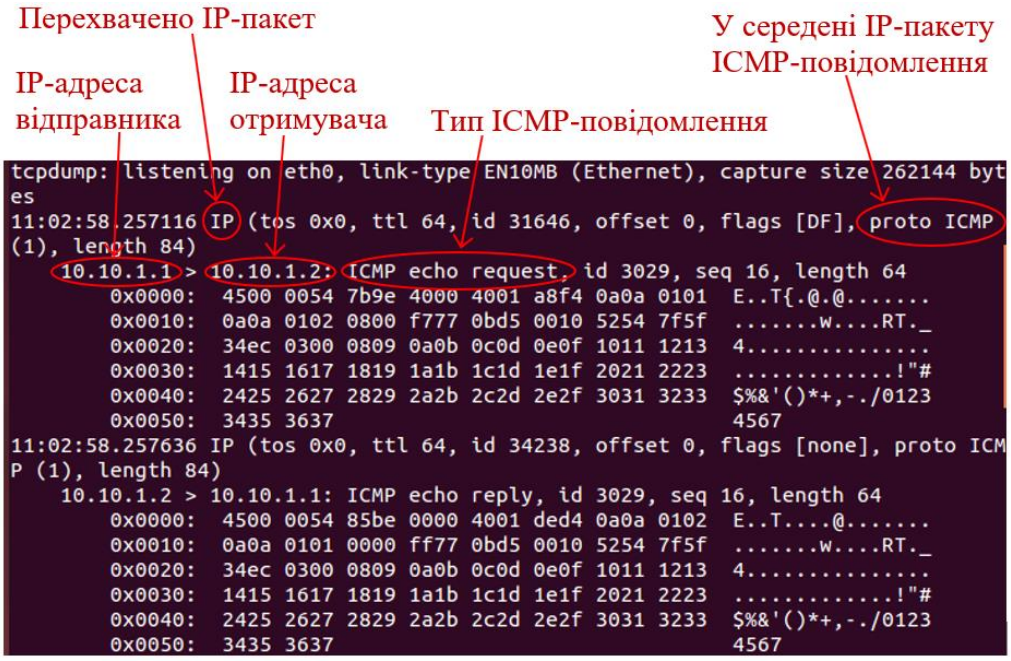


Рисунок 3.17 – Приклад виводу результатів прослуховування за допомогою програми tcpdump

3.4 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Зміст повинен містити наступні пункти:

- назва роботи;
- мета роботи;
- номер варіанту;
- для створених ВМ ім’я користувачів та ім’я ВМ
- скріншоти (чи зміст виведеного файлу) відомостей про інтерфейси створених ВМ (до призначення та після призначення IP-адрес (разом з командами призначення IP-адрес (для обох ВМ).
- скріншот (чи зміст виведеного файлу) фрагменту результату прослуховування командою tcpdump результату пінгування з поясненнями (приклад на рис.3.17).

3.5 Контрольні питання

1. Призначення терміналу ВМ?
2. Якою командою можна вивести інформацію щодо інтерфейсів ВМ?
3. Якою командою можна призначити IP-адресу ВМ?
4. Що таке «сніфер»?
5. Призначення програми tcpdump?
6. На якому мережевому рівні можливо прослуховування мережі?

Лабораторна робота № 4

ДОСЛІДЖЕННЯ МЕТОДУ ВИКОРИСТАННЯ МАСОК ТА ПРЕФІКСІВ ДЛЯ ВИЗНАЧЕННЯ IPV4-АДРЕС МЕРЕЖ ТА ХОСТІВ

Мета роботи. Навчитися визначати структуру IPv4-адреси, в тому числі мережну частину, частину вузла і маску підмережі, визначати різні типи IPv4-адрес та їх використання.

4.1 Загальні відомості щодо масок та префіксів IPv4-адрес

В стандарті IP вузли мережі розділені на окремі групи (підмережі, чи мережі IP, сегменти 3 рівня). Безпосередньо між собою за IP-адресами вузли можуть спілкуватися тільки в середині мережі. Для взаємодії вузлів, які знаходяться в різних мережах використовуються спеціальні пристрої (маршрутизатори – роутери) та протоколи. Тому в IP-мережах використовується дворівнева адресація – адреса мережі та адреса вузла (хосту чи маршрутизатора) в цій мережі.

В протоколі IPv4 адреса має довжину 32 біти в яких міститься адреса мережі (підмережі) та адреса хосту в цій мережі. На сьогодні основним механізмом виділення адреси мережи та адреси хосту з повної IP-адреси є механізм масок.

Маска являє собою 32-розрядний двійковий код, що містить в декількох перших (старших) розрядах «одиниці», а в інших - «нулі». Кількість одиниць в масці визначає кордон номера (ідентифікатора) мережі. Іншими словами, одиничні значення маски дозволяють виділити з повної IP-адреси номер мережі, а молодші розряди IP-адреси, що залишилися, визначають номер вузла в цій мережі (рис.4.1).

Рисунок 4.1 – Формування адреси мережі та адреси хосту цієї мережі за допомогою маски

Часто такий механізм виділення називають «виділення мережевої частини адреси за допомогою логічної операції І».

Зазвичай в документації повну IP-адресу записують наступним чином:

X.X.X.X/M

де X – байт в десятинному вигляді (0…255); M – довжина в бітах мережевої частки адреси у вигляді десяткового числа (в більшості випадках мережева частка адреси зветься «префікс», а M – довжина префікса).

Для виділення мережевої та хостової частини адрес треба спочатку перевести повну IP-адресу в двійковий код, а потім використати операцію «І» для визначення мережевої частини.

Також треба врахувати, якщо всі біти хостової частини (довжина хостової частини дорівнює 32–M) дорівнюють одиниці, то це, так звана, «широкомовна адреса». IP-пакет адресується всім хостам мережі, адреса якої формується з мережевої частині адреси. Таким чином, загальна кількість хостів в мережі, що адресовано, дорівнює 2^{32-M}-2.

Слід знати деякі правила використання IP-адрес в мережі Internet.

1. У стандартах Інтернету визначено декілька автономних (приватних) адрес, рекомендованих для автономного використання, які не можуть бути використані для адресації в мережі Internet:

10.0.0.0/8;
172.16.0.0/12;
192.168.0.0/24.

2. В мережі Internet не може бути двох однакових IP-адрес з різними масками.

4.2. Як з повної мережевої адреси виділити мережеву та хостову частини

Нехай, наприклад, повна мережева адреса має вигляд 60.255.110.21/18.

Тут 18 – це довжина префіксу (кількість безперервних одиниць у початковій частині маски).

При цьому маска (у двійковому вигляді) матиме вигляд:

11111111.11111111.11000000.00000000.

Нагадаємо, що «1» у масці вказують ті розряди повної адреси, які відносяться до мережевої частини адреси, а «0» – розряди, що належать до хостової частини.

Таким чином, перші два байти (16 біт) повної адреси відносяться до мережевої частини адреси, перші 2 біти (що залишилися з 18 біт префікса) у третьому байті повної адреси – до мережевої частини адреси (див. рис. 4.4), останні 6 біт 3-го байта вже ставляться до хостової частини адреси, всі біти 4-го байта повного адреси – до хостової частини адреси.

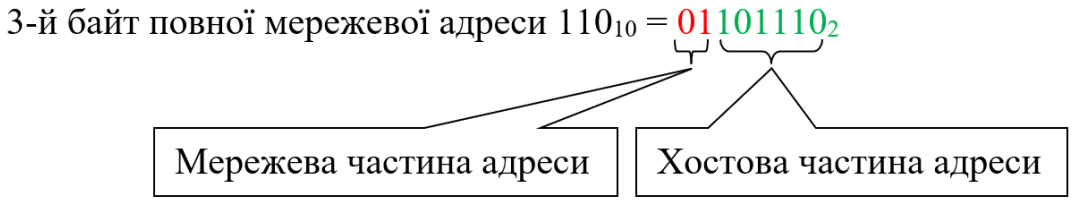
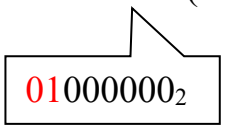


Рисунок 4.4 – Розподіл біт 3-го байта повної адреси між мережевою та хостовою частинами адреси

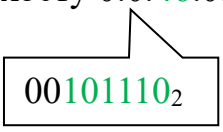
Так як 32-бітова адреса мережі – це мережна частина з повної адреси, доповнена нулями до 32 біт, то 3-й байт адреси мережі – це перші два біти 3-го байта повної адреси, а інші біти 3-го байта мережної адреси нульові .

Тобто адреса мережі – 60.255.64.0 (якщо бути точним, то 60.255.64.0/18)



Адреса хосту – це хостова частина повної адреси, яка може бути доповнена спереду нулями. У прикладі адреса хосту 0.0.46.0.

Можна 46.0.



А ось адреса першого та останнього хостів мережі, широкомовна адреса мережі вказується як повна адреса. Їх правильно записувати таким чином:

• адреса першого хосту мережі 60.255.64.0/18 – 60.255.64.1/18;

• адреса останнього хосту мережі 60.255.64.0/18 – 60.255.127.254/18 (див. рис. 4.5);

• широкомовна адреса мережі 60.255.64.0/18 – 60.255.127.255/18 (див. рис. 4.5).

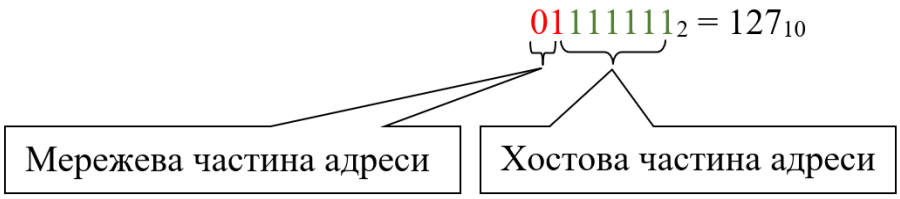


Рисунок 4.5 – Розподіл біт 3-го байта повної мережевої адреси останнього хосту мережі 60.255.64.0/18 та широкомовної адреси цієї мережі між мережевою та хостовою частинами адреси

4.3 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтесь із загальними відомостями щодо побудови IPv4-адрес (п.4.1, матеріали в системі «Лідер», матеріли з конспекту лекцій, матеріали додатку 3, матеріали з рекомендованої літератури).

2) В таблиці 4.1 для декількох варіантів (завданню), виданому викладачем, визначте значення довжини префіксу (стовпчик 4) по значенню маски (стовпчик 3) та значення маски (стовпчик 7) по значенню довжини префіксу (стовпчик 6).

Таблиця 4.1

Варіанти завдань

№ вар.	Завдання1			Завдання2		
	Повна IP-адреса	Маска	Довжина префіксу	Повна IP-адреса	Довжина префіксу	Маска
1	2	3	4	5	6	7
0.	60.255.110.21	255.255.252.0	/18	10.211.17.16	/8	255.0.0.0
1.	72.60.124.23	255.255.224.0		13.165.140.153	/10	
2.	238.78.57.116	255.248.0.0		59.3.115.89	/11	
3.	60.255.110.21	255 .255.192.0		112.231.164.30	/12	
4.	12.211.92.185	255.128.0.0		123.210.206.234	/13	
5.	165.114.253.9	255.255.252.0		220.24.105.100	/14	
6.	253.171.224.98	255.255.240.0		3.174.130.238	/15	
7.	225.194.116.5	255.240.0.0		79.80.159.149	/20	
8.	92.159.7.53	255.255.252.0		112.37.195.31	/17	
9.	43.117.230.183	255.255.192.0		98.107.124.156	/18	
10.	146.247.87.2	255.255.240.0		55.160.113.10	/19	
11.	188.233.122.101	255.255.224.0		56.211.33.164	/21	

1	2	3	4	5	6	7
12.	192.19.3.8	255.255.254.0		53.119.203.221	/22	
13.	84.6.223.106	255.255.252.0		67.200.116.39	/23	
14.	216.45.42.190	255.255.248.0		243.162.237.152	/22	
15.	138.46.140.94	255.248.0.0		4.82.38.2	/21	
16.	152.205.232.105	255.255.192.0		144.112.213.91	/20	
17.	107.214.175.68	255.255.224.0		210.254.11.42	/19	
18.	57.198.77.193	255.255.240.0		11.104.213.125	/18	
19.	122.227.157.232	255.255.128.0		201.24.249.88	/17	
20.	228.219.147.134	255.255.252.0		17.124.16.162	/18	
21.	151.22.163.204	255.248.0.0		55.174.76.242	/19	
22.	37.128.54.52	255.255.192.0		72.96.79.110	/20	
23.	59.145.202.91	255.255.224.0		92.9.234.56	/21	
24.	162.202.242.90	255.255.240.0		144.186.231.149	/22	
25.	159.25.94.89	255.255.252.0		178.15.86.139	/25	

Примітка. Варіант 0 – приклад заповнення

3) Використайте операцію «І» для визначення мережевої та хостової часток в IP-адресах, заданих в табл. 4.1 згідно завданню та заповніть табл. 4.2 відомостями для визначених згідно завданню мереж з табл. 4.1. Приклад формування адреси мережі та адреси хоста з повної IP-адреси хоста наведено в додатку 1.

Таблиця 4.2

Відомості про мережі

№ вар.	IP-адреса мережі	IP-адреса хоста	Адреса першого хоста мережі	Адреса останнього хоста мережі	Широкомовна адреса мережі	Кількість вузлів мережі
0.	60.255.64.0/18	0.0.46.21	60.255.64.1/18	60.255.127.254/18	60.255.127.255/18	16382

Примітка. Варіант 0 – приклад заповнення

4) В Cisco Packet Tracer побудуйте мережу згідно рис. 4.2 відповідно найменшого за номером варіанта свого завдання (Завдання1).

Приклад мережі, побудованої за варіантом №0 показаний на рис. 4.3.

5) З одного з хостів (за Вашим вибором) виконайте пінгування кожного з двох інших хостів.

6) З одного з хостів (за Вашим вибором) виконайте широкомовне пінгування.

7) Повторіть широкомовне пінгування в режимі симуляції (покрокове для одного пінг-запита).

Рисунок 4.2 – Мережа для експерименту

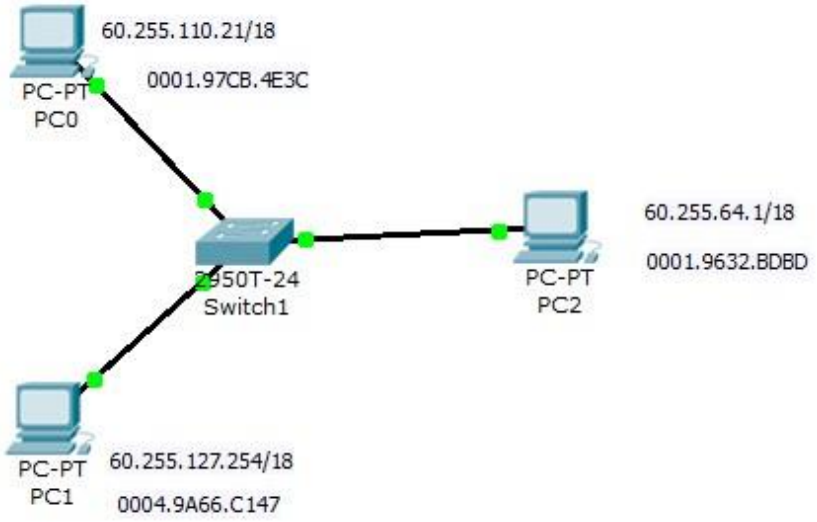


Рисунок 4.3 – Мережа для експерименту (приклад для варіанту №0)

4.4 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Зміст повинен містити наступні пункти:

– назва роботи;

– мета роботи;

– завдання (номери варіантів табл. 4.1);

– таблиця 4.1 з повністю заповненими рядками згідно Вашого завдання;

– таблиця 4.2 з повністю заповненими рядками згідно Вашого завдання;

– скріншот мережі для експерименту з IP- та MAC-адресами хостів згідно Вашого варіанту.

– скріншоти результатів пінгування за п.п. 5-6 послідовності виконання роботи;

- скріншот списку подій результату широкомовного пінгування в режимі симуляції в мережі (один пінг-запит)

– скріншоти докладної інформації щодо інформації пінг-запиту (перший крок) та пінг-відповіді (два останні кроки) з поясненнями до них.

4.5 Контрольні питання

1. Задана IP-адреса 194.20.133.19/17. Визначте IP-адресу мережі та IP-адресу вузла в мережі.

2. Задана IP-адреса з маскою або довжиною префіксу (приклад – табл. 4.3). Визначте тип адреси: адрес вузла, адрес мережі або широкомовна розсилка.

Таблиця 4.3

Адреса вузла / адреса мережі / широкомовна розсилка

IP-адреса	Маска	Тип адреси
10.1.1.1	255.255.255.252	
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	

3. Задана IP-адреса з маскою або довжиною префіксу (приклад – табл. 4.4). Визначте тип адреси: загальний або приватний.

Таблиця 4.4

Загальний / приватний

IP-адреса/довжина префіксу	Загальний/приватний
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	

4. При налаштування двох ПК в одній мережі ПК-А присвоєно IP-адресу 192.168.1.18, а ПК-Б IP-адресу 192.168.1.33. Маска мережі обох комп'ютерів 255.255.255.240. Чи зможуть ці ПК взаємодіяти один з одним безпосередньо?

Додатки

Додаток 1

Формат команди ping

Ping <опції> <адреса_вузла>

В якості адреси вузла можна передавати як ip-адреса, так і доменне ім'я. Опції налаштовують поведінка утиліти. Основні з них:

- -4 – використовувати тільки ipv4 (за замовчуванням);
- -6 – використовувати тільки ipv6;
- -A – адаптивний режим, час між відправленнями пакета адаптується до часу передачі і прийому пакета, але не менше ніж 200мс;
- -b – дозволити ping широкомовної адреси;
- -c – кількість пакетів, які потрібно відправити;
- -D – виводити час у вигляді UNIX timestamp;
- -f – режим флуду, в цьому режимі пакети передаються без затримок, може використовуватися для здійснення DoS атак на окремі вузли. Кількість точок, які виводить утиліта позначає кількість втрачених пакетів;
- -i – інтервал в секундах між відправкою пакетів;
- -I – використовувати цей мережевий інтерфейс для відправки пакетів;
- -l – режим перевантаження, відправляється дуже багато пакетів і система не стежить за відповідними пакетами;
- -n – не отримувати домени для ip адрес;
- -r – ігнорувати таблиці маршрутизації і відправити пакет на вказаний інтерфейс;
- -s – розмір одного пакета;
- -t – встановити TTL вручну;
- -v – більш детальний висновок.

Примітка. Не всі ці опції доступні в VMware Workstation

Додаток 2

Опції команди tcpdump

- -D – вивести вичерпний перелік доступних інтерфейсів;
- -i eth0 – перевірити певний інтерфейс (eth0);
- -i any – перевірити інтерфейси на предмет наявності будь-якого трафіку;
- -n – виводити IP- адреси, а не імена хостів;
- -nn – виводити IP-адреси разом з номерами портів, а не імена хостів з назвами протоколів;
- -q – відображати мінімальний обсяг даних про пакет;
- -t – відключити висновок мітки часу для всіх рядків;

- -tttt -включає для кожної з рядків відображення тимчасових міток в форматі за замовчуванням;
- -X – відображати дані пакета одночасно в шістнадцятковій і в ASCII кодуваннях;
- -XX – аналог -X, який також виводить ethernet header;
- -v, -vv, -vvv – збільшити обсяг повертаються даних про пакетах;
- -c – вивести вказане число пакетів, після чого стоп;
- -s – обчислити довжину snaplength захоплення в байтах (-s0, щоб обчислити все, якщо ви навмисно не захопили менше);
- -S – вивести абсолютні порядкові номери;
- -e – продемонструвати ethernet header;
- -q – вивести мінімум даних про пакет;
- -E – зробити розшифровку трафіку IPSEC, віддавши ключ шифрування.

Примітка. Не всі ці опції доступні в VMware Workstation.

Список літератури

1. Курс «Комп'ютерні мережі» у системі «Лідер». *Український державний університет науки і технологій.* URL: https://lider.ust.edu.ua (дата звернення: 02.10.2023).
2. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.
3. Жуков І. А., Гуменюк В. О., Альтман І. Є. Комп’ютерні мережі та технології : навч. посіб. Київ : НАУ, 2004. 276 с.

Навчально-методичне видання

Жуковицький Ігор Володимирович,
Заєць Олексій Петрович,
Дзюба Володимир Володимирович

КОМП'ЮТЕРНІ МЕРЕЖІ (ЧАСТИНА 1)

Навчально-методичні рекомендації до лабораторних робіт

Електронне видання

Експертний висновок склав д-р техн. наук, проф. Анатолій Косолапов

Зареєстровано НМВ УДУНТ (№ 664 від 24.10.2023)

В авторській редакції

Комп’ютерна верстка І. В. Жуковицький

Формат 60х84 1/16. Ум. друк. арк. 2,79. Обл.-вид. арк. 1,44.
Зам. № 102

Видавець: Український державний університет науки і технологій
вул. Лазаряна, 2, ауд. 2216, м. Дніпро, 49010.
Свідоцтво суб’єкта видавничої справи ДК № 7709 від 14.12.2022

Адреса видавця та дільниці оперативної поліграфії:
вул. Лазаряна, 2, Дніпро, 49010