МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

КОМП’ЮТЕРНІ МЕРЕЖІ

ЧАСТИНА 1

МОДЕЛЮВАННЯ КОМП’ЮТЕРНИХ МЕРЕЖ

Житомир
Вид-во ЖДУ імені Івана Франка
2022

УДК 004.7:004.94
Д60

Рекомендовано до друку вченою радою Житомирського державного університету імені Івана Франка

(протокол № 4 від 25.03.2022 р.)

Рецензенти:

О. Спірін – доктор педагогічних наук, професор, член-кореспондент НАПН України, проректор з наукової роботи та цифровізації інституту менеджменту освіти;

О. Коротун – кандидат педагогічних наук, доцент кафедри комп'ютерних наук Державного університету «Житомирська політехніка».

Комп'ютерні мережі. Частина 1. Моделювання комп'ютерних мереж: Лабораторний практикум. / Укладачі**:** О. С. Яценко, О. І. Яценко. – Житомир: Вид-во ЖДУ ім. І. Франка, 2022. – 76 с.

Запропонований лабораторний практикум містить лабораторні роботи з освітньої компоненти «Комп'ютерні мережі». Кожна лабораторна робота містить короткі теоретичні відомості відповідно до теми, індивідуальні завдання та приклади їх виконання Призначений для студентів фізико математичного факультету, що здобувають освіту за спеціальностями 014.09 Середня освіта (Інформатика), 015.39 Професійна освіта (Цифрові технології).

ЗМІСТ

ВСТУП

Глобалізація суспільства та активний розвиток сучасних інформаційних технологій супроводжуються збільшенням ролі комунікаційних систем різного призначення та комп'ютерних мереж, а це, в свою чергу, сприяє розвитку в області формуванню єдиного світового інформаційного простору. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі і навчальної, для якої важливе значення мають час та оперативність її доставки до користувачів.

Однією з основних тенденцій розвитку сучасних комп'ютерних мереж (КМ) стає розширення доступності інформаційно-обчислювальних ресурсів мереж для окремих абонентів. У зв'язку з цим окремі абоненти КМ стають все більш активними споживачами їх ресурсів і учасниками створення баз даних, що безпосередньо володіють технікою доступу до інформаційних ресурсів КМ. З іншого боку підвищення активності окремих абонентів комунікаційних мереж обумовлене розподілом інформаційно-обчислювальних ресурсів сучасних комп'ютерних мереж, у зв'язку з чим в розподілених системах різко зростає роль комунікацій як на рівні баз даних і прикладних завдань, так і на рівні технічних систем.

В період пандемії роль комп'ютерних мереж значно зросла як на рівні роботи сучасних підприємств та організацій так і на рівні освіти. Все частіше використовуються в процесі навчання та роботи сервіси обміну документами (електронна пошта), хмарні сховища, сервіси обміну повідомленнями в on-line, електронні бібліотеки тощо, що значно збільшує ефективність як навчання так і роботи.

Особливе місце займають сучасні технології комп'ютерних мереж, серед яких слід виділити локальні та глобальні мережі. Це пояснюється необхідністю використання корпоративної інформації, що міститься в корпоративних базах даних, що можуть розташовуватися як в окремих підрозділах організації, так й за її межами. Сучасні технології оброблення документів різного призначення

базуються на засобах телекомунікаційного зв’язку й стандартів комп’ютерних мереж, які виступають як транспортні системи передачі даних.

Для підвищення ефективності функціонування мереж підприємств та організацій повинні використовуватися засоби їх модернізації у випадку збільшення кількості робочих станцій та користувачів. Це призводить до необхідності більш детальнішого вивчення та використання спеціальних пристроїв та відповідних стандартів для об’єднання окремих локальних мереж в єдину.

Важливу роль в підготовці фахівців, що мають відповідні знання та навички відіграє вивчення освітньої компоненти «Комп’ютерні мережі» з використанням в навчальному процесі програми Cisco Packet Tracer.

Програма Cisco Packet Tracer – це багата на функції програма моделювання комп’ютерних мереж, що дозволяє експериментувати з проектуванням та «поведінкою» мережі та оцінювати можливі сценарії. Вона здатна імітувати роботу мережевого обладнання та різних типів з’єднань, що дозволяє проектувати мережі різного розміру та складності.

Цей симулятор дозволяє користувачам розробляти власні мережі, імітувати роботу різних протоколів, зберігати та коментувати свої розробки. Користувачі можуть досліджувати та використовувати мережеві пристроїв, такі як концентратори, маршрутизатори, сервери, робочі станції, різні типи з’єднання між ними та ін.

ЛАБОРАТОРНА РОБОТА № 1
СТВОРЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ

Мета роботи: ознайомитись з типами мережевого обладнання та з середовищем трасування пакетів. Навчитися створювати комп'ютерну мережу з допомогою комутаторів та перевіряти її роботу

Теоретичні відомості

Комп'ютерна мережа – сукупність комп'ютерів та інших пристроїв, що з'єднані лініями зв'язку та обмінюються інформацією між собою відповідно до певних правил – протоколів.

Основна мета мережі – забезпечити користувачам можливість спільного використання мережевих ресурсів. *Мережними ресурсами* називають інформацію, програмне та апаратне забезпечення.

Щоб організувати локальну комп’ютерну мережу з невеликою кількістю комп'ютерів (10 – 30) найчастіше використовується одна з типових топологій (звичайна шина, кільцева, зірка або повнозв’язна топологія). Ці топології мають властивість однорідності – всі комп'ютери володіють однаковими правами на доступ до інших комп'ютерів (за винятком центрального комп'ютера в топології «зірка» Однорідність структури дозволяє легко збільшити кількість комп'ютерів, полегшує технічне обслуговування та експлуатацію мережі. Однак ці топології накладають обмеження певні обмеження на:

- довжину лінії зв’язку між двома вузлами;
- кількість вузлів в мережі;
- інтенсивність трафіку.

Для зняття цих обмежень використовуються спеціальні методи. структурування мережі та спеціальне мережеве обладнання – повторювачі (ретранслятори), концентратори, вузли, мости, комутатори, маршрутизатори. Це обладнання називається комунікаційним, з його допомогою окремі сегменти мережі взаємодіють один з одним.

Ретранслятор – найпростіший пристрій зв'язку, використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою

збільшення загальної довжини мережі. Ретранслятор покращує якість передаваного сигналу (відновлює потужність, амплітуду сигналу і т. д.). Ретранслятор який має кілька портів і з'єднує кілька фізичних сегментів, часто називають концентратором або хабом.

Міст (англ. Bridge) – ділить середовище передачі мережі на частини (логічні сегменти), передаючи інформацію з одного сегмента мережі на інший тільки в тому випадку, коли така передача є необхідною, тобто якщо адреса комп'ютера призначення належить іншій підмережі Міст ізолює трафік однієї підмережі від трафіку іншої, покращуючи загальну продуктивність передачі даних в мережі.

Комутатор (*switch*) за принципом обробки кадрів практично не відрізняється від моста. Єдина відмінність полягає в тому, що він є свого роду комунікаційним мультипроцесором, оскільки кожен з його портів оснащений мікросхемою, яка обробляє кадри за алгоритмом моста незалежно від мікросхем інших портів. Завдяки цьому загальна продуктивність комутатор, як правило, вища від продуктивності традиційного моста, що має один процесор.

Маршрутизатор або *роутер* (*router*) – спеціалізований мережевий комп'ютер, який має два або більше мережних інтерфейсів та пересилає пакети даних між різними сегментами мережі. Маршрутизатор може зв'язувати неоднорідні мережі різної архітектури. Для прийняття рішень про пересилку пакетів він використовує інформацію про топологію мережі та правила, встановлені адміністратором.

Шлюз – використовується для об'єднання мереж з різними типами програмне забезпечення та апаратне забезпечення.

Практична частина

1. Додайте на робочу область програми 5 комутаторів Switch 2960-24TT. За замовчуванням вони називаються Switch0 – Switch4.

2. Додайте на робоче поле 8 комп'ютерів з іменами за замовчуванням PC0 – PC7.

3. Об’єднайте пристрої до мережі Ethernet, як показано на рис. 1.1. Комп'ютер з комутатором об’єднуються витою парою, а комутатори між собою

– крос-кабелем. Всі пристрої для підключення використовують порти FastEthernet.

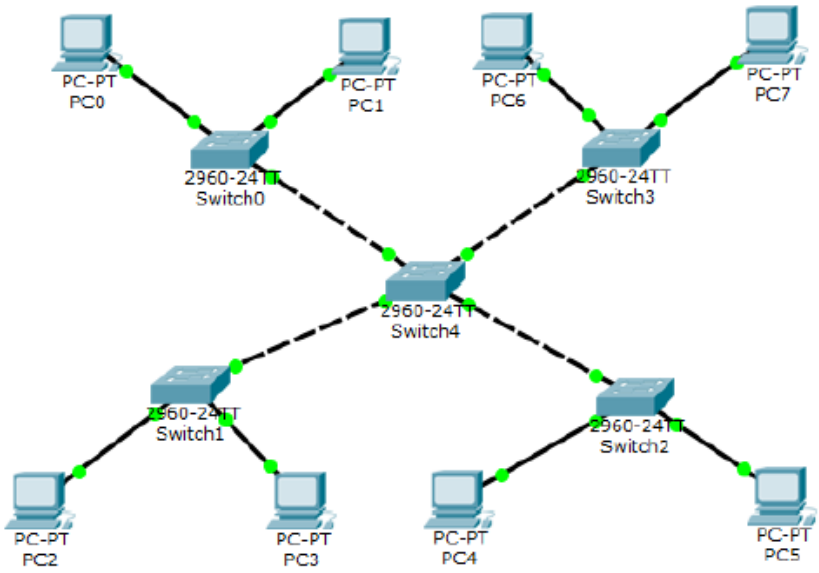


Рис. 1.1. Модель мережі Ethernet

4. Збережіть створену топологію за допомогою команди *Save* в меню *File*.

5. Відкрийте вікно властивостей пристрою PC0, клацнувши лівою кнопкою миші на його зображення. Перейдіть на вкладку *Desktop*і відкрийте командний рядок, натиснувши на *Command Prompt*.

6. Для виведення списку доступних команд в командний рядок внесіть *?* та натисніть *Enter*.

7. Налаштування комп'ютера здійснюється за допомогою команди *ipconfig*. Наприклад, для того, щоб задати PC0 мережеву адресу *192.168.1.2* і маску *255.255.255.0* в командному рядку потрібно внести:

ipconfig 192.168.1.2 255.255.255.0

8. Для перевірки присвоєних значень мережевої адреси і маски в командний рядок потрібно повторно ввести ipconfig. З'явиться повідомлення про задані мережні параметри пристрою:

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80:230:A3FF:FEAA:BD12

IP Address.....: 192.168.1.2

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 0.0.0.0

9. IP-адресу та мережеву маску мережі також можна встановити використовуючи графічний інтерфейс пристрою. Для цього у вікні *Desktop* необхідно набрати *IP Configuration.* Відкриється вікно, що зображено на рис. 1.2. Мережева адреса вводиться в поле *IP Adress*, а маска – в поле *Subnet Mask.* Перемикач способу присвоєння IP-адреси повинен бути в положенні *Static*.

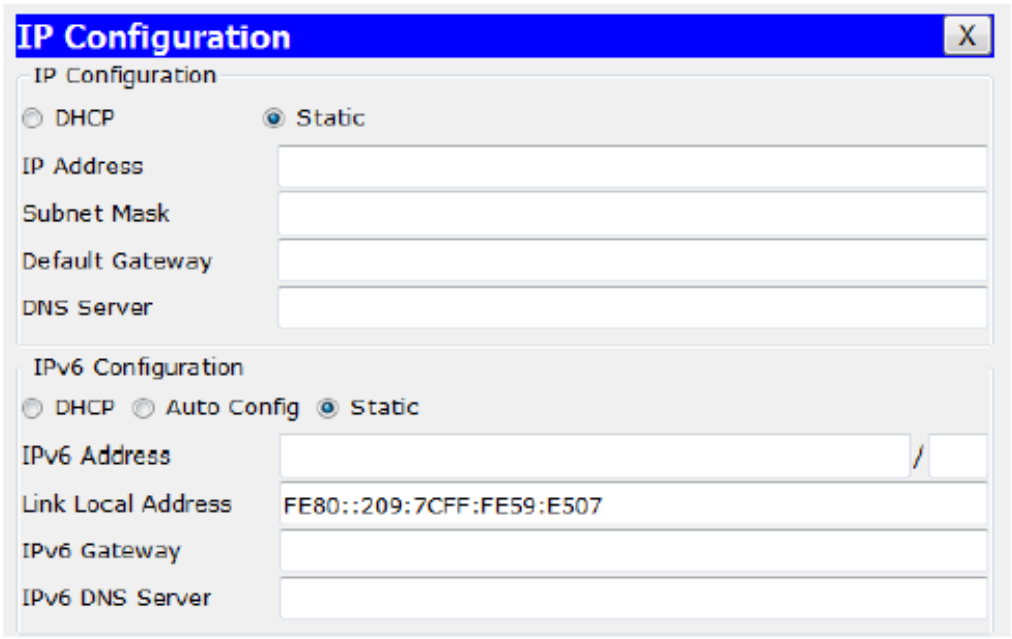


Рис. 1.2. Вікно налаштувань IP Configuration

10.Аналогічно для решти комп’ютерів призначте адреси використовуючи один з перерахованих вище способів. Мережні адреси та маска підмережі пристроїв наведені в таблиці. 1.1.

Таблиця 1.1. Настройки комп'ютерної мережі

Ім’я компютера	**IP-адреса**	**Маска підмережі**
ПК0	192.168.1.2	255.255.255.0
ПК1	192.168.1.3	255.255.255.0
ПК2	192.168.1.4	255.255.255.0
ПК3	192.168.1.5	255.255.255.0

ПК4	192.168.1.6	255.255.255.0
ПК5	192.168.1.7	255.255.255.0
ПК6	192.168.1.8	255.255.255.0
ПК7	192.168.1.9	255.255.255.0

11. Перевірте правильні мережних налаштувань пристроїв та роботоздатність мережі за допомогою команди *ping*. Для цього, потрібно відкрити командний рядок пристрою, ввести *ping* і IP-адресу іншого мережевого пристрою. Наприклад, зайдемо на комп'ютер PC0 і «пропінгуємо» комп'ютер PC1. Нижче наведені результати виконайте команди *ping:*

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

Таким чином, якщо пристрої мережі сконфігуровані правильно, можна пропінгувати з кожного комп’ютера будь-який інший.

12. У середовищі Packet Tracer можна простежити рух пакетів різних мережевих протоколів з допомогою режиму симуляції. Щоб перейти до режиму симуляції, натисніть кнопку *Simulation Mode* у правому нижньому куті робочої області або комбінацію клавіш *Shift+S.*

Справа від робочої області відкриється вікно *Simulation Panel* (див. рис. 1.3), в верхній частині якого знаходиться область подій *Event List* та кнопка очистки списку подій *Reset Simulation*. Управління відтворенням здійснюється з допомогою кнопок *Play Controls*. Так для переходу до наступнеої події потрібно

натиснути кнопку *Capture / Forward*. В нижній частині вікна знаходиться фільтр потоків.

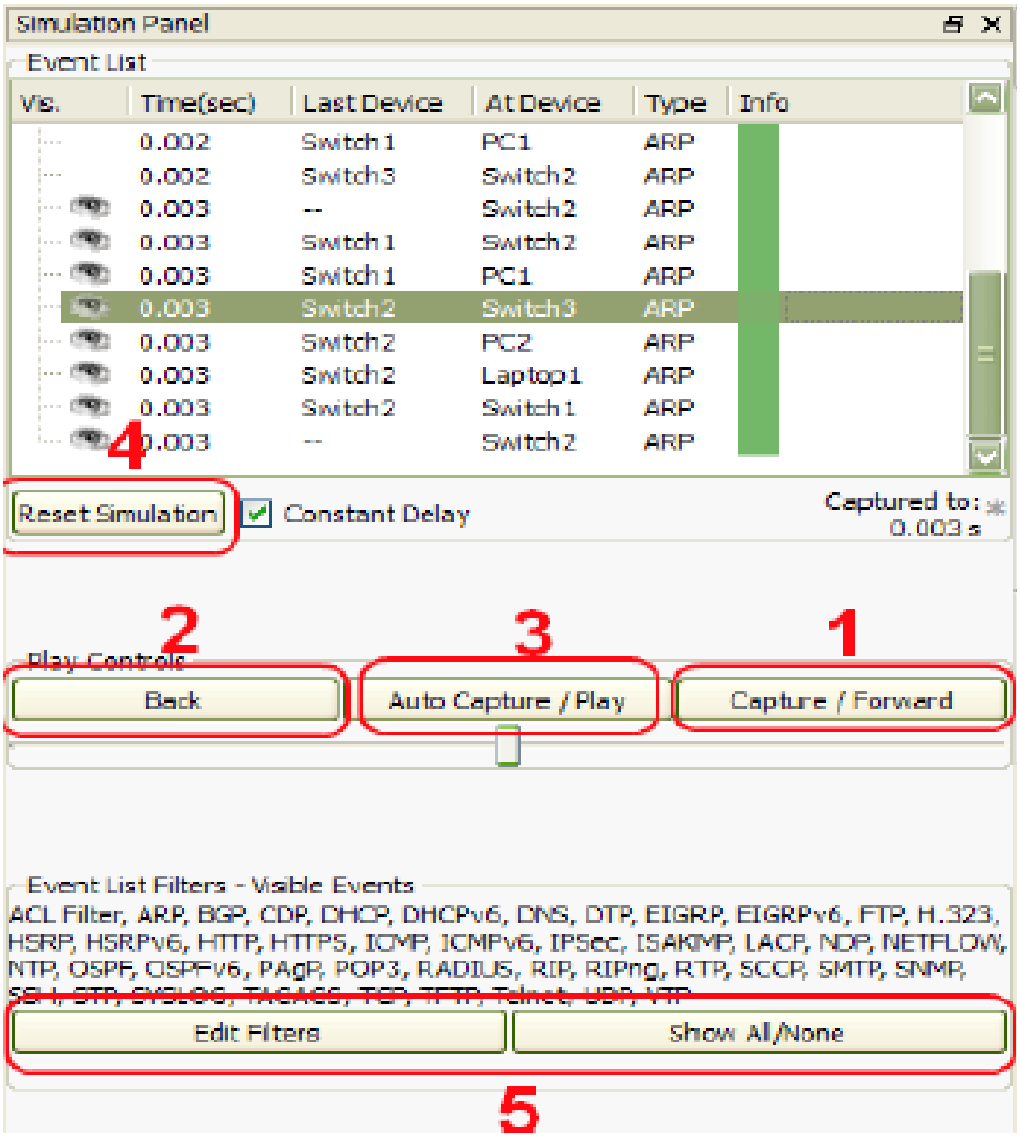


Рис. 1.3. Вікно Simulation Panel

13. З вузла PC1 пропінгуйте вузол PC3. Для того щоб виключити випадковий трафік між вузлами із запропонованого для дослідження списку протоколів виберіть тільки протокол ICMP. Відкрийте командний рядок пристрою PC1, введіть *ping* та IP-адресу мережевого пристрою PC3. В результаті таких дій на вузлі PC1 утвориться пакет («конверт») (рисунок 1.4).

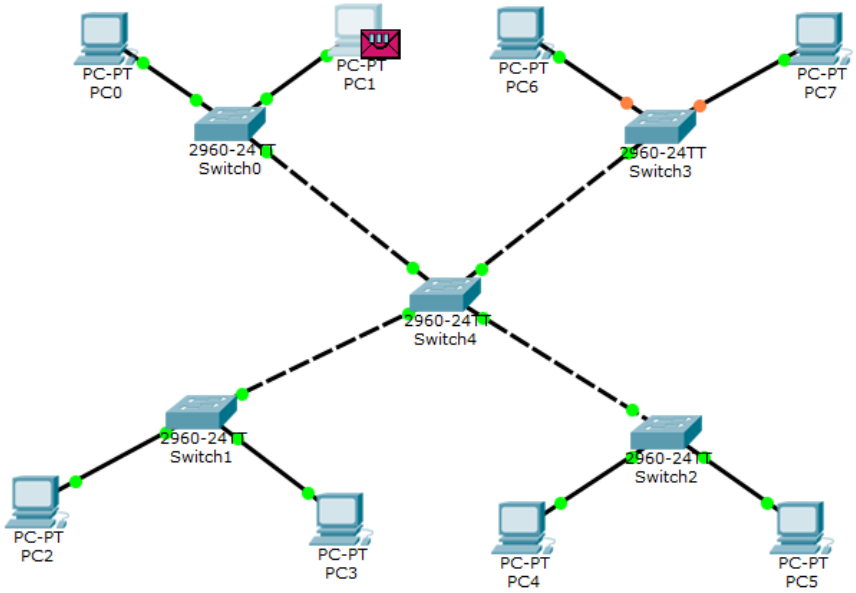


Рис. 1.4. Створення запиту в режимі симуляції

При цьому в полі *Event List* зявиться даний пакет з зазначенням його типу

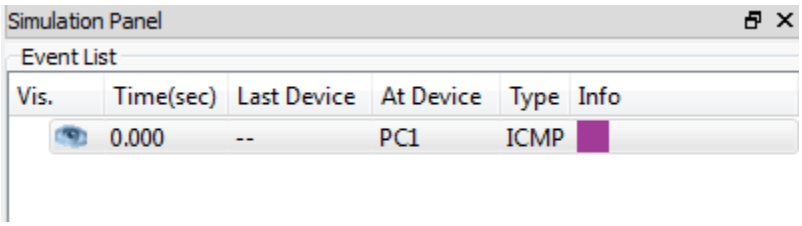


Рис. 1.5. Контроль роботи протоколів

Для отримання більш детальної інформації про пакет, натисніть на нього лівою кнопкою миші. На вкладці *OSI Model* можна побачити, на якому мережної моделі OSI був сформований пакет та які рівні він пройде для переходу на наступний вузол (рис. 1.6). На вкладці *Outbound PDU Details* відображається структура пакету (рис. 1.7)

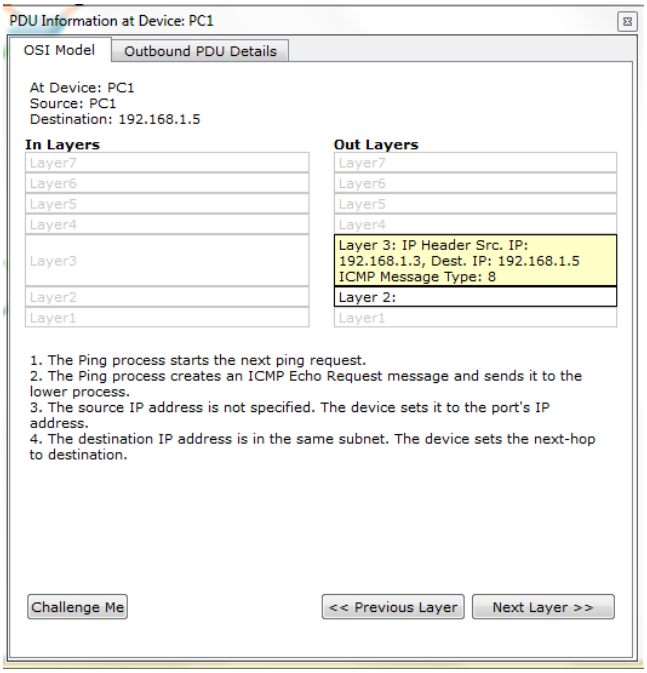


Рис. 1.5. Пакет на рівнях моделі OSI

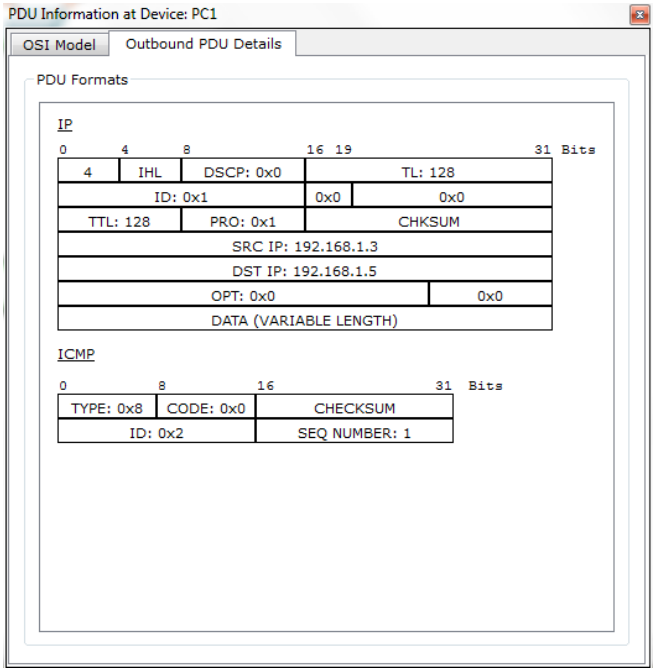


Рис. 1.6. Структура пакету

14. Щоб запустити пакет в мережу, потрібно натиснути кнопку *Capture / Forward* у вікні *Simulation Panel*. Пакет перейде на комутатор Switch0, оскільки це єдине мережне підключення вузла PC1. Комутатор Switch0 пересилає пакет на комутатор Switch4. У свою чергу, комутатор Switch4 пересилає пакет на Switch1, а потім Switch1 надсилає передаваний пакет на вузол PC3., PC3, після отримання пакета, визначає, що він призначений для нього, і, сформувавши відповідь, відправляє пакет на PC1.

Після того, як PC1 отримав відповідь від PC3, у вікні командного рядка з'явиться запис, що повідомляє про проходження ехо-запиту:

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=7ms TTL=128

Завдання для індивідуальної роботи

1. Створіть топологію мережі відповідно до варіанту (табл. 1.2). У всіх варіантах в якості комутаторів використайте Switch 2960.

2. Призначте комп'ютерам IP-адреси відповідно до вказаного діапазону адрес (Таблиця 1.3). Мережна маска для всіх пристроїв 255.255.255.0.

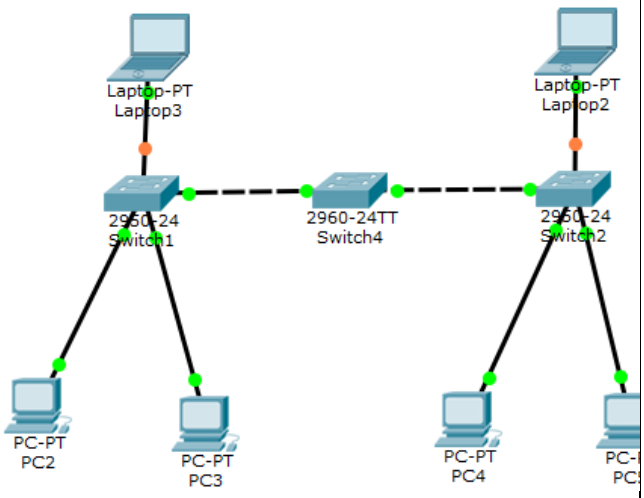
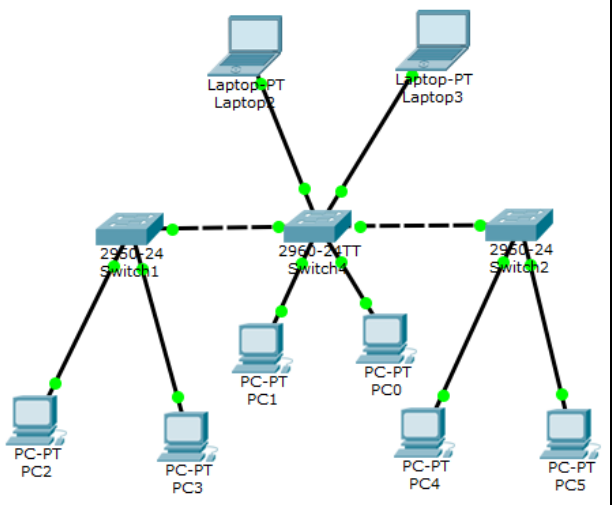
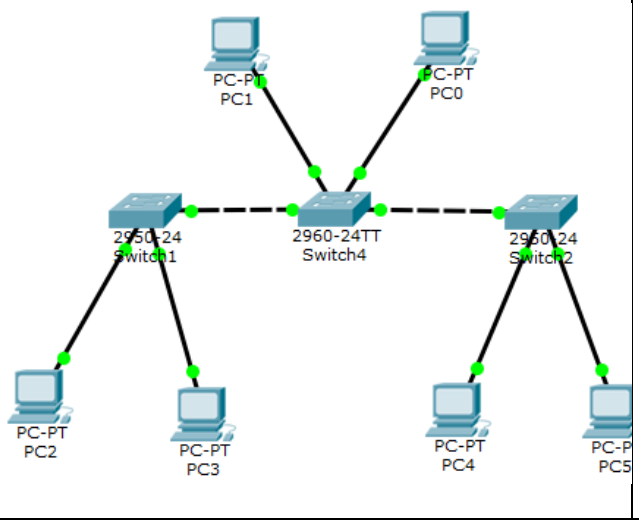
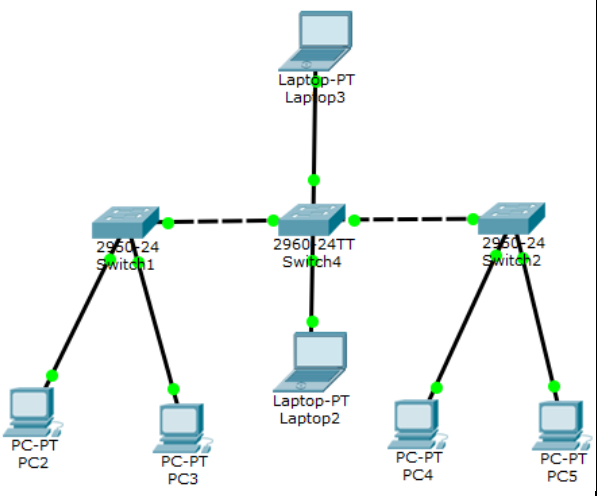
3. Дайте всім кінцевим вузлам різні імена.

4. Перевірте налаштування кожного кінцевого вузла (команда *ipconfig*).

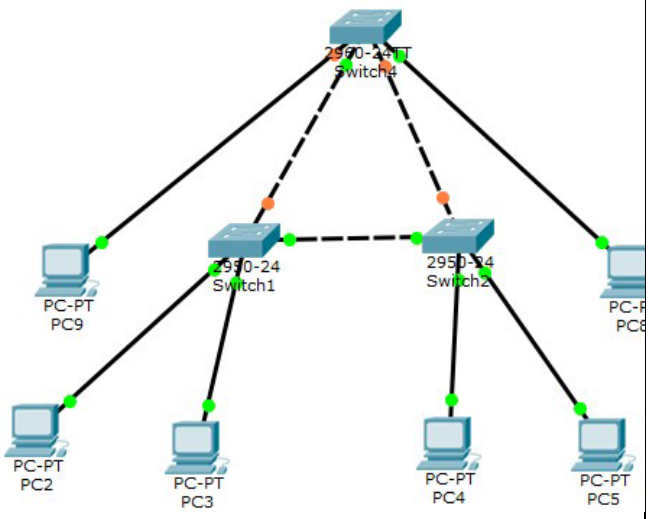
5. Перевірте всі з'єднання між комп'ютерами (команда *ping*).

6. У режимі симуляції надішліть запит (команда *ping*) з PC3 до PC5. Відстежуйте рух пакета ICMP.

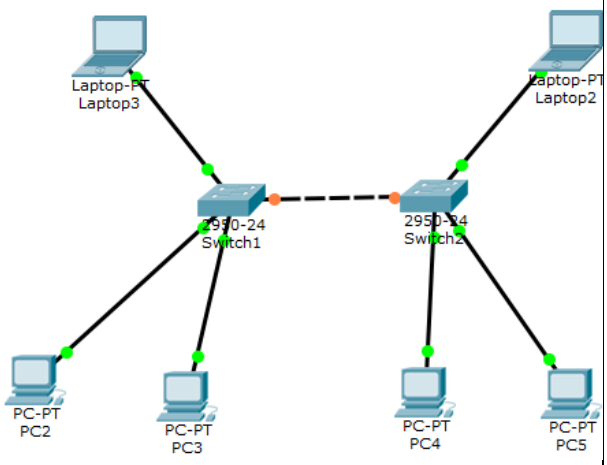
Таблиця 1.2. Параметри завдання топології мережі

Варіант 1	Варіант 2
	
Варіант 3	**Варіант 4**
	

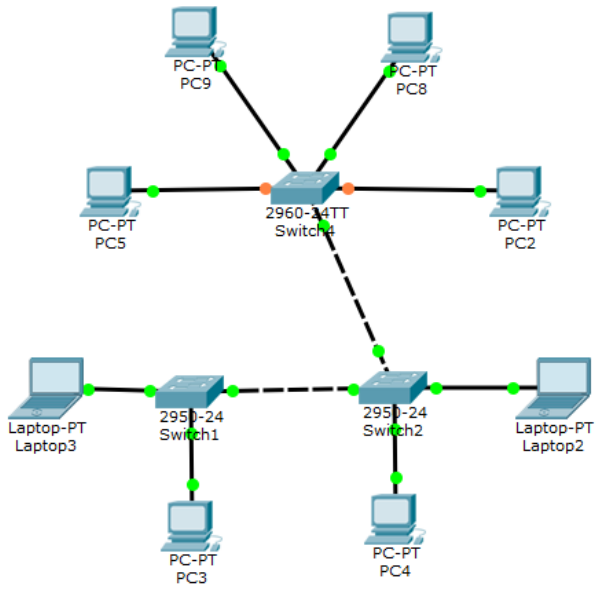
Варіант 5



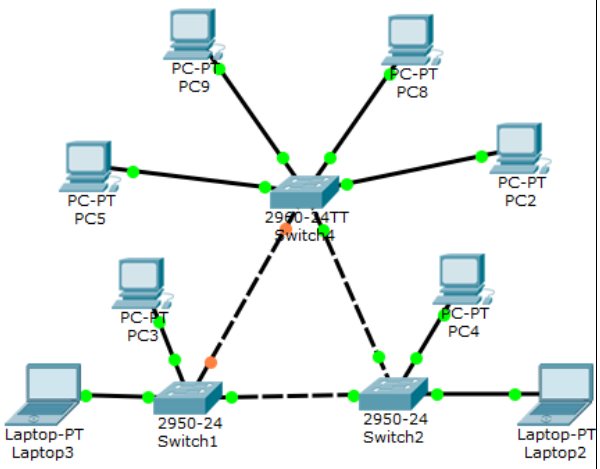
Варіант 6



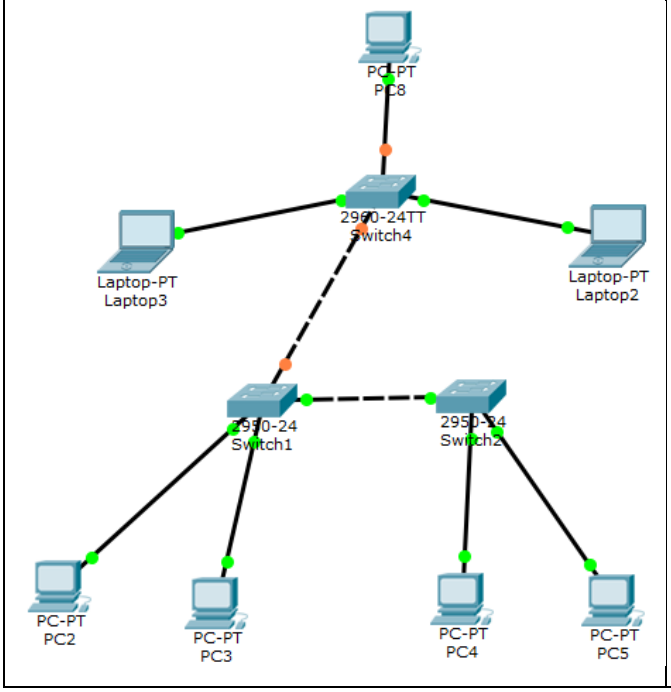
Варіант 7



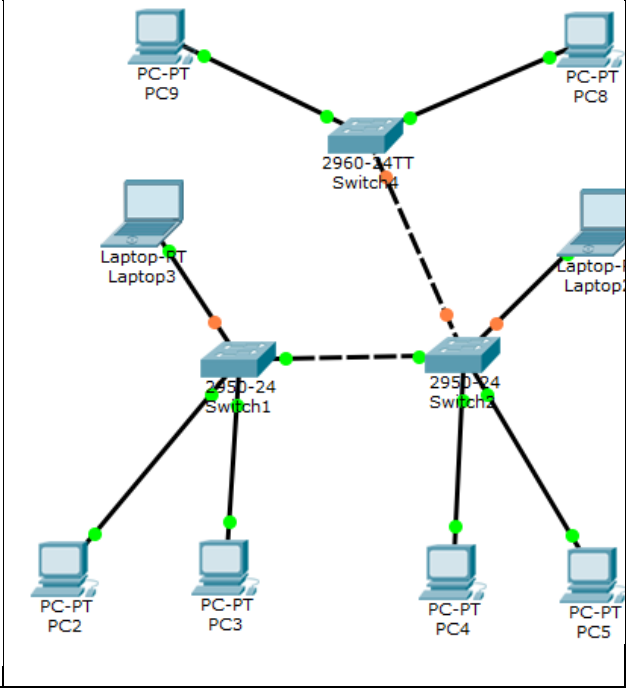
Варіант 8



Варіант 9



Варіант 10



Таблиця 1.3. Варіанти діапазонів адрес

№ варіанта	**1**	**2**	**3**	**4**	**5**
Діапазон адрес	112.168.5.15 112.168.5.25	12.208.6.15 12.208.6.25	144.18.9.15 144.18.9.25	133.73.9.60 133.73.9.69	12.208.6.15 12.208.6.25
№ варіанта	**6**	**7**	**8**	**9**	**10**
Діапазон адрес	13.18.0.45 13.18.0.55	152.164.8.75 152.164.8.85	122.8.85.45 122.8.85.55	155.38.0.0 155.38.0.9	212.28.68.15 212.28.68.25

Вимоги до звіту

1. Зображення топології мережі.
2. Скрін роботи команди ipconfig кожного кінцевого вузла.
3. Скрін роботи команди ping між усіма кінцевими вузлами.
4. Скрін з режиму симуляції шляху слідування одного запиту з PC3 до PC5.
5. Скрін кадру запиту після його отримання на PC5.
6. Загальні висновки по роботі.

Контрольні запитання

1. Яка максимальна кількість пристроїв у мережі підтримує пакет Packet Tracer?

2. Які типи мережевих пристроїв і з'єднань можна використовувати в Packet Tracer?

3. Як перейти до інтерфейсу командного рядка пристрою?

4. Як додати до топології та налаштувати новий пристрій?

5. Що таке комп'ютерна мережа?

6. Назвіть основні компоненти мережі?

7. Чим комутатор відрізняється від моста?

ЛАБОРАТОРНА РОБОТА № 2
ОБЧИСЛЕННЯ ПІДМЕРЕЖ IPv4

*Мета роботи: в*ивчити адресацію в IP-мережах, навчитись розраховувати адреси мереж і підмереж та визначати маску та адреси пристроїв для підмережі.

Теоретичні відомості

IP-адреса – унікальна мережева адреса вузла в комп'ютерній мережі, побудованій на протоколі IP. Адреса IPv4 складається з 32 бітів, які розділені на 4 частини по 8 біт відповідно (ці частини називаються октетами).

Приклади IP-адрес:

217.20.147.94 = 11011001.00010100.10010011.01011110

172.16.2.15 = 10101100.00010000.00000010.0000111

178.68.128.168 = 10110010.01000100.100000000.10101000

З цих 32 біт частина відноситься до адреси хоста, до якого належить до ця IP-адреса, а інша частина – я до адреси мережі, в якій цей хост знаходиться. Перша частина (зліва направо) IP-адреси позначає адресу мережі, а друга частина (решта бітів) – це адреса хоста. Щоб дізнатися, скільки біти відноситься до адреси мережі потрібно скористатись маскою мережі.

Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet – (Internet Network Information Center). Номер вузла в протоколі IP призначається незалежно від його локальної адреси.

Маска підмережі – бітова маска, яка визначає, яка частина IP-адреси мережного вузла відноситься до адреси мережі, а яка – до адреси самого вузла в цій мережі (при цьому, на відміну від IP-адреси, маска підмережі не є частиною IP-адреси пакету).

Маска мережі складається з 32 біт, але на відміну від IP-адреси, в ній одиниці та нулі не можуть «змішуватися». У мережевій масці біти рівні 1 визначають адресу мережі, а біти, що дорівнюють 0 зарезервовані для адрес хостів.

Приклади мережевих масок:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.0.0.0 = 11111111.000000000.000000000.000000000

255.255.240.0 = 11111111.11111111.11110000.00000000

255.255.255.128 = 111111111.111111111.111111111.10000000

Іноді маска мережі пишеться коротко у вигляді «префіксу маски». Число в префіксі означає кількість бітів, що відносяться до адреси мережі.

Приклад:

/16 = 11111111.11111111.000000000.00000000 = 255.255.0.0

/24 = 11111111.11111111.11111111.0000000 = 255.255.255.0

/26 = 11111111.11111111.11111111.11000000 = 255.255.255.192

Щоб дізнатися, яка частина IP-адреси належить до частини мережі, потрібно виконати бінарну логічну операцію AND(И) IP-адреси та маски мережі. Операція полягає в порівнянні двох бітів, і тільки в одному випадку бінарна операція дає одиницю на виході – у випадку порівняння двох одиниць. В інших випадках логічна операція «И» дає виході 0.

Результати порівняння логічної операції «И» порівняння двох бітів:

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

Кожна мережа IPv4 має широковещательный адресу (адреса для відправка даних на всі вузли в мережі, значення яких завжди дорівнює останній адресі в мережі) і адресу мережі (її значення завжди дорівнює першій адресі мережі).

Розрахувати кількість вузлів мережі можна проаналізувавши її маску. Якщо відняти кількість бітів, що використовуються мережевою частиною, то отримаємо кількість бітів, що використовуються для вузлів. Тоді

Кількість вузлів у підмережі $= 2^n - 2$,

де n – кількість вільних бітів (нулів) у хості, а «-2» - це вирахування адреси мережі та широковещательного адреса.

Кількість підмереж мережі розраховується за формулою

Кількість підмереж = 2^n,

де *n* – кількість зайнятих бітів на хост-частину.

Практична частина

Приклад 1. Визначте адресу мережі, якщо *IP-адреса* хоста *192.168.10.10 і маска підмережі 255.255.255.0.*

Переводимо IP-адресу з десяткової системи числення в двійкову:

192.168.10.10 = 110000000.10101000.00001010.0000101010

Перетворюємо маску мережі з десяткової системи числення на двійкову:

255.255.255.0 = 11111111.11111111.11111111.00000000

Додаємо IP-адресу з маскою за допомогою логічної операції «И».

1100000000.10101000.00001010.00001010 (IP-адреса)

И

111111111.11111111.11111111.00000000 (Маска)

=

1100000000.10101000.00001010.00000000 (мережева адреса)

переводимо адресу мережі з двійкової системи в десяткову та отримуємо 192.168.10.0 адреса мережі в десятковій формі з маскою 255.255.255.0.

Одиниці в масці вказують на частину мережевої адреси (1100000000.10101000.00001010), а нулі на частину адреси хоста (00001010).

Приклад 2. Визначте мережну адресу, якщо IP-адреса хоста 172.30.239.145, а маска підмережі 255.255.192.0.

Переводимо IP-адресу з десяткової системи числення в двійкову:

172.30.239.145 = 10110100.00100010.11101111.111011111

Перетворюємо маску мережі з десяткової системи числення на двійкову:

255.255.192.0 = 11111111.11111111.11000000.00000000

Складаємо IP-адресу з маскою за допомогою логічної операції «И».

10110100.00100010.11101111.11101111 (IP-адреса)

И

111111111.11111111.11000000.00000000 (маска)

=

10110100.00100010.11000000.000000000 (мережева адреса)

Переводимо адресу мережі з двійкової системи числення в десяткову і отримуємо *172.30.192.0* адресу мережі в десятковій формі з маскою *255.255.192.0.*

Проаналізувавши ці два приклади, можна побачити, що якщо маска підмережі має в октеті десяткове значення 255, результатом завжди буде вихідне значення цього октету. Якщо маска підмережі має в октеті десяткове значення 0, результат для цього октету завжди буде 0.

Приклад 3. Визначте максимальну кількість вузлів у мережі за допомогою маски *255.255.192.0.*

Оскільки маска підмережі становить *255.255.192.0,* префікс буде */18* (тобто 18 біт для мережевої адреси). IPv4-адреса містить 32 біти. Отже, для вузлової частини залишається *32 – 18 = 14 біт.* Виходячи з цього, максимальна кількість вузлів у даній мережі

$2^{14} – 2 = 16384 – 2 = 16382$ *вузли.*

Приклад 4. Визначте яку кількість підмереж із маскою *255.255.240.0* можна створити в мережі з маскою *255.255.0.0.*

Маска мережі 255.255.0.0 або /16

Маска підмережі 255.255.240.0 або /20

Кількість бітів у маски мережі – 16, а маски підмережі – 20. Різниця складає 4 біти. Таким чином, можна створити $2^4 = 16$ підмереж.

Завдання для індивідуальної роботи

1. Відповідно до варіанту (табл. 2.1.) за вказаною адресою IPv4 та маскою підмережі визначте такі параметри:

- адреси мереж А і Б;
- широковещательные адреси мереж А і Б;
- максимальну кількість вузлів у мережах А та Б;
- діапазон доступних адрес вузлів в мережах А і Б.
- кількість можливих підмереж Б в мережі А.

Таблиця 2.1. Параметри завдання

Номер варіанту	IP-адреса	Маска мережі А	Маска мережі Б
1	128.107.0.55	255.255.0.0	255.255.255.0
2	192.135.250.180	255.255.255.0	255.255.255.248
3	10.101.99.228	255.0.0.0	255.255.128.0
4	91.19.35.13	255.255.224.0	255.255.255.224
5	190.15.157.6	255.0.0.0	255.255.192.0
6	65.16.16.182	255.255.0.0	255.255.224.0
7	81.16.190.64	255.255.128.0	255.255.255.0
8	125.18.19.16	255.255.240.0	255.255.255.0
9	196.168.26	255.255.248.0	255.255.255.248
10	156.56.3.64	255.192.0.0	255.255.0.0

2. Заповніть таблицю 2.2.

Таблиця 2.2. Результати розрахунків

Параметри	Мережа А	Мережа Б
Маска мережі		
Мережева адреса		
Адреса трансляції мережі		
IPv4-адреса першого вузла в мережі		
IPv4-адреса останнього вузла в мережі		
Кількість вузлів в мережі		
Кількість можливих підмереж В у мережі А		

3. Створіть в середовищі Packet Tracer мережу А що складається з трьох стаціонарних ПК, ноутбуку та одного комутатора Switch 2960 25TT (див. рис. 2.1).

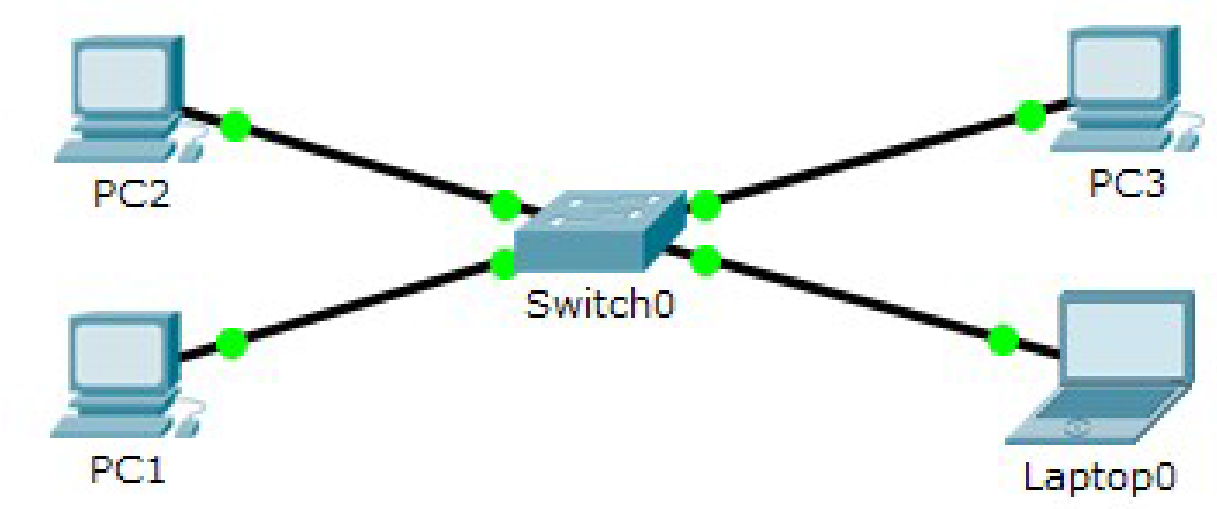


Рис. 2.1. Топологія мережі

4. Всім кінцевим вузлам мережі А задайте IP-адреси:

- PC1 – третя адреса мережі А;

- PC2 – четверта адреса мережі А;

- PC3 – п’ята адреса мережі А.

- leptop1 – остання адреса мережі А.

5. Встановіть відповідні мережеві маски для всіх кінцевих вузлів.

6. Перевірте параметри кожного кінцевого вузла за допомогою команди *ipconfig.*

7. Перевірте роботоздатність мережі за допомогою команди *ping.*

Вимоги до звіту

1. Розрахунки відповідно до п. 1.1... 1.5.

2. Заповнена таблиця 2.2.

3. Скрін топології мережі.

4. Скрін роботи команди *ipconfig* кожного вузла.

5. Скрін роботи команди *ping* між усіма вузлами.

6. Загальні висновки по роботі.

Контрольні запитання

1. Що таке 1 байт? Чому він рівний?

2. Яка довжина адреси IPv4? Ipv6?

3. Що таке маска мережі?

4. Як визначити максимальну кількість вузлів у мережі?

5. Як визначити кількість підмереж у мережі?

6. Навіщо потрібен широковещательный трансляції?

ЛАБОРАТОРНА РОБОТА № 3
РОЗДІЛ МЕРЕЖІ ПІДМЕРЕЖІ ОДНАКОВОЇ ДОВЖИНИ

Мета роботи: навчитися працювати з підмережами, ділити мережу на рівні підмережі та ефективно використовувати адресний простір мережі.

Теоретичні відомості

Безкласова адресація CIDR (англ. Classless Inter-Domain Routing) – метод IP-адресації, що дозволяє гнучко керувати простором IP-адрес, не використовуючи жорстку систему класової адресації. Використання цього методу дозволяє економно використовувати обмежений ресурс IP-адрес, оскільки можливе застосування різних масок підмереж до різних підмереж.

Підмережі дають змогу створювати кілька логічних мереж у межах однієї мережі класу A, B або C.

Спочатку метод CIDR розглядався як спосіб розподілу IP-адрес між клієнтами інтернет-провайдером у вигляді діапазонів IP-адрес (так звані блоки), а не виділення адреси певного класу. Як правило, інтернет-провайдер виділяє своїм клієнтам адрес певних класів, що призводить до деякого профіциту в одному місці і до дефіциту в іншому. Звертаючись до технології CIDR, провайдери змогли «нарізати» блоки з виділеного їм адресного діапазону, що максимально задовольнлять вимоги кожного клієнта , залишаючи, в той де час, можливість його майбутнього безпроблемного росту.

Кожен канал передачі даних у мережі повинен мати унікальний ідентифікатор мережі, при цьому кожен вузол у каналі має бути членом однієї і тієї ж мережі. Якщо розбити основну мережу на невеликі підмережі, то це створить мережу взаємопов'язаних підмереж. Кожен канал передачі даних в цій мережі матиме унікальний ідентифікатор мережі або підмережі. Будь-який пристрій або шлюз, що з'єднує *n* мереж або підмереж, повинен мати *n* унікальних IP-адрес – по одній для кожного з взаємопов'язаних мереж або підмереж.

Розділення мережі на підмережі виконується шляхом розширення маски підмережі за рахунок бітів, які визначають ідентифікатор вузла в адресі. Це дозволяє створювати ідентифікатор підмережі.

Практична частина

Приклад 1. Нехай задана мережа *74.126.205.0* з маскою мережі *255.255.255.0.* Потрібно створити 4 підмережі.

Обраховуємо кількість бітів у основній масці, необхідних для створення підмереж. Оскільки потрібно створити 4 підмережі, тобто 2^2, то це означає, що буде запозичено 2 біти в основної маски мережі:

74.126.205.0 - 01001010.01111110.11001101.00000000

*255.255.255.192 - 11111111.11111111.11111111.**11000000***

Розширення маски до значення 255.255.255.192 відбулося за рахунок двох бітів вихідної частини вузла в адресі, які були використані для створення підмереж. Ідентифікатор вузла тепер містить шість бітів, що залишилися, тому кожна підмережа може містити 64 (2^6) адрес вузлів, 62 з яких фактично можуть бути віднесені до пристроїв, оскільки ідентифікатори вузлів не можуть складатися лише з одиниць або нулів. З урахуванням всіх перерахованих вище факторів створені підмережі представлені в таблиці. 3.1.

Таблиця 3.1. Представлення мережі в десяткових та двійкових системах числення

Підмережа (10)	**Підмережа (2)**
74.126.205.0	01001010.01111110.11001101. **00**000000
74.126.205.64	01001010.01111110.11001101. **01**000000
74.126.205.192	01001010.01111110.11001101. **11**000000
74.126.205.128	01001010.01111110.11001101. **10**000000
Маска підмережі (10)	**Маска підмережі (2)**
255.255.255.192	11111111.11111111.11111111.11000000

Технологія розподілу на підмережі в цьому прикладі дозволяє створити чотири підмережі, і мережа потім буде мати вигляд як на рис. 3.1.

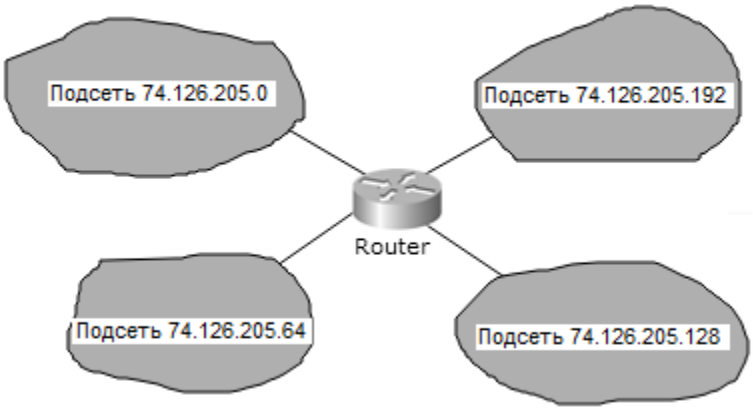


Рис. 3.1. Логічне представлення розбиття мережі методом CIDR

Кожна підмережа може підтримувати до 62 адрес вузлів. З цього можна зробити висновок, що чим більше бітів використовується для маски підмережі, тим більше підмереж доступно. Однак чим більше доступно підмереж, чим менше хост-адрес, доступних у кожній підмережі.

Перевіримо роботоздатність цієї мережі. Для цього:

1. Створимо в середовищі Packet Tracer топологію, що містить один роутер Generic Router-PT-Empty (Router1), чотири комутатори Switch 2960-24TT (Switch0 – Switch3) и 8 ПК (PC0 – PC7).

2. Додамо до маршрутизатора чотири Gigabit Ethernet-модулі PT-ROUTER-NM-1CGE в роутер. Для цього відкриваємо властивості Router1, на вкладці Physical на моделі роутера натискаємо кнопку живлення для вимкнення, вибираємо вказаний модуль підключення, встановлюємо чотири таких модулі в вільні слоти та включаємо роутер.

3. Комп'ютери з комутаторами об’єднаємо кученою парою. Порти підключення – FastEthernet. Комутатори з роутером також будуть об’єднаємо кученою пара. Порти з'єднання – GigabitEthernet. Топологія моделі мережі представлена на рис. 3.2.

4. Збережемо створену топологію.

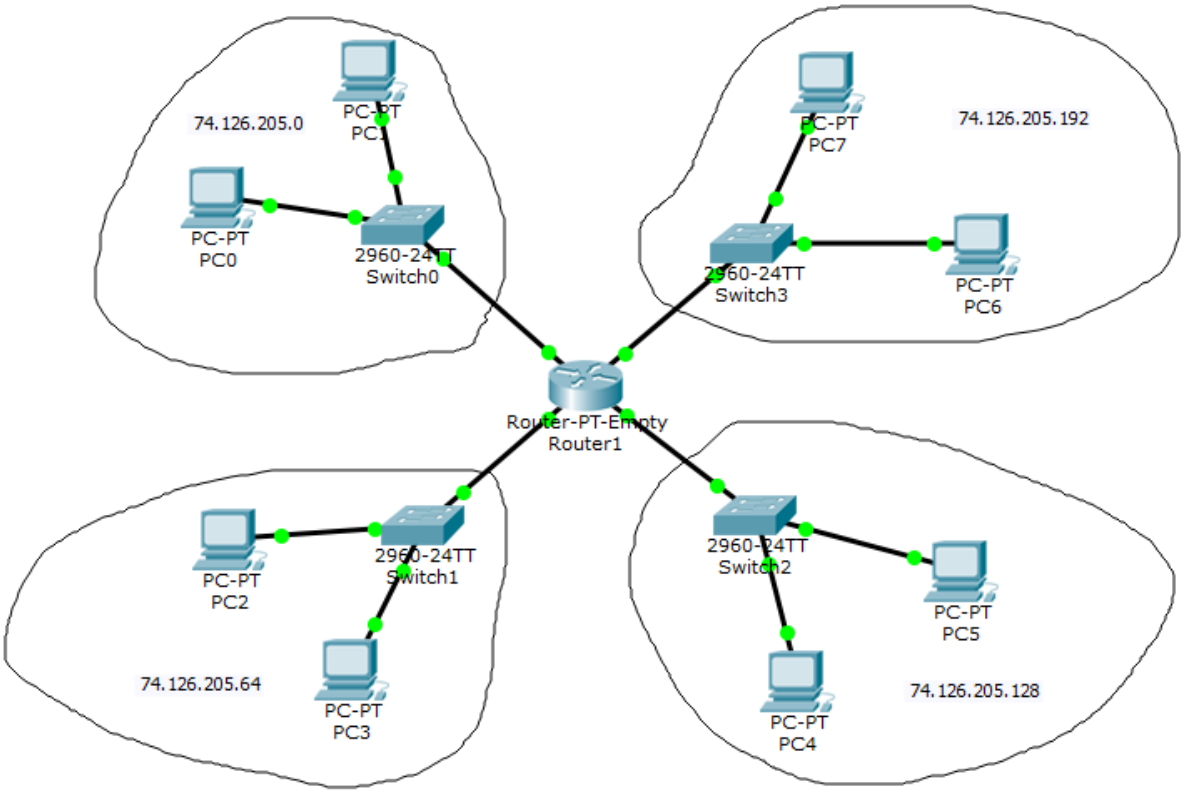


Рис. 3.2. Топологія мережі

5. Налаштуйте елементів мережі. У кожній підмережі ми зарезервуємо для маршрутизатора першу доступну IP-адресу, а комп’ютерам присвоїмо другу та наступні адреси. Маска мережі для всіх пристроїв – *255.255.255.192.*

6. Щоб налаштувати PC0, який належить до першої підмережі, відкриємо його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адрес *Static* у полі *IP Address* введемо другу доступну адресу підмережі – *74.126.205.2*, в поле *Subnet Mask* – маску мережі *255.255.255.192*, а в полі *Default Gateway* (шлюз за замовчуванням) вкажемо першу доступну IP-адресу підмережі, зарезервовану для роутера – *74.126.205.1*. Комутатор PC1 налаштовується аналогічно, але в *IP Address* вводимо останню доступну адресу підмережі – *74.126.205.62.*

7. Задаємо IP-адресу для другої підмережі: комп’ютер PC2 – *74.126.205.66*, комп’ютер PC3 – *74.126.205.126*, шлюз – *74.126.205.65*; для третьої підмережі: комп'ютер PC4 – *74.126.205.130*, комп'ютер PC5 – *74.126.205.190*, шлюз –

74.126.205.129; комп'ютер PC6 – *74.126.205.194*, комп’ютер PC7 – *74.126.205.254*, шлюз – *74.126.205.193*.

8. Виконаємо настройку роутера, яка в нашому випадку буде заключатись в окремому мережевому налаштування кожного з Gigabit Ethernet-модулів, до яких підключені комутатори підмереж. Відкриємо властивості маршрутизатора та перейдем до вкладки *Config* та в підменю *INTERFACE* виберемо модуль GigabitEthernet0/0, до якого підключено перший комутатор підмережі *74.126.205.0*. У поле *IP Address* введіть першу зарезервовану IP-адресу підмережі – *74.126.205.1*, а в поле *Subnet Mask* – маску мережі *255.255.255.192*. Потім увімкніть даний модуль – для *Port Status* встановимо значення On. Інші три модулі налаштовані аналогічно – в полі *IP Address* вказуємо першу зарезервовану IP-адресу підмережі, комутатор якої підключений до модуля.

9. Перевіримо роботоздатність мережі. Наприклад, зайдемо на комп'ютера PC0 і пропінгуємо комп'ютер PC7. Для цього відкриємо властивості комп'ютера PC0, на вкладці *Desktop* виберемо *Command Promt* і у вікні, що відкриється в командному рядку введемо команду ping та IP-адресу комп'ютера PC7.

Нижче наведено результати команди *ping:*

PC>ping 74.126.205.254

Pinging 74.126.205.254 with 32 bytes of data:

Reply from 74.126.205.254: bytes=32 time=0ms TTL=127

Reply from 74.126.205.254: bytes=32 time=0ms TTL=127

Reply from 74.126.205.254: bytes=32 time=0ms TTL=127

Reply from 74.126.205.254: bytes=32 time=0ms TTL=127

Ping statistics for 74.126.205.254:

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

Approximate round trip times in milli-seconds:

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

Це підтверджує правильність мережевих налаштувань пристроїв та загальну роботоздатність мережі.

Завдання для індивідуальної роботи

1. Відповідно до варіанту (табл. 3.2) за вказаною IP-адресою та маскою розділіть задану мережу на чотири рівні підмережі.

Таблиця 3.2. Параметри завдання

Номер варіанта	**Адреса мережі**	**Маска мережі**
1	129.138.60.0	255.255.252.0
2	191.197.206.0	255.255.254.0
3	17.53.208.0	255.255.248.0
4	144.29.236.0	255.255.252.0
5	48.185.104.0	255.255.248.0
6	109.88.38.0	255.255.254.0
7	13.140.208.0	255.255.240.0
8	78.97.205.0	255.255.255.0
9	192.199.140.0	255.255.252.0
10	87.247.176.0	255.255.240.0

2. Виконайте розрахунки та заповніть таблицю 3.3.

Таблиця 3.3. Результати розрахунків

Ім'я підмережі	**А**	**Б**	**В**	**Г**
Мережева адреса підмережі				
Маска підмережі				
Префікс маски підмережі				
Широковещательна адреса підмережі				

Доступний діапазон адрес вузлів в підмережі				
Кількість вузлів у підмережі				

3. В середовищі Packet Tracer створіть топологію, аналогічну тій, що описана в прикладі (рис. 3.2).

4. Всім кінцевим вузлам задайте IP-адреси та маски із описаних раніше підмереж (А, Б, В, Г):

- всім інтерфейсам маршрутизатора задати перші допустимі ІП-адреси підмережі;

- першим вузлам в підмережі задати другі допустимі IP-адреси;

- другим вузлам задати останні допустимі IP-адреси.

5. Перевірте параметри кожного цільового вузла за допомогою команди ipconfig.

6. Перевірте стан здоров'я мережі за допомогою команди ping.

Вимоги до звіту

1. Розрахунок знаходження параметрів всіх підмереж.

2. Скрін топології мережі.

3. Скрін роботи команди ipconfig для кожного кінцевого вузла.

4. Скрін роботи команди ping між першим і рештою вузлів.

5. Загальні висновки по роботі.

Контрольні запитання

1. Навіщо потрібна мережева адреса?

2. Що таке CIDR?

3. У чому різниця між безкласовою та класовою адресою?

4. Як розподіляються адреса хоста та адреса підмережі в IP-адресі?

ЛАБОРАТОРНА РОБОТА № 4
РОЗДІЛЕННЯ МЕРЕЖІ НА ПІДМЕРЕЖІ ЗМІННОЇ ДОВЖИНИ

Мета роботи: навчитися працювати з підмережами, ділити мережу на підмережі змінної довжини та ефективно використовувати адресний простір мережі.

Коротка інформація з теорії

Для ефективного використання адресного простору існує метод *маски підмережі змінної довжини* (анг. Variable Length Subnet Masking – VLSM). Маски підмережі змінної довжини дають можливість створення декількох масок підмережі в одній мережі, можливість розбивати на підмережі групи IP-адрес. Методи CIDR і VLSM дозволяють рекурсивно ділити частини адресного простору на дрібніші частки. Основна відмінність між ними полягає в тому, що при використанні маски підмережі змінної довжини рекурсія виконується на адресному просторі, що виділений організації раніше. При цьому схема поділу адресного простору прихована в середині організації.

В технології CIDR розподіл на підмережі у всіх підмережах використовується одна й та ж маска підмережі. Це означає, що кожна підмережа містить однакову кількість доступних адрес хостів. Іноді це може знадобитися, але в більшості випадків використання однакової маски підмережі для всіх підмереж призводять до неекономічного розподілу адресного простору.

VLSM дозволяє використовувати різні маски для кожної підмережі, що дає можливість більш раціонально розподіляти адресний простір.

Наприклад, припустимо, що існує мережа класу С з адресою 192.214.11.0, і її потрібно розділити на три підмережі. В одній підмережі повинно бути близько 100 вузлів, а дві інші – по 50. Виключаючи дві адреси 0 (номер мережі) та 255 (широковещательный адрес для сети), теоретично для мережі класу С доступно 256 хост-адрес, тобто від 192.214.11.0 до 192.214.11.255. Очевидно, що розбити таку мережу на підмережі з заданою вище кількістю вузлів, без використання VLSM, неможливо.

Щоб визначити параметри підмережі в мережі 192.214.11.0, спочатку потрібно визначити маску мережі, яка для звичайної мережі класу С буде мати

вигляд 255.255.255.0. Для поділу мережі класу С з адресою 192.214.11.0 на підмережі можна використати кілька масок вид 255.255.255.X. Маска, починаючи з найвищого (лівого) біта, повинна мати неперервний ряд одиниць і закінчуються нулями.

До VLSM мережі, як правило, ділилися лише простими масками. В цьому випадку був вибір: застосувати маску 255.255.255.128 і розділити адресний простір дві підмережі по 128 вузлів кожному або розбити його маскою 255.255.255.192 на чотирьох підмережі по 64 хости в кожній. Однак жодна з цих процедури не відповідають вимогам отримати сегменти мережі розміром 100 вузлів і ще два 50-вузлових сегмента кожен.

Виконати поставлене завдання можна використавши маски різної довжини. По-перше, мережу 192.214.11.0 на дві підмережі маскою 255.255.255.128. Отримаємо дві підмережі по 128 вузлів в кожній. Ці підмережі будуть представлені адресами 192.214.11.0 (.0 – .127) і 192.214.11.128 (.128 – .255). Потім другу підмережу з адресою 192.214.11.128 розділимо ще на дві підмережі за допомогою маски 255.255.255.192 – отримаємо дві підмережі з 64 адресами в кожній: підмережі 192.214.11.128 (адреси від .128 до 191) та 192.214.11.192 (адреси від .192 до 255).

Надивлячись на те, що при використанні VLSM довжину маски можна довільно змінювати, існує одне обмеженні: ви максимальна довжина маски – 30 од. Це обмеження пов'язано з тим, що при довжині маски 31 біт на номер вузла залишається один розряд. З допомогою одного розряду можна пронумерувати лише два вузли. Але стандарт передбачає, що дві адреси завжди зайнятий – це номер мережі (підмережі) і широковещательна адреса.

Практична частина

Нехай задана мережа 74.126.205.0 з мережевою маскою 255.255.255.0. Розробимо схему поділу цієї мережі на 4 підмережі за допомогою VLSM: підмережа А повинна містити 14 вузлів, підмережа Б – 28 вузлів, підмережа В – 15 вузлів, підмережа Г – 5 вузлів.

Визначимо, яку маску підмережі варто використати щоб отримати потрібну кількість вузлів.

Мережа А: має вмістити 14 вузлів. Найближчий підходить значення $2^n = 16$, це означає що кількість бітів вузлової частини $n=4$, кількість бітів для ідентифікатора підмережі становитимуть $8 - 4 = 4$ біти. Отже, маска цієї підмережі буде *255.255.255.240* або */28.*

Мережа Б: повинна вмістити 28 вузлів. Найбільше підходить значення $2^n = 32$, значить кількість бітів вузлової частини $n = 5$, а кількість бітів для ідентифікатора підмережі становитимуть $8 - 5 = 3$ *біти*. Отже, маска цієї підмережі буде *255.255.255.224* або */27.*

Мережа В: повинна мати 15 вузлів. Найбільше підходить значення $2^n = 16$, але тому, що кожна мережа повинна мати широковещательний адрес та адресу підмережі, то 16 для цієї підмережі буде недостатньо. Тому вибираємо $2^n = 32$. Кількість бітів частини вузла n = 5, а кількість бітів для ідентифікатора підмережі становитиме 8 – 5 = 3 біти. Таким чином, маска цієї підмережі буде 255.255.255.224 або /27.

Мережа Г: має містити 5 вузлів. Найближчий підходить значення $2^n = 8$, значить кількість бітів частини вузла n = 3, а кількість бітів для ідентифікатора підмережі становитиме 8 – 3 = 5 біт. Тому маска цієї підмережі буде 255.255.255.248 або /29.

VLSM-розбиття на підмережі схоже на традиційне в тому, що в ньому, для створення підмережі, запозичаються біти. Формули обчислення кількості можливих підмереж та кількості вузлів в кожній підмережі також можуть застосовуватись. Різниця лише в тому, що розбиття на підмережі виконується в декілька етапів. При використанні VLSM мережа спочатку розбивається на підмережі, які, в свою чергу, знову діляться на підмережі. Цей процес може повторитися багато разів для створення підмереж різних розмірів. Для початку відсортуємо підмережі, які потрібно створити, за кількістю доступних вузлів:

- мережа Б: 32 вузли;
- мережа В: 32 вузли;

- мережа А: 16 вузлів;
- мережа Г: 8 вузлів.

Графічне представлення розбиття на підмережі методом VLSM показано на рис. 4.1.

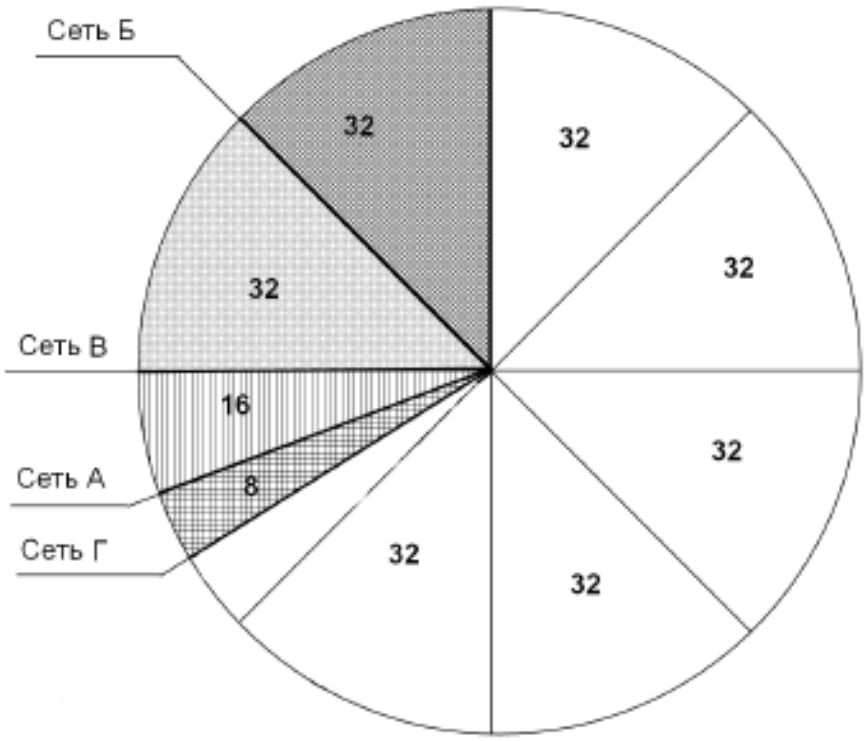


Рис. 4.1. Графічне представлення підмережі методом VLSM

Далі розіб'ємо задану мережу (в якій доступно 256 адрес) по 32 адреси (найбільша підмережа, яку ви шукаєте). У отриманих підмережах кількість бітів ідентифікатора підмережі – 3, тому нові підмережі будуть виглядати так:

*01001010.01111110.11001101.**000**00000*

*01001010.01111110.11001101.**001**00000*

*01001010.01111110.11001101.**010**00000*

*01001010.01111110.11001101.**011**00000*

*01001010.01111110.11001101.**100**00000*

*01001010.01111110.11001101.**101**00000*

*01001010.01111110.11001101.**110**00000*

*01001010.01111110.11001101.**111**00000*

Нам потрібні тільки перші дві підмережі (для Б і В). Маска у цих підмереж буде *255.255.255.224* або */27*.

Щоб визначити наступної підмережі, розділимо мережу 01001010.01111110.11001101.**010**00000 навпіл (тобто запозичаємо ще один біт для ідентифікатора підмережі).

Ми отримуємо дві мережі:

*01001010.01111110.11001101.**0100**0000*

*01001010.01111110.11001101.**0101**0000*

Перша з цих підмереж призначена для мережі А маскою /28. Другу – ще раз ділимо навпіл, тобто запозичаємо ще один біт у ідентифікатора підмережі. Отримаємо ще дві мережі:

*01001010.01111110.11001101.**01010**000*

*01001010.01111110.11001101.**01011**000*

Перший з них відповідає мережі Г з маскою /29.

Результат переведення значень знайдених підмереж в десяткову форму представлений в таблиці. 4.1.

Таблиця 4.1. Параметри підмережі

Ім'я	**Підмережа (2)**	**Підмережа (10)**	**Маска (10)**
Б	01001010.01111110.11001101. **000**00000	74.126.205.0	255.255.255.224
В	01001010.01111110.11001101. **001**00000	74.126.205.32	255.255.255.224
А	01001010.01111110.11001101. **0100**0000	74.126.205.6	255.255.255.240
Г	01001010.01111110.11001101. **01010**000	74.126.205.80	255.255.255.248

Для визначення діапазону доступних у підмережі вузлів необхідно спочатку додати номера підмережі додати одиницю (це буде адреса першого вузла), а

потім до номера підмережі додати кількість доступних адрес (це буде адреса останнього вузла). Результати представлені в таблиці. 4.2.

Таблиця 4.2. Діапазон доступних вузлів

Ім'я	**Підмережа**	**Маска**	**Діапазон доступних адрес**
Б	74.126.205.0	255.255.255.224	74.126.205.1 - 74.126.205.30
В	126.205.32	255.255.255.224	74.126.205.33 - 74.126.205.62
А	74.126.205.64	255.255.255.240	74.126.205.65 - 74.126.205.78
Г	74.126.205.80	255.255.255.248	126.205.81 - 74.126.205.86

Метод VLSM розподілу на підмережі в цьому прикладі дозволяє створити чотири підмережі з заданою кількістю вузлів у кожній (рисунок 4.2). Створення мережі з чотирьох підмереж і настроювання мережевих компонент в Packet Tracer описаний в попередній роботі.

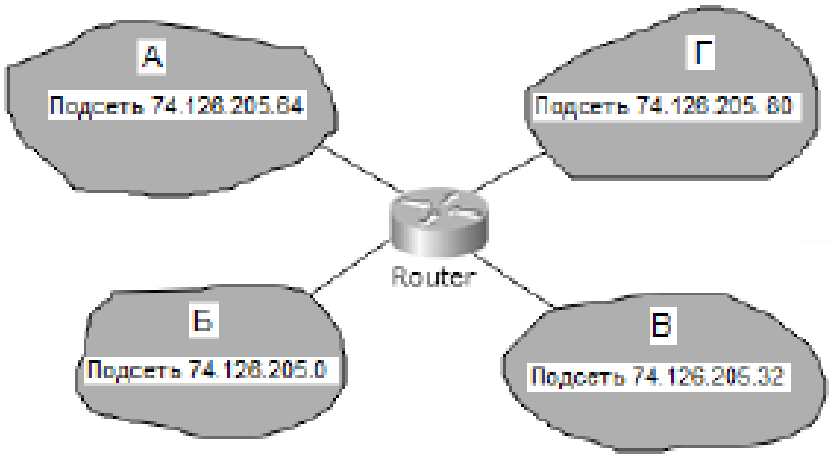


Рис. 4.2. Логічне представлення розбиття мережі методом VLSM

Завдання для індивідуальної роботи

1. Відповідно до варіанту (табл. 4.3) за вказаною IP-адресою та маскою підмережі розділіть задану мережу на чотири підмережі враховуючи кількість вузлів в кожній з допомогою методу VLSM.

			Кількість вузлів в підмережі

Номер варіанту	Адреса мережі	Маска мережі	А	Б	В	Г
1	126.198.0.0	255.254.0.0	155	255	86	161
2	192.200.0.0	255.248.0.0	72	104	130	109
3	10.192.0.0	255.252.0.0	73	55	133	106
4	156.168.0.0	255.248.0.0	92	180	105	102
5	81.176.0.0	255.248.0.0	89	158	171	60
6	91.184.0.0	255.252.0.0	80	100	64	150
7	190.128.0.0	255.254.0.0	09	65	155	62
8	65.48.0.0	255.248.0.0	120	132	90	146
9	125.192.0.0	255.240.0.0	64	95	59	181
10	14.160.0.0	255.224.0.0	50	258	140	107

2. Виконати розрахунки та заповнити таблицю 4.4.

Таблиця 4.4. Результати розрахунку

Ім'я підмережі				
Мережева адреса підмережі				
Маска підмережі				
Префікс маски підмережі				
Широковещательный адрес подсети				
Діапазон доступних адрес вузлів в підмережі				
Кількість вузлів у підмережі				

3. Створіть топологію мережі в середовищі Packet Tracer.

4. Для всіх кінцевих вузлів задайте IP-адреси та маски із обчислених раніше підмереж (A, B, C, D):

a) для всіх інтерфейсів маршрутизатора задати перші допустимі IP-адреси підмережі;

b) першім вузлам в підмережі присвойте другі допустимі IP-адреси;

c) другим вузлам присвойте останні допустимі IP-адреси.

5. Перевірте параметри кожного вузла за допомогою команди ipconfig.

6. Перевірте роботоздатність мережі за допомогою команди ping.

Вимоги до звіту

1. Обчисліть параметри всіх підмереж.

2. Скрін топології мережі.

3. Скрін виконання команди ipconfig кожного цільового вузла.

4. Скрін виконання команди ping між першим і рештою цільових вузлів.

5. Загальні висновки по роботі.

Контрольні запитання

1. Які форми запису масок ви знаєте?

2. Що таке метод VLSM?

3. Чи можна використовувати VLSM у локальній комп'ютерній мережі?

4. Яка максимальна довжина маски при використанні VLSM?

5. Як VLSM сприяє економному використанню адресного Простір?

ЛАБОРАТОРНА РОБОТА № 5
НАСТРОЮВАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ В ПРОГРАМІ CISCO PACKET TRACER

Мета роботи: навчитися організувати бездротові мережі, налаштовувати Wi-Fi-точки доступу через веб-інтерфейс та кінцеві вузли мережі.

Теоретичні відомості

Бездротова комп'ютерна мережа – комп'ютерна мережа без використання кабельної проводки, повністю відповідає стандартам для звичайних проводових мереж (наприклад, Ethernet). В якості носія інформації виступають радіохвилі СВЧ-діапазону. Зараз для організації бездротових мереж широко використовується Стандарт IEEE 802.11, більш відомий як Wi-Fi.

Wi-Fi – це бренд Wi-Fi Alliance для бездротових мереж на основі стандарту IEEE 802.11. Під абревіатурою Wi-Fi (від англ. Wireless Fidelity, що можна перекласти як «бездротова точність» або «бездротова якість») в даний час розвивається ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах.

Як правило, мережна схема Wi-Fi містить принаймні одну точку доступу і не менше одного клієнта. Також є можливість підключити двох клієнтів в режимі точка-точка, коли точка доступу не використовується, і клієнти підключаються, а клієнти об’єднуються через мережеві адаптери «напряму». Точка доступу передає свій ідентифікатор мережі з допомогою спеціальних сигнальних пакетів зі швидкістю 0,1 Мбіт/с кожні 100 мс. Таким чином, 0,1 Мбіт/с – найменша швидкість передачі даних для Wi-Fi. Точка доступу організована за допомогою Wi-Fi-роутера.

Wi-Fi-роутер – це пристрій, який підключається до мережі Інтернет за допомогою кабелю та передає з'єднання на інші пристрої, наприклад, ноутбук або смартфон.

Методи обмеженого доступу в Wi-Fi-мережах.

1. *Фільтрація MAC-адрес*. Цей метод не входить до стандарту IEEE 802.11. Фільтрацію можна проводити трьома способами:

- точка доступу дозволяє отримати доступ до станцій з будь-якою MAC-адресою;

- точка доступу дозволяє отримати доступ лише до MAC-адреси, яка знаходить в довірчому списку;

- точка доступу забороняє доступ станціям, MAC-адреси яких знаходяться в «чорному списку»;

Більш надійним з точки зору безпеки є другий варіант, хоча він не призначений для підміни MAC-адреси.

2. *Режим прихованого ідентифікатора SSID* (від англ. Service Set IDentifier). Для своєї ідентифікації точка доступу періодично надсилає кадри-маячки. Кожен такий кадр містить службову інформацію для підключення і, зокрема, присутній SSID (ідентифікатор безпроводової мережі). У випадку, якщо прихованого SSID це поле порожнє, тобто неможливо виявити вашу бездротову мережу та не можна до неї підключитись.

Методи шифрування в Wi-Fi-мережах.

1. *WEP-шифрування* (від англ Wired Equivalent Privacy). Використовує симетричний потоковий шифр RC4 (англ. Rivest Cipher 4), який функціонує досить швидко. На сьогоднішній день WEP і RC4 не вважаються криптостійкими. Основними недоліками є:

- використання для шифрування паролю, який задається користувачем;

- недостатня довжина ключа шифрування;

- використання функції CRC32 для контролю цілісності пакетів;

- повторне використання векторів ініціалізації тощо.

2. *TKIP-шифрування* (англ. Temporal Key Integrity Protocol) також використовує симетричний потоковий шифр RC4, що не робить цей метод більш криптостійким.

3. *CKIP-шифрування* (англ. Cisco Key Integrity Protocol).. Має схожість з протоколом TKIP. Створений компанією Cisco. Використовує протокол CMIC (англ. Cisco Message Integrity Check) для перевірки цілісності повідомлень.

4. *Шифрування WPA.* Замість вразливого RC4 він використовує криптографічно сильний алгоритм шифрування AES. Існує два режими:

- Pre-Shared Key (WPA-PSK) – кожен вузол вводить пароль для доступу до мережі;

- Enterprise – верифікація здійснюється серверами RADIUS.

5. *WPA2-шифрування* (IEEE 802.11i). Прийняте в 2004 році, а з 2006 WPA2 підтримує все виготовлене Wi-Fi обладнання. У цьому протоколі використовує RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Основою є алгоритм AES. Для сімісності зі старим обладнанням існує підтримка TKIP і EAP (англ. Extensible Authentication Protocol) з деякими його доповненнями. Як і в WPA – два режими роботи: Pre-Shared Key и Enterprise.

WPA і WPA2 мають наступні переваги:

- ключі шифрування генеруються під час з'єднання, а не розподіляються статично;

- для контролю цілісності повідомлень використовується алгоритм Michael;

- використовується набагато довший вектор ініціалізації.

Стандарти Wi-Fi. Термін Wi-Fi не є лише технічним. Він активно використовується користувачами бездротових мереж групи стандартів IEEE 802.11. Однак термін IEEE 802.11 та англійська літера, що характеризує певну фізичну специфікацію. На даний момент найбільш поширеними є стандарти Wi-Fi, перелічені в таблиці. 5.1.

Таблиця 5.1. Стандарти Wi-Fi

Стандарт	**Рік**	**Частота, ГГц**	**Швидкість, Мбит/с (середня / максимальна)**	**Радіус дії, м (в приміщенні / на відкритому просторі)**
802.11	1997	2,4	0,9/2,0	20/100
802.11a	1999	5.0	23/54	35/120
802.11b	1999	2,4	4,3/11	38/140
802.11г	2003	2,4	19/54	38/140

802.11n	2009	5,0	74/248	70/250
802.11y	2008	3,7	23/54	50/5000

Практична частина

1. Додайте на робочу область програми Packet Tracer стаціонарний комп’ютер та Wi-Fi роутер WRT300N. Комп’ютер з роутером об’єднайте витою парою. Порт підключення комп'ютера FastEthernet, роутера – Ethernet.

2. Стандартна IP-адреса сучасних бездротових маршрутизаторів – *192.168.0.1* з маскою – *255.255.255.0*. Призначені адресу та маску роутера можна перевірити у вікні властивостей пристрою на вкладці *Config* в підменю *LAN*.

3. Для того щоб підключити комп'ютер до маршрутизатора у вікні властивостей комп'ютера на вкладці *Desktop* виберіть *IP Configuration.* Для автоматичного отримання IP-адреси перемикач способу призначення адреси встановимо в положення DHCP. Через деякий час у відповідних полях з'явиться IP-адреса комп'ютера, маска мережі та IP-адреса шлюзу.

4. Щоб відобразити настройки мережі, відкрийте на комп’ютері командний рядок (*Desktop/Command Promt*) і введіть команду *ipconfig /all.* Результат виконання команди буде мати вигляд:

PC>ipconfig /all

FastEthernet0 Connection:(default port)

Physical Address.....: 00D0.9739.B139

Link-local IPv6 Address.....: FE80::2D0:97FF:FE39:B139

IP Address.....: 192.168.0.100

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 192.168.0.1

DNS Servers.....: 0.0.0.0

DHCP Servers.....: 192.168.0.1

DHCPv6 Client DUID.....: 00-01-00-01-29-8D-D2-19-00-D0-97-39-B1-39

5. Щоб перевірити зв’язок комп'ютера з роутером, потрібно надіслати запит з комп'ютера за допомогою команди *ping:*

PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=255

Reply from 192.168.0.1: bytes=32 time=0ms TTL=255

Reply from 192.168.0.1: bytes=32 time=0ms TTL=255

Reply from 192.168.0.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.0.1:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 2ms, Average = 0ms

6. Відкрийте на вкладці Desktop у властивостях комп'ютера Web Browser. В рядок введення URL введіть IP-адресу роутера. Відкриється вікно запиту на введення імені користувача та пароля. За замовчуванням на всіх маршрутизаторах Wi-Fi встановлено ім'я «admin»і пароль «admin». Після їх входу перейдемо до сторінки налаштування роутера. Цю сторінку також можна відкривати через властивості роутера на вкладці GUI. Але в реальних умовах доступ до Доступ до налаштувань Wi-Fi-роутера можна отримати лише через браузер підключеного до нього комп’ютера.

На сторінці налаштування маршрутизатора є кілька вкладок:

а) На вкладці *Setup* налаштовується вхідне Інтернет-з’єднання (Internet Setup), яке можна налаштувати на отримання динамічних настройок (DHCP), статичних настройок PPPoe. Усі ці параметри повідомляє інтернет-провайдер. Також на вкладці Setup можна налаштувати IP-адресу маршрутизатора всередині локальної мережі (Network Setup) та встановити DHCP-сервер (сервер автоматичної роздачі IP-адрес в мережі), в ролі якого також може виступати в якості Wi-Fi-роутер.

б) На вкладці *Wireless* підменю *Basic Wireless Setting* можна сконфігурувати установки безпроводної мережі:

- *Network Mode (Режим роботи)* – керування режимами швидкості передачі даних;

- *Network Name (SSID) (*Ідентифікатор мережі) – ім'я бездротової мережі, трансляція якого можна приховати (SSID Broadcast – Disable);

- Standard Channel – встановлює канал передачі даних;

- в підменю *Wireless Security* налаштовується режим безпеки (Security Mode) бездротової мережі – вибирається метод шифрування (WEP, WPA, WPA2) і встановлюється пароль на підключення до мережі;

- в підменю *Wireless MAC Filter* налаштовується фільтрація за MAC-адресою – дозвіл на підключення до бездротової мережі тільки певних вже відомих пристроїв.

в) На вкладці *Access Restrictions* можна заборонити доступ до мережі тому чи іншому пристрою або протоколу.

г) На вкладці *Application and Gaming* пункт Port Forwarding використовується для налаштування так званого «пробросу» портів (технологія трансляції мережевої адреси залежно від TCP/UDP-порта отримувача).

д) на вкладці *Administration* можна налаштувати доступ до роутера (ім'я, пароль, доступ до мережі, доступ до Web-інтерфейсу).

На вкладці *Wireless* в підменю *Basic Wireless Setting* в полі ідентифікатора мережі вводимо ім'я мережі LabRab. Режим безпеки у підменю *Wireless Security* встановимо WPA2 Personal. Алгоритм шифрування – AES. Пароль (Passphrase) повинна містити не менше 8 символів, в це поле вводимо, наприклад, 11111111.
7. Підключимо ноутбук до нашої бездротової мережі. До робочої області програми додаємо пристрій Laptop. За замовчуванням ноутбук не містить Wi-Fi модуль. Щоб встановити його, необхідно відкрити властивості Laptop, вибрати вкладку *Physical*, на моделі ноутбука натисніть кнопку живлення для вимкнення, вийняти модуль підключення до локальної мережі, та на його місце встановити модуль Wi-Fi WPC300N і увімкнути ноутбук. Потім перейдіть на вкладку *Config* в підменю *Wireless0*. Перемикач IP Configuration повинен бути в положенні DHCP для автоматичного отримання IP-адреси. У полі SSID вводимо назву мережі – LabRab. Перемикач аутентифікації встановлюємо в положення WPA2-PSK і в поле PSK Pass Phrase вводимо заданий раніше пароль 11111111. Ноутбук

підключиться до вказаної бездротової мережі. Перевірити підключення можна з допомогою меню *PC Wireless* на вкладці *Desktop* властивостей ноутбука. На вкладці *Connect* відображається список безпроводових мереж і основна інформація про них (рис. 5.1). З допомогою цього інтерфейсу також можна підключитись до бездротової мережі. Для цього потрібно вибрати мережу, натиснути кнопку *Connect* та вказати тип шифрування та пароль. На вкладці *Link information* ідентифікаторами відображається потужність сигналу якість зв'язку. Отримати більш детальну інформацію про мережу можна натиснути кнопку *More information*.

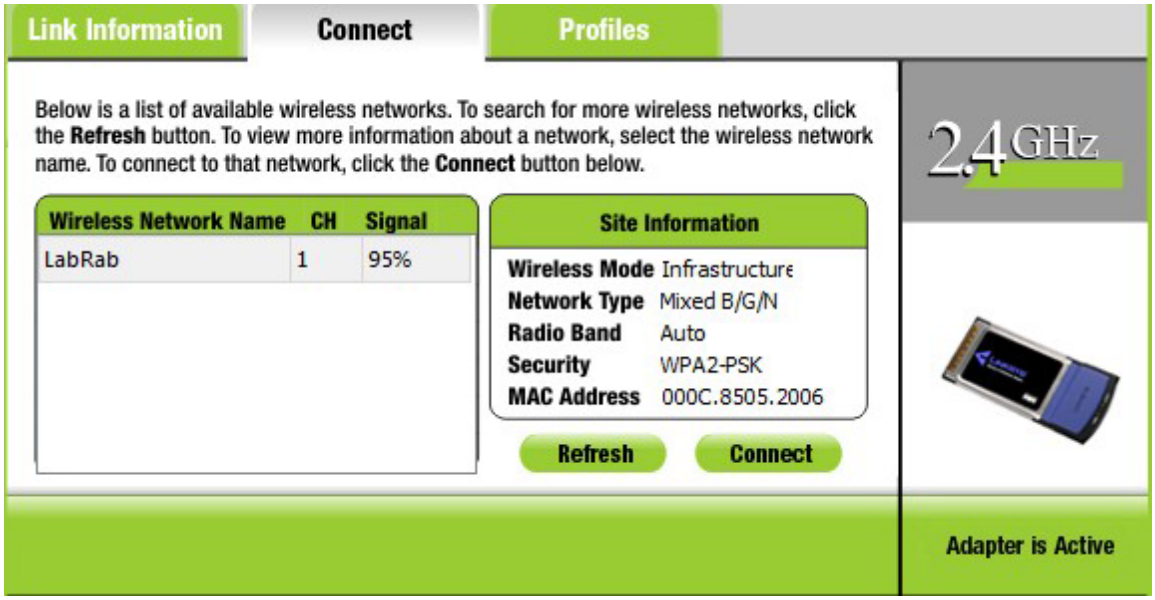


Рис. 5.1. Вікно підключення до бездротової мережі

8. Інші пристрої до мережі Wi-Fi без широковещания SSID підключитися аналогічно: у властивостях пристрою на вкладці *Config* в подменю *Wireless0* потрібно, як описано вище, заповнити поля SSID, Authentication, IP Configuration.

Завдання для індивідуальної роботи

1. Додайте в робочу область Packet Tracer настільний комп'ютер (PCPT PC1) та Wi-Fi роутер (WRT300N) і підключіть їх прямим кабелем типу вита пара.

2. Через Web-інтерфейс комп'ютера PC1 виконуємо налаштування Wi-Fi роутера відповідно до зазначеного варіанту (табл. 5.1).

3. Змініть внутрішню IP-адресу роутера відповідно до таблиці. 5.2. (При зміні локальної IP-адреси роутера з'єднання з ПК переривається, тому що IP-адреси цих пристроїв будуть в різних мережах. Для відновлення підключення необхідно на PC зайти в пункт *IP Configuration* вибрати *Static*, а потім *DHCP*. В результаті PC отримає нову IP-адресу з новим номером мережі.

Таблиця 5.1. Параметри завдання перемикання WAN

Номер варіанта	**Тип комутації провайдера**	**Настройки провайдера для роутера**
1	Автоматичні налаштування	-
2	Статичні налаштування	IP-адреса Інтернету – 45.45.42.42 Маска підмережі – 255.255.0.0 Шлюз за промовчанням – 45.45.0.1 DNS-сервер – 58.255.0.1
3	Параметри PPPoe	Username – a87svfk Password – dsfjhDFS921
4	Автоматичні налаштування	-
5	Статичні налаштування	Internet IP Address – 19.52.132.22 Subnet Mask – 255.255.255.0 Default-Gateway – 19.52.132.1 DNS Server – 158.55.30.41
6	Параметри PPPoe	Username – ADSo23473 Password – sdgkj56hg
7	Автоматичні налаштування	-
8	Параметри PPPoe	Username – BVB44556 Password – htrbYJJYfg676
9	Статичні налаштування	Internet IP Address – 88.45.42.42 Subnet Mask – 255.255.0.0 Default-Gateway – 88.45.0.1 DNS Server – 88.45.0.1

10	Автоматичні налаштування	-

4. Збережіть поточну конфігурацію.

5. Увімкніть сервер «Отримання автоматичних налаштувань» (DHCP) для клієнтів. Діапазон видачі IP-адрес задайте відповідно до табл. 5.2.

Таблиця 5.2. Параметри визначення діапазону адрес для DHCP-сервера

Номер варіанта	**IP-адреса роутера**	**Перша адреса діапазону**	**Остання адреса діапазону**	**Маска мережі**
1	192.168.2.254	192.168.2.20	192.168.2.200	255.255.255.0
2	192.168.7.254	192.168.7.50	192.168.7.100	255.255.255.0
3	192.168.50.254	192.168.50.100	192.168.50.130	255.255.255.0
4	192.168.8.254	192.168.8.140	192.168.8.200	255.255.255.0
5	192.168.5.254	192.168.5.200	192.168.5.220	255.255.255.0
6	192.168.22.254	192.168.22.60	192.168.22.90	255.255.255.0
7	192.168.70.254	192.168.70.90	192.168.70.120	255.255.255.0
8	192.168.150.254	192.168.150.120	192.168.150.160	255.255.255.0
9	192.168.12.254	192.168.12.180	192.168.12.210	255.255.255.0
10	1192.168.90.254	192.168.90.70	192.168.90.90	255.255.255.0

6. Налаштуйте бездротову мережу відповідно до таблиці 5.3.

Таблиця 5.3. Параметри завдання бездротового налаштування

Номер варианту	**Швидкість передачі сигналу, (Мбит/с)**	**Канал передачі данных**	**Ширина каналу, (МГц)**	**Режим захисту**	**Шифрування**
1	11	2	20	WEP	40/64-біт
2	300	4	40	WPA Pers.	TKIP
3	54	6	20	WPA2 Pers.	AES
4	11	8	20	WEP	40/64-біт

5	300	10	40	WPA Pers.	TKIP
6	54	9	20	WPA2 Pers.	AES
7	11	7	20	WEP	40/64-біт
8	300	5	40	WPA Pers.	TKIP
9	54	3	20	WPA2 Pers.	AES
10	11	1	20	WEP	40/64-біт

7. В якості ідентифікатора Використовуйте ідентифікатор (SSID) бездротової мережі використайте «власне ім'я + номер варіанту».

8. Дозвольте трансляцію SSID.

9. Змініть пароль для входу на роутер.

10. Збережіть поточну конфігурацію.

11. Підключіть маршрутизатор до інтернету (елемент Cloud-PT).

12. Додайте другий комп'ютер PC2 до мережі та підключіть його до маршрутизатора з допомогою витої пари. Призначте інтерфейсу PC2 другу доступну адресу в мережі з маскою 255.255.255.0. Як шлюз за замовчуванням використовуйте IP-адресу маршрутизатора.

13. Додайте в мережу ноутбук, планшет і смартфон. Ці пристрої повинні підключатися до мережі по бездротовому зв'язку з динамічним налаштування мережі (рис. 5.2).

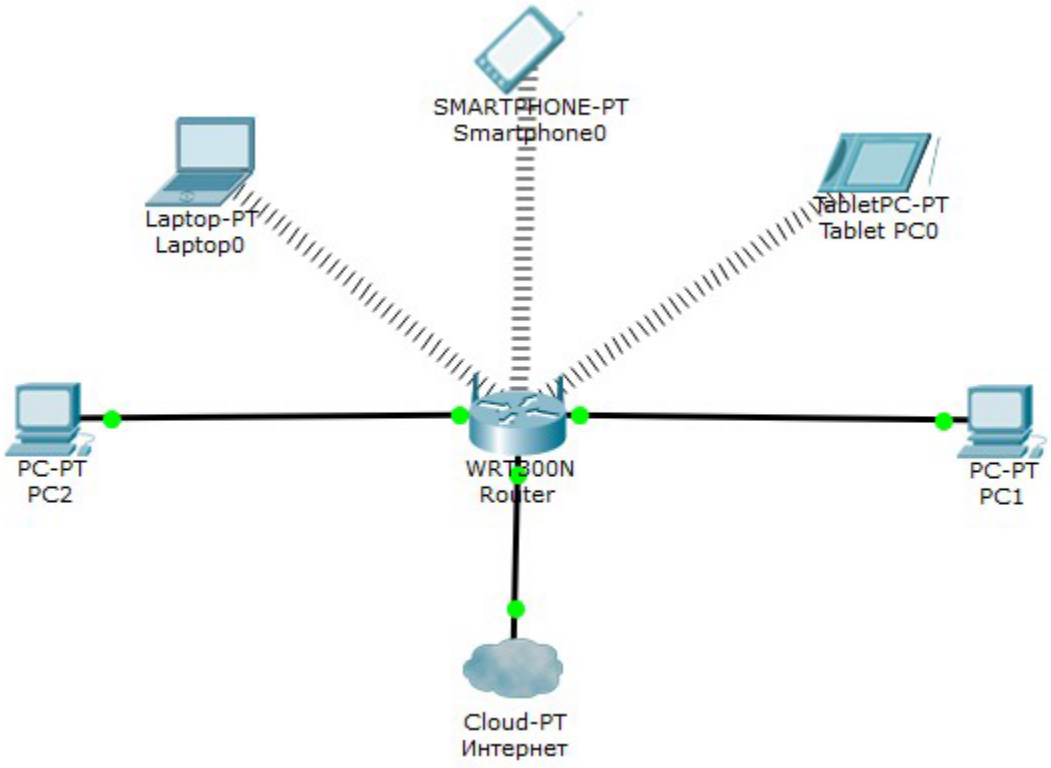


Рис. 5.2. Топологія мережі

14. Перевірте налаштування всіх цільових вузлів в мережі за допомогою команди *ipconfig /all.*

15. Переконайтеся, що мережа працює за допомогою команди *ping.*

Вимоги до звіту

1. Зображення топології мережі.

2. Зображення кожної вкладки маршрутизатора.

3. Зображення команди *ipconfig* кожного цільового вузла.

4. Зображення команди *ping* від кожного вузла термінала до маршрутизатора.

5. Загальні висновки по роботі.

Контрольні запитання

1. Як працює Wi-Fi?

2. Що таке SSID?

3. Що забезпечує стабільний захист бездротового каналу?

4. Як скинути маршрутизатор Wi-Fi?

5. Призначення бездротових маршрутизаторів.

6. Чому мені потрібно транслювати SSID?

ЛАБОРАТОРНА РОБОТА № 6
ОБ'ЄДНАННЯ ПІДМЕРЕЖ

Мета роботи: знайомитись я з поняттям «взаємопов'язані мережі» та принципами взаємодії між мережами.

Теоретичні відомості

Існують мережі будь-якого розміру, від простих, що складаються з двох комп'ютерів, до систем, що з'єднують мільйони пристроїв. У невеликих офісних мережах, домашніх мережах можна організувати спільний доступу до ресурсів, таких як принтери, документи, зображення та і т. д. між локальними комп'ютерами.

Домашні та малі офісні мережі часто налаштовуються людьми, які працюють з дому або віддаленого офісу і яким необхідне підключення до корпоративної мережі або інших централізованих ресурсів. Крім того, фізичні особи-підприємці використовують домашні мережі та невеликі офісна мережі в рекламних цілях для продажу продукції, замовлення витратних матеріалів, взаємодії з клієнтами тощо. Як правило, мережна взаємодія є більш ефективна і дешевша, ніж традиційні методи комунікації, наприклад, пошта або міжміські телефонні дзвінки.

На підприємствах і великих організаціях мережі можуть використовуватися в ще більших масштабах, щоб дозволити співробітникам збирати, зберігати та отримувати інформацію на мережевих серверах. Крім того, мережі дозволяють налагодити швидкий зв'язок у вигляді електронної пошти, обміну миттєвими повідомленнями, а також функції співпраці між співробітниками. Багато компаній використовує мережі для надання продуктів і послуг клієнтам шляхом підключення до Інтернет.

Маршрут, за яким повідомлення йде від джерела до місця призначення може бути простим, наприклад, одним кабелем, що з'єднує один комп'ютер з іншим, або складним, як мережа, що буквально охоплює весь світ. Інфраструктура мережі – це платформа, що підтримує певну мережу. Вона виконує роль

стабільного та надійного каналу передачі даних. Інфраструктура мережі включає в себе три категорії мережевих компонентів: пристроїв, середовище, послуги.

Пристрої та середовища є фізичними елементами або обладнанням мережі. Апаратне забезпечення часто є видимою частиною мережевої платформи – ноутбук, ПК, комутатор, маршрутизатор, бездротова точка доступу або кабелі, що використовуються для підключення пристроїв. Деякі компоненти – невидимі. У випадку бездротових мереж повідомлення передаються за допомогою невидимого радіочастотного або інфрачервоного випромінювання.

Компоненти мережі використовуються для надання послуг та процесів. Це комунікаційні програми, які називаються програмним забезпеченням. яке працює на мережевих пристроях. Мережевий сервіс надає дані у відповідь на запит. Сервіси включають в себе багато мережевих додатків, які люди використовують щодня, наприклад, електронна пошта та послуги веб-хостингу для веб-сайтів. Процеси забезпечують функціональність, яка направляє та переміщує повідомлення у мережі. Процеси для нас менш очевидні, але критично важливі для роботи мереж.

Для здійснення зв'язку в мережі використовується середовище передачі даних. Воно забезпечує канал, через який передається повідомлення від джерело до місця призначення.

Практична частина

Нехай задані мережа «А» 192.168.1.0 з маскою мережі 255.255.255.0 і мережа «Б» 172.16.0.0 з мережевою маскою 255.255.0.0. Їх потрібно об'єднати.

1. Створіть в середовищі Packet Tracer топологію, що містить один маршрутизатор Generic Router-PT-Empty (Router0), один комутатор Generic Switch-PTEmpty (Switch0), одну бездротову точку доступу Generic Access-Point-PT (Access Point0), 2 ПК (PC0 – PC1) и 2 планшети (Tablet PC0 и Tablet PC1).

2. Додайте один оптичний Gigabit Ethernet-модуль PT-ROUTER-NM-1FGE до маршрутизатора для підключення мережі A та один Gigabit Ethernet-модуль PTROUTER-NM-1CGE в роутер для підключення мережі B. Для цього ми відкриємо властивості Router0, на вкладці *Physical* на моделі роутера натиснемо

кнопку живлення, щоб його вимкнути, виберемо зазначені модулі з'єднання, встановимо їх у вільні слоти і включимо роутер.

3. Додамо один Gigabit Ethernet-модуль PT-SWITCH-NM-1FGE в комутатор. Відкриємо властивості Switch0 на вкладці *Physical* на моделі комутатора натисніть кнопку живлення, щоб вимкнути її, виберіть вказаний модуль з'єднання, встановіть його у слот. Щоб підключити комп'ютери, виберіть і встановіть у вільні слоти два модулі PT-SWITCH-NM-1CFE і включити комутатор.

4. Комп'ютери з комутатором з'єднаємо крученою парою – порти підключення FastEthernet. Роутер з комутатором з'єднаємо оптичним кабелем – порти підключення GigabitEthernet. Планшети з'єднаємо з точкою доступу по відкритому бездротовому з'єднанню. Точку доступу з роутером з'єднаємо витою парою – порти, відповідно, Port0 та GigabitEthernet. Топологія мережевої моделі показана на рис. 6.1.

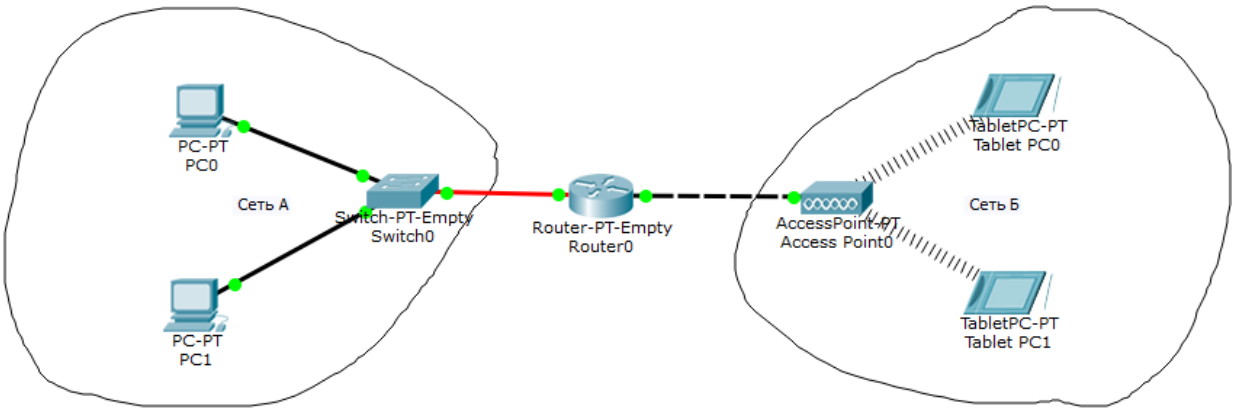


Рис. 6.1 Приклад мережевого зв'язування

5. Налаштуємо елементи мережі. У кожній мережі резервуємо для роутера, першу доступну IP-адресу, а вузлам терміналів будемо задавати другу та наступну доступні адреси.

6. Щоб налаштувати комп'ютер PC0, який належить до мережі А, відкриємо його властивості. На вкладці *Desktop* виберем пункт *IP Config* і для режиму отримання IP-адреси *Static*, в поле *IP Address* введемо другу доступну адресу підмережі – 192.168.1.2, в полі *Subnet Mask* – маску мережі 255.255.255.0, а

Default Gateway – першу доступну IP-адресу підмережі, зарезервовану для роутера: 192.168.1.254. Компютер PC1 налаштовується аналогічно, але в поле *IP Address* вводимо останню доступну адресу підмережі – 192.168.1.254.

7. Задаємо IP-адреси для пристроїв мережі B:

- планшетний ПК0 – 172.16.0.2 маска 255.255.0.0, шлюз – 172.16.0.1;

- планшет PC1 – 172.16.255.254 маска 255.255.0.0, шлюз – 172.16.0.1.

8. Виконуємо настройку роутера, що в нашому випадку буде заключатися в окремому мережному налаштуванні кожного з модулів, до яких підключені комутатор та точка доступу. Відкриємо властивості роутера, перейдемо на вкладку *Config* и в підменю *INTERFACE* та виберемо модуль GigabitEthernet0/0, до якого підключено комутатор першої мережі A 192.168.1.0. У полі IP Address введемо першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – маску мережі 255.255.255.0. Після цього вмикаємо цей модуль – *Port Status* встановлюємо на *On*. Другий модуль налаштовуємо аналогічно – в поле *IP Address* вносимо першу зарезервовану IP-адресу мережі B, тобто 172.16.0.1, а в полі *Subnet Mask* – 255.255.0.0.

9. Перевіряємо роботоздатність мережі. Наприклад, зайдемо на комп'ютер PC0 та пропінгуємо планшетного PC1. Для цього відкриємо властивості PC0, на вкладці *Desktop* виберем пункт *Command Promt* і в вікні, що відкриється в командному рядку, введемо команду *ping* та IP-адресу комп’ютера *Tablet PC1*. Нижче наведені результати виконання команди *ping:*

PC>ping 172.16.0.254

Pinging 172.16.0.254 with 32 bytes of data:

Reply from 172.16.0.254: bytes=32 time=1ms TTL=127

Reply from 172.16.0.254: bytes=32 time=18ms TTL=127

Reply from 172.16.0.254: bytes=32 time=20ms TTL=127

Reply from 172.16.0.254: bytes=32 time=11ms TTL=127

Ping statistics for 172.16.0.254:

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

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 20ms, Average = 12ms

Це підтверджує правильність мережевих налаштувань пристроїв та загальну роботоздатність мережі.

Завдання для індивідуальної роботи

1. Відповідно до зазначеного варіанту (табл. 6.1) об'єднати мережі «А» та «В». В якості пристрою об’єднання використайте роутер Generic Router-PT-Empty. В якості комутатора – Generic Switch-PTEmpty, в якості точки доступу – Generic Access-Point-PT. Спосіб підключення мережі до роутера вказаний в таблиці. 6.2.

2. Додати до маршрутизатора і комутатора необхідні модулі для об'єднання мереж.

3. Встановіть IP-адреси та маски для всіх вузлів відповідно до таблиці 6.3.

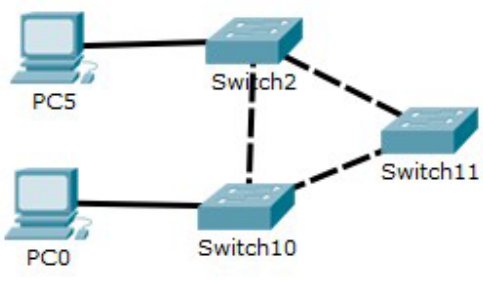
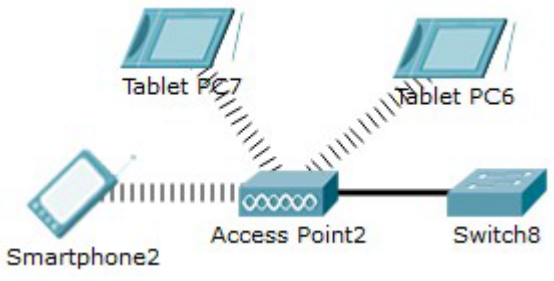
- всім інтерфейсам маршрутизатора задайте останнє допустиме значення IP-адреси мережі;

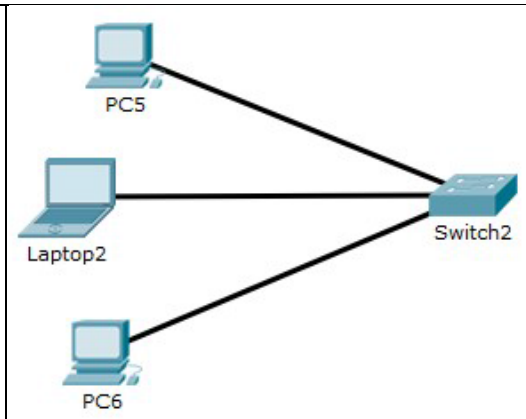
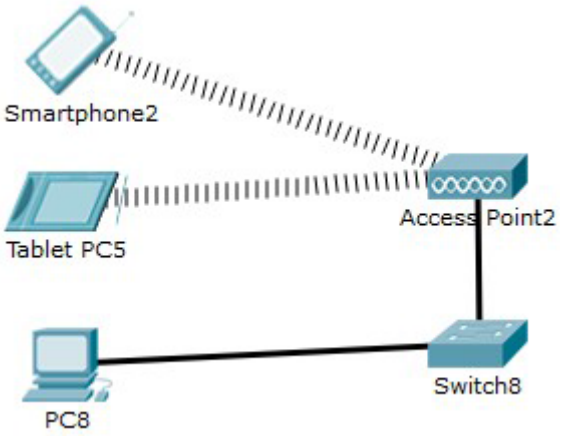
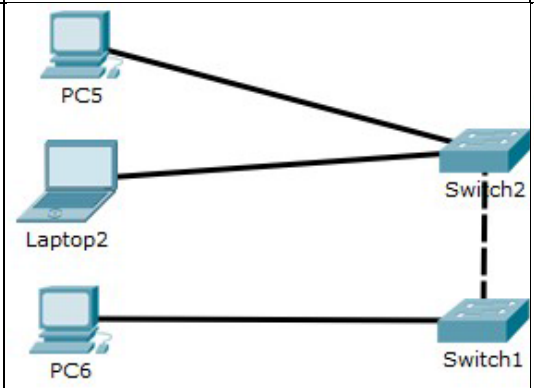
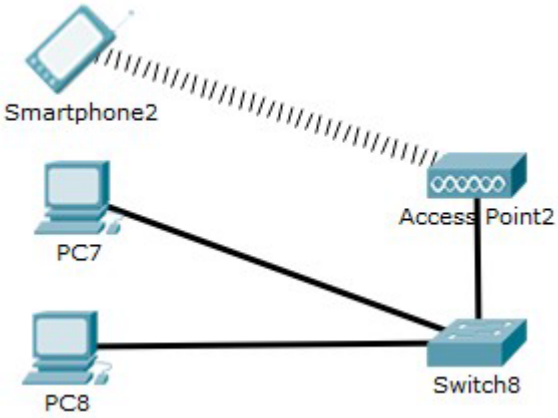
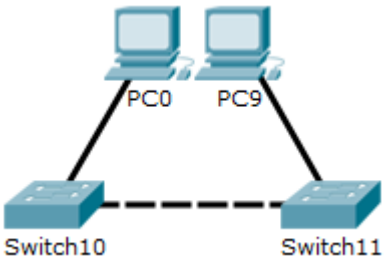
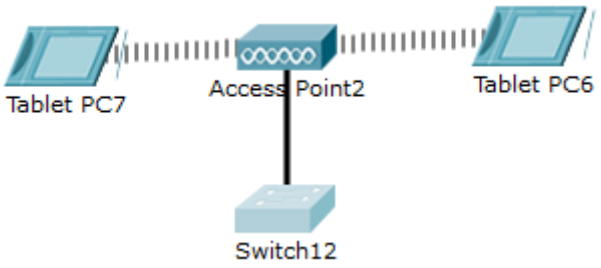
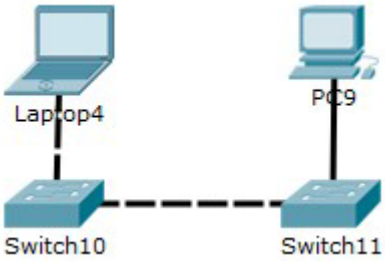
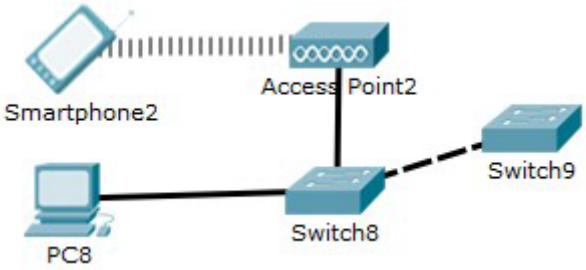
- встановіть дійсні IP-адреси для всіх цільових вузлів у мережах, починаючи з першого.

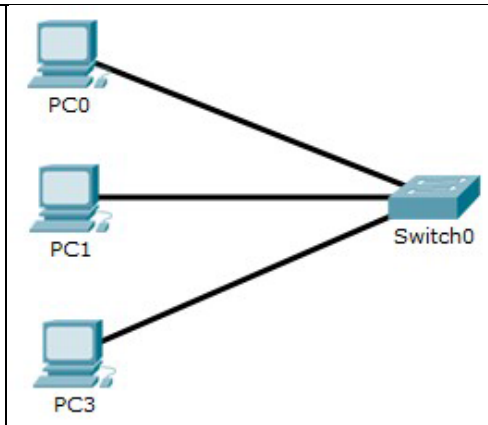
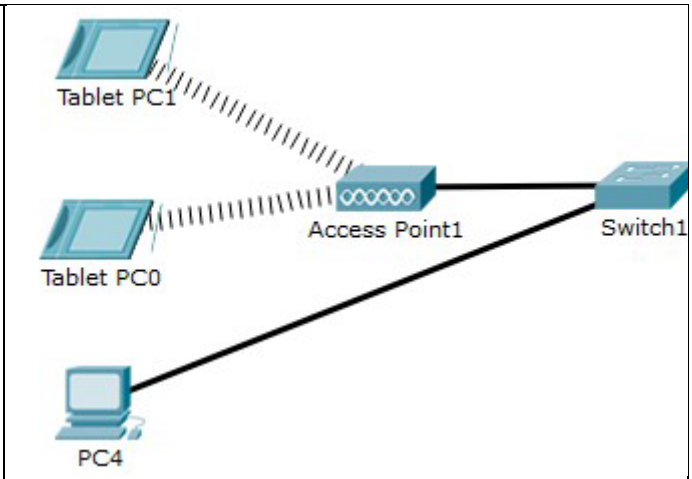
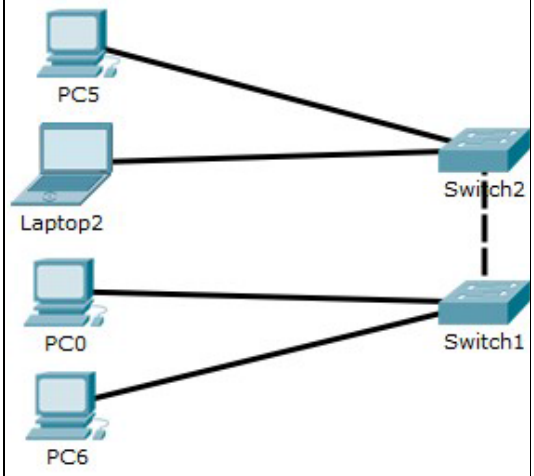
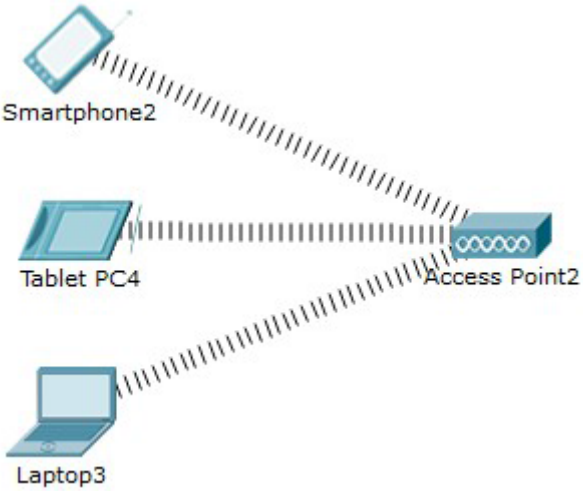
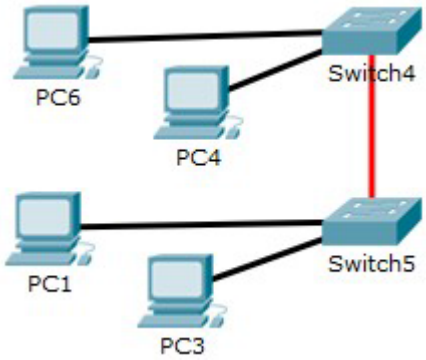
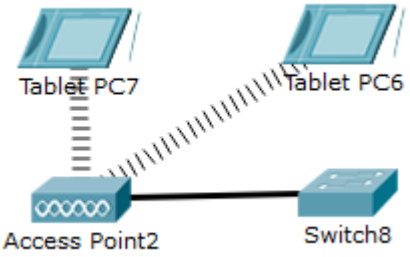
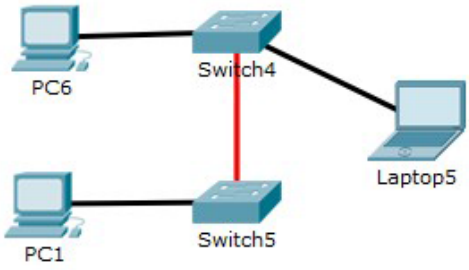
4. Перевірте параметри кожного цільового вузла за допомогою команди *ipconfig.*

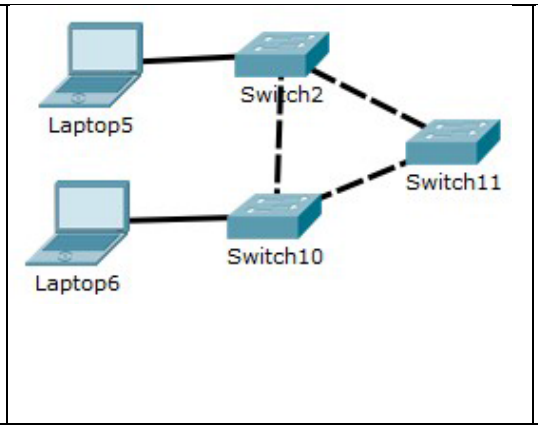
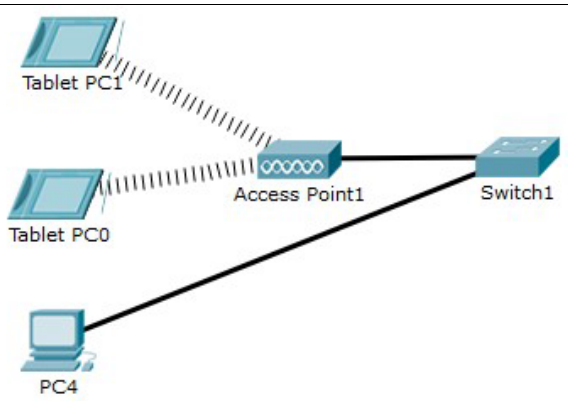
5. Перевірте роботоспроможність мережі за допомогою команди *ping.*

Таблиця 6.1. Варіанти завдань топології мережі

№ вар.	Мережа А	Мережа Б
1		

2	 PC5 Laptop2 Switch2 PC6	 Smartphone2 Tablet PC5 Access Point2 PC8 Switch8
3	 PC5 Laptop2 Switch2 PC6 Switch1	 Smartphone2 PC7 Access Point2 PC8 Switch8
4	 PC0 PC9 Switch10 Switch11	 Tablet PC7 Access Point2 Tablet PC6 Switch12
5	 Laptop4 PC9 Switch10 Switch11	 Smartphone2 Access Point2 Switch9 PC8 Switch8

6	 PC0 PC1 PC3 Switch0	 Tablet PC1 Access Point1 Switch1 Tablet PC0 PC4
7	 PC5 Switch2 Laptop2 PC0 Switch1 PC6	 Smartphone2 Tablet PC4 Access Point2 Laptop3
8	 PC6 Switch4 PC4 PC1 Switch5 PC3	 Tablet PC7 Tablet PC6 Access Point2 Switch8
9	 PC6 Switch4 Laptop5 PC1 Switch5	 Tablet PC7 Access Point2 Tablet PC6

10		

Таблиця 6.2. Параметри перемикання мережі

№ варіанту	**Мережа А**	**Мережа Б**
1	Switch10 витою парою	Switch8 оптичним кабелем
2	Switch2 оптичним кабелем	Switch8 витою парою
3	Switch2 витою парою	Switch8 оптичним кабелем
4	Switch10 оптичним кабелем	Switch12 витою парою
5	Switch11 витою парою	Switch9 оптичним кабелем
6	Switch0 оптичним кабелем	Switch1 витою парою
7	Switch1 витою парою	AccessPoint2 витою парою
8	Switch5 оптичним кабелем	Switch8 витою парою
9	Switch5 витою парою	AccessPoint2 витою парою
10	Switch11 оптичним кабелем	Switch1 витою парою

Таблиця 6.3. IP-адреси та маски для всіх вузлів

№ варіанту	**Адреса мережі А**	**Маска мережі А**	**Адреса мережі Б**	**Маска мережі Б**
1	155.54.14.128	255.255.255.128	16.58.25.32	255.255.255.224
2	182.167.19.64	255.255.255.192	11.16.16.192	255.255.255.224
3	194.151.156.192	255.255.255.192	47.58.69.64	255.255.255.224
4	189.178.15.32	255.255.255.224	13.161.19.64	255.255.255.192
5	65.5.54.128	255.255.255.128	49.46.43.192	255.255.255.192

6	18.15.54.64	255.255.255.192	52.14.16.0	255.255.255.128
7	165.55.18.192	255.255.255.192	13.19.49.32	255.255.255.224
8	168.98.46.32	255.255.255.224	82.84.86.192	255.255.255.192
9	65.49.18.128	255.255.255.128	15.8.66.0	255.255.255.192
10	54.12.18.64	255.255.255.192	19.19.46.192	255.255.255.224

Вимоги до звіту

1. Зображення топології мережі.

2. Скрін результату роботи команди ipconfig кожного цільового вузла.

3. Скрін результату роботи ping між усіма цільовими вузлами.

4. Скрін зображення інструмента *Inspect/Port Status Summary Table* для роутера.

5. Загальні висновки по роботі.

Контрольні запитання

1. Що таке мережа?

2. Навіщо використовувати маршрутизатори?

3. У чому різниця між бездротовим маршрутизатором і точкою доступу?

4. На якому рівні працює маршрутизатор?

5. На якому рівні працює перемикач?

ЛАБОРАТОРНА РОБОТА № 7
СТАТИЧНА ТА ДИНАМІЧНА МАРШРУТИЗАЦІЯ

Мета роботи: ознайомитися з принципом роботи статичної маршрутизації та з принципом функціонування динамічної маршрутизації. Ознайомитись з мережевим протоколом RIP.

Теоретичні відомості

Маршрутизація (англ. Routing) – це процес визначення маршруту слідування інформації в мережах зв'язку.

Маршрути можуть бути встановлюватись адміністративно (статичні маршрути) або розраховуватись з допомогою алгоритмів маршрутизації, на основі топології та інформації про стан мережі, отриманої за допомогою протоколів маршрутизації (динамічних маршрутів).

Статична маршрутизація – це тип маршрутизації, в якому маршрути вказуються в явному вигляді під час налаштування маршрутизатора. Вся маршрутизація відбувається без участі будь-яких протоколів маршрутизації.

Статичними маршрутами можуть бути:

- маршрути, які не змінюються з часом;
- маршрути, що змінюються відповідно до розкладу.

При визначенні статичного маршруту вказується наступне:

- адреса мережі, на яку спрямовується трафік;
- маска мережі;
- адреса шлюзу (вузла), що сприяє подальшій маршрутизації (або безпосередньо підключений до маршрутної мережі);
- метрика маршруту (необов'язково).

Якщо є кілька маршрутів на одну мережу, деякі маршрутизатори вибирають маршрут з мінімальною метрикою.

У деяких маршрутизаторах можна вказувати інтерфейс на який потрібно направляти мережевий трафік, а також додаткові умови, відповідно до який вибирається маршрут.

Переваги статичної маршрутизації:

- легке налагодження та конфігурація в невеликих мережах;

- відсутність додаткових накладних витрат (через відсутність протоколів маршрутизації);

- миттєва готовність (не потрібен час для конфігурації/налаштування).

- низьке навантаження на процесор маршрутизатора;

- Передбачуваність у будь-який момент часу;

Недоліки статичної маршрутизації:

- погане масштабування (додавання (N+1)-ї мережі вимагатиме зробити 2*(N+1) записів про маршрути, при чому на більшості маршрутизаторів таблиця маршрутів буде різною, при N > 3 ... 4 процес налаштування стає дуже трудомістким);

- низька стійкість у ситуаціях, коли розрив відбувається між пристроями другого рівня і порт маршрутизатора не отримує статус Down (відключено);

- відсутність динамічного балансування навантаження;

- необхідність ведення окремої документації до маршрутів, проблема синхронізації документації та реальних маршрутів.

У реальних умовах статична маршрутизація використовується в випадках, коли у є шлюз за замовчуванням (вузол, який має зв’язок з іншими вузлами) і 1-2 мережі.

Протокол маршрутизації – це мережевий протокол, який використовують маршрутизатори для визначення можливих маршрутів слідування даних у складеній комп'ютерній мережі. Протокол маршрутизації може працювати тільки з пакетами, що належать до одного з протоколи, наприклад, IP, IPX або Xerox Network System, AppleTalk. Маршрутизовані протоколи визначають формат пакетів (заголовків), найважливіша інформація із яких для маршрутизації – адреса призначення.

Динамічна маршрутизація здійснюється за рахунок динамічних протоколів маршрутизації. З їх допомогою маршрутизатор будує та оновлює таблицю маршрутизації.

Залежно від алгоритму маршрутизації протоколи поділяються на два типи: дистанційно-векторні протоколи та протоколи стану каналів зв’язку.

Різниця між дистанційно-векторними протоколами і протоколами стану каналів досить суттєва. Останній з'явився пізніше, коли класові мережі відходили у минуле. Їх основним принципом – збереження стану всіх мережевих каналів. Вони будують карту мережі і самостійно визначити оптимальні маршрути. Їх відмінною рисою є здатність надсилати оновлення лише при зміні топології і лиши тим маршрутизаторам, для яких дана інформація буде актуальною.

Алгоритм дистанційно-векторної маршрутизації визначає напрямок (вектор) і відстань (лічильник вузлів) для кожного з каналів зв’язку, з яких складається мережа. Під час використання цього алгоритму маршрутизатор періодично (наприклад, кожні 30 секунд) надсилає всю або частину своєї маршрутної таблиці «своїм сусідам». Періодичні оновлення надсилаються маршрутизаторам, які використовують дистанційно-векторний алгоритм, навіть якщо в мережі не відбулося ніяких змін. Отримавши таблицю маршрутизації від свого сусіда, маршрутизатор може перевірити вже відомі маршрути та внести необхідні зміни на основі отриманого оновлення. Цей процес іноді називають «маршрутизацією за чутками», тому що уявлення маршрутизатора про структуру мережі ґрунтується на даних сусідів. Дистанційно-векторні протоколи маршрутизації засновані на алгоритмі Беллмана-Форда і використовує його для пошуку найкращого маршруту.

Практична частина

У найпростішому випадку при об'єднанні мереж, між якими є кілька роутерів, використовується статична маршрутизація. Наприклад, візьмемо дві мережі: 192.168.1.0 з маскою 255.255.255.0 та 172.16.0.0 з маскою 255.255.255.0, між якими буде два роутери з мережею між ними 10.10.10.0 з маскою 255.255.255.252.

Частина 1. Статична маршрутизація.

1.На робоче поле програми Packet Tracer додайте два комутатори 2950-24 (Switch0 і Switch1), два роутери Router 1841 (Router0 и Router1), два стаціонарних комп'ютери (PC0 і PC1).

2. Підключіть всі пристрої з комутатором за допомогою витої пари, а роутери між собою – крос-кабелем. Порти підключення для всіх пристроїв – FastEthernet. Топологія мережевої моделі показана на рис. 7.1.

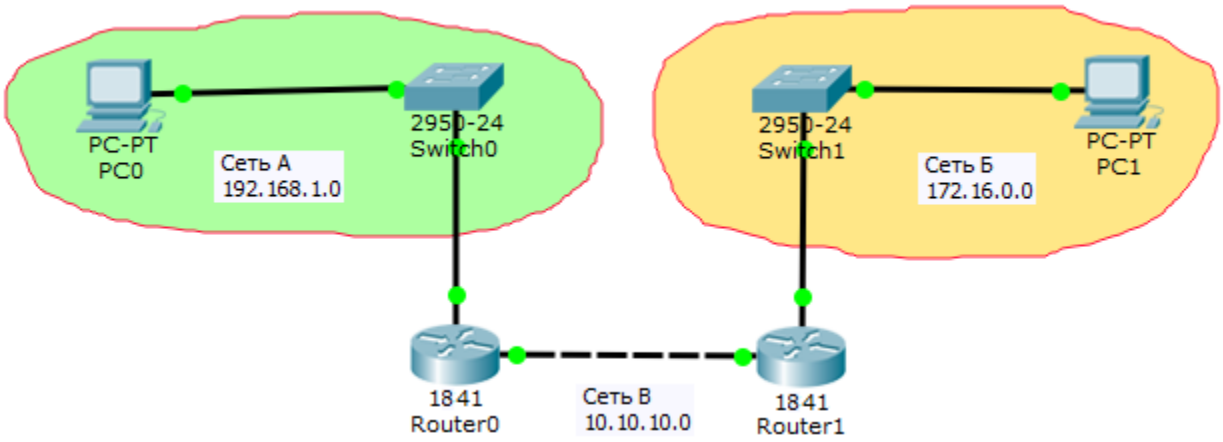


Рис. 7.1. Топологія мережевої моделі

3. Збережіть створену топологію.

4. Налаштуйте елементи мережі. Резервуємо для роутера Router0 першу доступну IP-адресу в мережі А – 192.168.1.1, а для роутера Router1 – першу доступну IP-адресу в мережі В – 172.16.0.1.

5. Щоб налаштувати PC0, відкрийте його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адреси *Static* в поле *IP Address* введіть другу доступну мережеву адресу – 192.168.1.2, в поле *Subnet Mask* – маску мережі 255.255.255.0, а в полі *Default Gateway* вкажіть першу доступні IP-адресу мережі А, зарезервовану для роутера тобто 192.168.1.1. Комп’ютер PC1 мережі Б налаштовуйте аналогічно, але в поле *IP Address* введіть адресу – 172.16.0.2, а в поле *Default Gateway* – 172.16.0.1.

6. Налаштуйте роутер Router0. Давайте відкриємо властивості роутера, перейдіть на вкладку *Config* та в підменю *INTERFACE* виберіть модуль FastEthernet0/0, до якого підключена мережа А. У поле IP Address введіть першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – мережну

маску 255.255.255.0. Після цього включіть цей модуль – *Port Status* установим в *On*. В інтерфейсі FastEthernet0/1 встановіть адресу 10.10.10.1 та мережну маску 255.255.255.252 мережі Б.

7. Аналогічно, налаштуйте Router1. На інтерфейсі FastEthernet0/0 вкажіть адресу 172.16.0.1 та маску мережі 255.255.255.0 мережі В, а на інтерфейсі FastEthernet0/1 задайте адресу 10.10.10.2 та мережеву маска 255.255.255.252 мережі В.

8. Оскільки Router0 не знає про мережу В, а Router1 – про мережу А, додайте відповідні статичні маршрути до маршрутизаторів. Відкрийте властивості Router0, перейдіть на вкладку *Config* та в підменю *ROUTING* виберіть *Static*. У полі *Network* введіть адресу мережі Б – 172.16.0.0, в *Mask – її маску* 255.255.255.0, а в якості наступного переходу в полі *Next Hop* вкажіть Router1, до якого підключено Router0, – 10.10.10.2 (рис. 7.2). Для додавання цих відомостей до списку адрес натисніть кнопку *Add*.

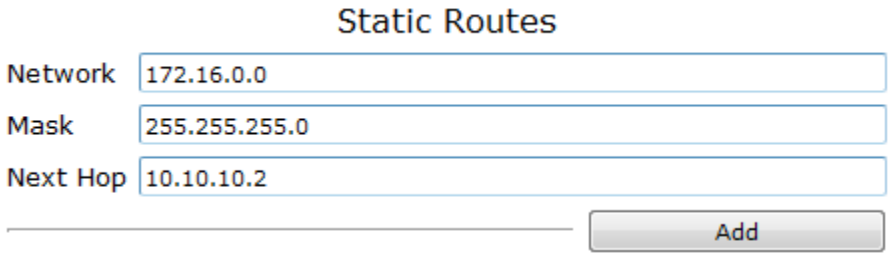


Рис. 7.2. Додавання статичного запису в Router0

Router1 налаштовується аналогічно. У полі *Network* введіть адресу мережі А – 192.168.1.0, в *Mask* – її маску 255.255.255.0, а в якості наступного переходу, у полі *Next Hop* вкажіть інтерфейс Router0, до якого підключено Router1, – 10.10.10.1.

9. Перевірте правильність налаштувань мережевих пристроїв і працездатність мережі. Пропінгуйте з компютера PC0 комп’ютер PC. Для цього ми відкриємо властивості комп'ютера PC0 на вкладці *Desktop* виберемо пункт *Command* Promt і у вікні, що відкриється, в командному рядку, введемо команду

ping та IP-адресу комп'ютера PC1. Нижче наведені результати виконання команди *ping:*

PC>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=13ms TTL=126

Reply from 172.16.0.2: bytes=32 time=11ms TTL=126

Reply from 172.16.0.2: bytes=32 time=11ms TTL=126

Reply from 172.16.0.2: bytes=32 time=14ms TTL=126

Ping statistics for 172.16.0.2:

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

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 14ms, Average = 12ms

10. Перевіряємо шлях пакетів з мережі А в мережу Б. У командний рядок комп'ютера PC0 вводимо команду *tracert* та IP-адресу комп'ютера PC1. Нижче наведено результати команди *tracert:*

PC>tracert 172.16.0.2

Tracing route to 172.16.0.2 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 192.168.1.1

2 0 ms 0 ms 0 ms 10.10.10.2

3 12 ms 12 ms 12 ms 172.16.0.2

Trace complete.

Такий результат підтверджує, що всі мережні пристрої настроєно належним чином.

Частина 2. Динамічна маршрутизація.

Для об'єднання мереж, між якими є якась кількість роутерів, використовується динамічна маршрутизація. Розглянемо динамічну маршрутизацію на топології мережі з попереднього прикладу.

1. Залишимо всі мережні налаштування пристроїв без з мін, за винятком статичних маршрутів – видаляємо усі налаштовані статичні маршрути на Router0 і Router1. Для цього відкриємо властивості роутера, переходимо на вкладку

Config, у підменю *ROUTING* вибираємо *Static*, у полі *Network Address* виділяємо запис та натискаємо кнопку *Remove*.

2. Тепер, після видалення маршрутів, Router0 не знає про мережу Б, а Router1 про мережу А. Настроїмо динамічну маршрутизацію за протоколом RIP на обох маршрутизаторах. Для цього кожному роутеру потрібно визначити, які мережі до нього підключені. Відкриємо властивості Router0, перейдемо на вкладку *Config*, в підменю *ROUTING* виберемо пункт RIP. У полі *Network* введемо адреси підключених мереж 10.10.10.0 та 192.168.1.0 і додамо їх до списку за допомогою кнопки Add (рис. 7.3).

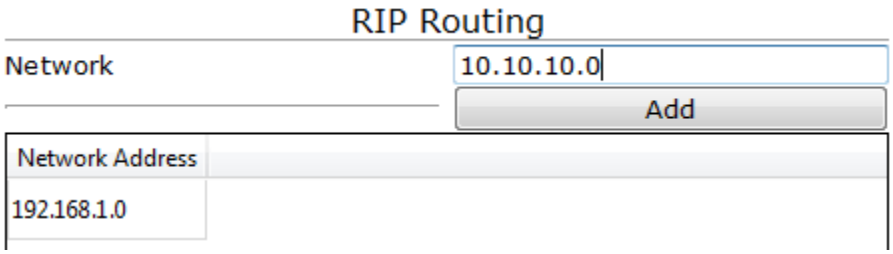


Рис. 7.3. Оголошення мереж в маршрутизаторі0

3. Аналогічно для Router1 оголосимо мережі 10.10.10.0 та 172.16.0.0.

4. Перевіримо правильність мережевих налаштувань пристроїв і працездатність мережі. Пропінгуємо з комп'ютера PC0 комп'ютер PC1. Нижче наведені результати команди *ping:*

PC>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=11ms TTL=126

Reply from 172.16.0.2: bytes=32 time=12ms TTL=126

Reply from 172.16.0.2: bytes=32 time=12ms TTL=126

Reply from 172.16.0.2: bytes=32 time=12ms TTL=126

Ping statistics for 172.16.0.2:

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

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 12ms, Average = 11ms

5. Перевіримо шлях пакетів з мережі А в мережу Б. Нижче представлені результат команди *tracert:*

PC>tracert 172.16.0.2

Tracing route to 172.16.0.2 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 192.168.1.1

2 0 ms 0 ms 0 ms 10.10.10.2

3 11 ms 12 ms 11 ms 172.16.0.2

Trace complete.

З цього випливає, що всі пристрої в мережі налаштовані правильно.

Завдання для індивідуальної роботи

1. Додайте на робоче поле програми Packet Tracer три комутатори Switch 2950-24 (Switch0 – Switch2), три загальні роутери Generic Router-PT-Empty (Router0 – Router2), шість стаціонарних комп'ютерів (PC1 – PC6).

2. Додайте до кожного роутери по три Gigabit Ethernet-модуля PT-ROUTERNM-1CGE і створіть мережу відповідно до рис. 7.4.

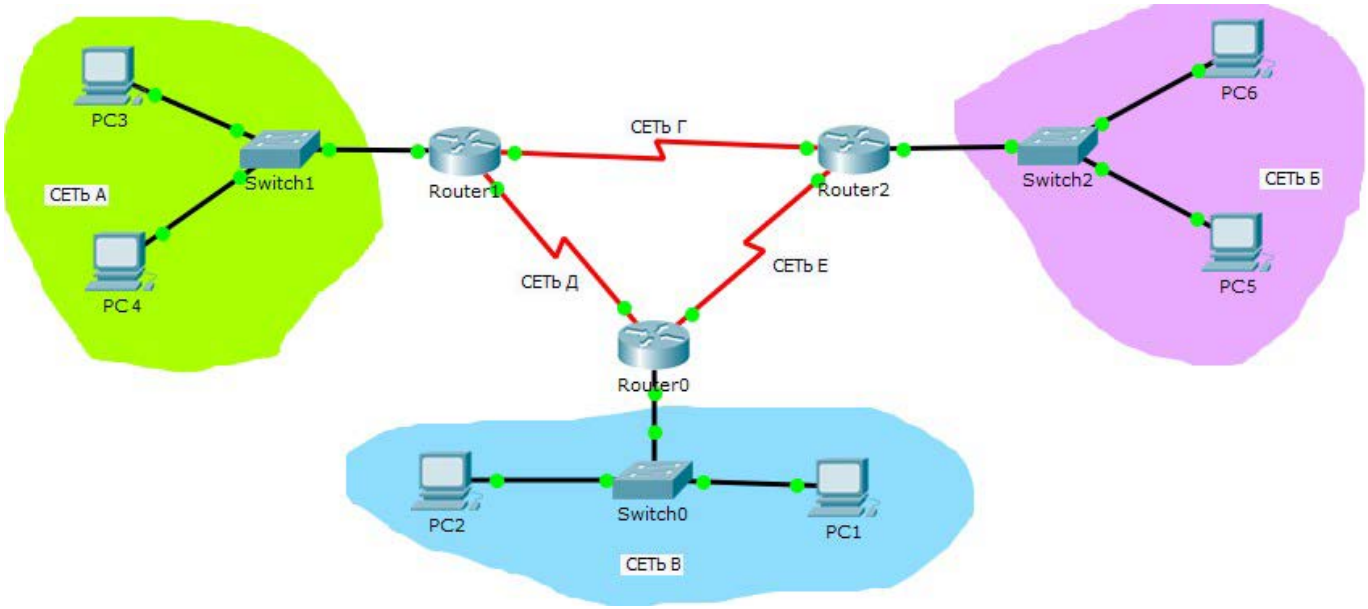


Рис. 7.4. Топологія мережі

3. Призначте всім вузлам статичні IP-адреси відповідно до варіанту (табл. 7.1). Для мереж А, Б, В використовуйте мережеву маску 255.255.255.0, а для мереж Г, Д, Е – 255.255.255.252.

Таблиця 7.1. Варіанти завдань

№ вар.	Мережа А	Мережа Б	Мережа В	Мережа Г	Мережа Д	Мережа Е
1	92.16.0.0	45.44.47.0	72.28.200.0	223.16.166.8	22.16.0.4	78.4.4.16
2	90.15.128.0	7.27.37.0	45.228.25.0	223.166.18.8	20.15.128.4	42.45.15.16
3	92.135.0.0	57.27.25.0	27.42.27.0	232.16.13.8	22.135.0.4	55.13.13.16
4	10.101.64.0	41.77.123.0	77.77.7.0	94.45.41.8	223.16.166.4	11.11.11.16
5	25.98.0.0	123.16.166.0	31.169.1.0	42.42.7.8	223.166.18.4	22.22.22.16
6	56.6.128.0	123.166.18.0	169.1.196.0	75.28.72.8	202.16.13.4	25.165.16.16
7	81.16.0.0	192.16.13.0	16.163.1.0	49.4.4.8	61.49.48.4	3.16.166.16
8	91.29.192.0	123.99.81.0	106.49.19.0	19.196.16.8	65.46.98.4	3.166.18.16
9	90.155.0.0	192.16.19.0	158.89.1.0	19.16.18.8	18.156.5.4	3.16.13.16
10	65.16.128.0	77.88.2.0	198.19.169.0	41.84.65.8	4.46.46.4	15.15.15.16

4. Інтерфейсам роутерів призначте першу та другу доступні адреси мережі. Цільовим пристроям слід надавати адреси, починаючи з третьої доступної адреси.

5. Створіть на роутерах статичні маршрути до невідомих їм мереж:

- для Router0 додайте статичні маршрути в мережу А, Д, Е.

- для Router1 додайте статичні маршрути в мережі Б, В, Е.

- для Router2 додайте статичні маршрути в мережу А, В, Д.

6. Перевірте роботу мережі за допомогою команди *ping*.

7. Виконайте трасування між вузлами PC3 і PC6, PC5 і PC1.

8. Перевірте таблицю маршрутизації роутерів за допомогою інструменту «Inspect/Routing Table

9. Видаліть всі статичні маршрути на роутерах.

10. Оголосіть на роутерах безпосередньо підключені до них мережі для роботи протоколу динамічної маршрутизації RIP:

- для маршрутизатора0 оголосити маршрути в мережі В, Д, Е.

- для маршрутизатора1 оголосити маршрути в мережі А, Д, Г.

- для маршрутизатора2 оголосити маршрути в мережі В, Е, Г.

11. Перевірте роботу мережі за допомогою команди *ping*.

12. У режимі симуляції відправте запит з PC1 на PC3. Прослідкуйте за рухом пакетів по протоколу ICMP.

13. Виконайте трасування між вузлами PC3 і PC6, PC5 і PC1. Видаліть під'єднання мережі Г. Повторіть трасування.

14. Перевірте таблицю маршрутизації роутерів за допомогою інструменту *Inspect/Routing Table*.

Вимоги до звіту

1. Зображення топології мережі.

2. Зображення команди *ipconfig* кожного цільового вузла.

3. Зображення команди *tracert* відповідно до пункту 7 завдання.

4. Зображення вікна *Inspect/Routing Table* для кожного маршрутизатора відповідно до пункту 8 завдання.

5. Зображення вікна *Simulation Panel* відповідно до пункту 12 завдання.

6. Зображення команди *tracert* відповідно до п.13 завдання.

7. Зображення вікна *Inspect/Routing Table* для кожного роутера відповідно до пункту 14 завдання.

8. Загальні висновки по роботі.

Контрольні запитання

1. Що таке маршрутизація?

2. Де використовується статична маршрутизація?

3. Де використовується динамічна маршрутизація?

4. У чому різниця між статичною і динамічною маршрутизацією?

5. Які переваги динамічної маршрутизації?

6. Які недоліки статичної маршрутизації?

ЛАБОРАТОРНА РОБОТА № 8
НАСТРОЙКА ТА ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ПОШТИ

Мета роботи: ознайомитися з принципом роботи електронної пошти та її протоколами (SMTP і POP3). Навчитися налаштувати поштову скриньку.

Теоретичні відомості

Електронна пошта (англійська e-mail – електронна пошта) – технологія та служба з пересилки та отримання електронних повідомлень («листи», «електронні листи» або «повідомлення») між користувачами комп'ютерної мережі (в тому числі мережі Інтернет).

Електронна пошта за складом елементів і принципом роботи практично повторює систему звичайної (паперової) пошти, запозичуючи як терміни (пошта, лист, конверт, вкладення, коробка, доставка та інші) так і помітні особливості – простоту використання, надійність, і, в той же час, немає гарантії доставки.

Перевагами електронної пошти є: адреси виду «username@domain_name», які людина може легко сприймати та запам’ятовувати, можливість передачі як звичайного, так і відформатованого тексту, а також довільних файлів (текстові документи, медіафайли, програми, архівів тощо); незалежність серверів (в загальному випадку вони звертаються безпосередньо один до одного); досить висока надійність доставки повідомлень, простота використання людьми і програмами.

Недоліки електронної пошти: наявність такого явища, як спам (масова реклама та вірусні розсилки); можливі затримки з доставкою повідомлень; обмеження розміру повідомлення і загального розміру повідомлення у поштовій скриньці.

Розвиток інтернет-технологій привів до появи сучасних протоколів обміну повідомленнями, які надають більше можливостей обробки листів, різноманітні послуги та зручність у роботі. Наприклад, протокол SMTP, який працює за принципом клієнт-сервер, призначений для відправки повідомлень з комп'ютера до адресату. Як правило, доступ до SMTP-сервера не захищається паролем, тому можна для відправки повідомлень використовувати будь-який відомий сервер у

мережі. На відміну від серверів для відправки електронних листів, доступ до серверів для зберігання повідомлень захищено паролем. Тому для отримання та збереження листів потрібно використовувати сервер або службу в якій існує обліковий запис. Ці сервери працюють за протоколами POP і IMAP, які відрізняються способом зберігаються електронних листів.

SMTP (англ. Simple Mail Transfer Protocol – простий протокол передачі пошти) — широко використовуваний мережевий протокол, призначений для передача електронної пошти в мережах TCP/IP.

У той час як сервери електронної пошти та інші агенти пересилки повідомлень використовують SMTP для надсилання та отримання поштових повідомленнь електронної пошти, клієнтські поштові додатки, які працюють на користувацькому рівні, зазвичай використовують SMTP лише для надсилання повідомленнь на поштовий сервер для ретрансляції. Для отримання повідомлень клієнтські програми зазвичай використовують або *POP* (англ. Post Office Protocol – протокол поштового відділення) або *IMAP* ((англ. Internet Message Access Protocol – протокол доступу до повідомлень електронної пошти в мережі Інтернет), або пропрієтарні системи (Microsoft Exchange и Lotus Notes/Domino) для доступу до облікового запису поштової скриньки.

POP3 (англ. Post Office Protocol, Version 3 – протокол поштового відділення, версія 3) – стандартний інтернет-протокол прикладного рівня, що використовується клієнтами електронної пошти для отримання листів з віддаленого сервера за TCP/IP-з'єднанням.

POP і IMAP є найпоширенішими інтернет-протоколами для доступу до пошти. Практично всі сучасні клієнти і сервери електронної пошти підтримують обидва стандарти. Більшість постачальників послуг електронної пошти також підтримують протокол IMAP і POP3.

Практична частина

Нехай задана мережа 192.168.1.0 з маскою 255.255.255.0, що складається з двох настільних ПК, комутатора та сервера. Необхідно налаштувати поштовий сервер і настроїти обидва ПК для отримання та надсилання електронних листів.

1. Додаємо на робоче поле програми Packet Tracer два стаціонарних комп'ютери (PC0 і PC1), комутатор 2960-24TT (Switch0) і сервер Generic Server-PT (Server0).

2. Підключаємо всі пристрої до комутатора за допомогою витої пари. Порти підключення всіх пристроїв і комутатора – FastEthernet. Топологія моделі мережі представлена на рис. 8.1.

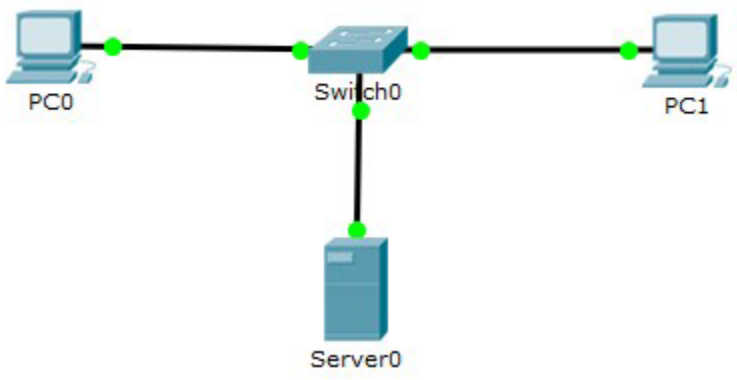


Рис. 8.1. Топологія мережі

3. Збережіть створену топологію.

4. Налаштуємо елементи мережі. Зарезервуємо для сервера – другу доступну IP-адресу, а стаціонарним комп'ютерам будемо задавати адреси послідовно з третього доступного. Мережева маска для всіх пристроїв – 255.255.255.0.

5. Щоб налаштувати PC0, відкриємо його властивості. На вкладці *Desktop* виберемо пункт *IP Config* і для режиму отримання IP-адреси *Static* в поле *IP Address* введемо третю доступну мережеву адресу – 192.168.1.3, в поле *Subnet Mask*– маску мережі 255.255.255.0, а поле *Default Gateway* за промовчанням можемо залишити порожнім, тому що у нас немає виходу за мережі нашої мережі. Другий стаціонарний комп’ютер налаштовано аналогічно.

6. Щоб налаштувати серверу, відкриємо його властивості, перейдемо на вкладку *Config* і в підменю *INTERFACE* виберемо модуль *FastEthernet0*. У поле *IP Address* ведемо другу зарезервовану IP-адресу мережі – 192.168.1.2, а в поле *Subnet Mask* – маску мережі 255.255.0. Після цього включимо цей модуль – *Port Status* установим в *On*. Далі налаштуємо сервіс *EMAIL*.

Перейдіть на вкладку *Services* та виберемо підменю *EMAIL*. Для ввімкнення перемикачі *SMTP Service* и *POP3 Service* встановимо в положення *On*.

Призначимо доменне ім'я поштовому серверу - в поле *Domain Name* введемо, наприклад, *zu.edu.ua*. Натиснtvj кнопку *Set*, щоб зберегти ім'я домену. Далі створимо два облікові записи користувачів. Для цього потрібно в поле *User* ввести ім'я облікового запису, а в поле *Password – пароль.* Для додання запису до бази даних, натиснемо кнопку "+". Таким чином, створюємо ще два записи: user1 з паролем user1 і user2 з паролем user2.

7. Настроювання поштових скриньок на ПК0 і ПК1. На вкладці *Desktop* вибираємо елемент *Email.* З'явиться вікно для настроювання поштової скриньки. У полі *Your Name* вкажемо довільне ім'я поштової скриньки, яке зберігатиметься тільки на локальному ПК (наприклад, для PC0 – U1, а для PC2 – U2). В полі *Email Address* потрібно вказати повне ім'я поштової скриньки

email = имя учетной записи на сервере + @ + доменное имя сервера

Для PC0 це user1@zu.edu.ua, а для PC1 це user2@zu.edu.ua. В розділі *Server Information* вкажемо IP-адресу для серверів вхідної і вихідної пошти – в нашому випадку *Incoming Mail Server* и *Outgoing Mail Server* адреса буде однакова для обох ПК – 192.168.1.2. У розділі *Logon Information* вкажемо ім'я та пароль облікового запису, раніше записаного на сервері (для PC0 – user1 з паролем user1, а для PC1 – user2 з паролем user2). Щоб зберегти конфігурацію, натиснемо кнопку *Save*.

8. Перевіримо працездатність поштових скриньок. Наприклад, давайте зайдемо на компютер PC0 до розділу *Desktop / Email.* Відкриється вікно *Mail Browser*. Для відправки листа натиснемо кнопку *Compose.* У полі *To* вкажемо e-mail адресу отримувача – user2@zu.edu.ua, в поле *Subject* введемо тему листа (наприклад, «тест»), а в нижнє поле – текст листа (наприклад, «Мій перший текст!!!»). Щоб надіслати повідомлення, натиснемо кнопку *Send.* Після відправки листа в нижній частині вікна з'явиться запис про те, що повідомлення було відправлено
(рис. 8.2).

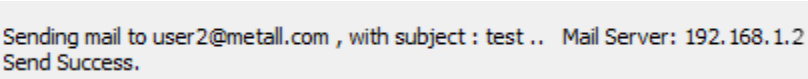


Рис. 8.2. Повідомлення про успішну відправку листа

Щоб прочитати отриманий лист, перейдемо до розділу *Desktop / Email* на комп'ютері PC1 та натиснемо кнопку *Receive*. Відобразиться список усіх отриманих листів (див. Рис. 8.3). Відкрити лист можна подвійним натисканням лівої кнопки миші.

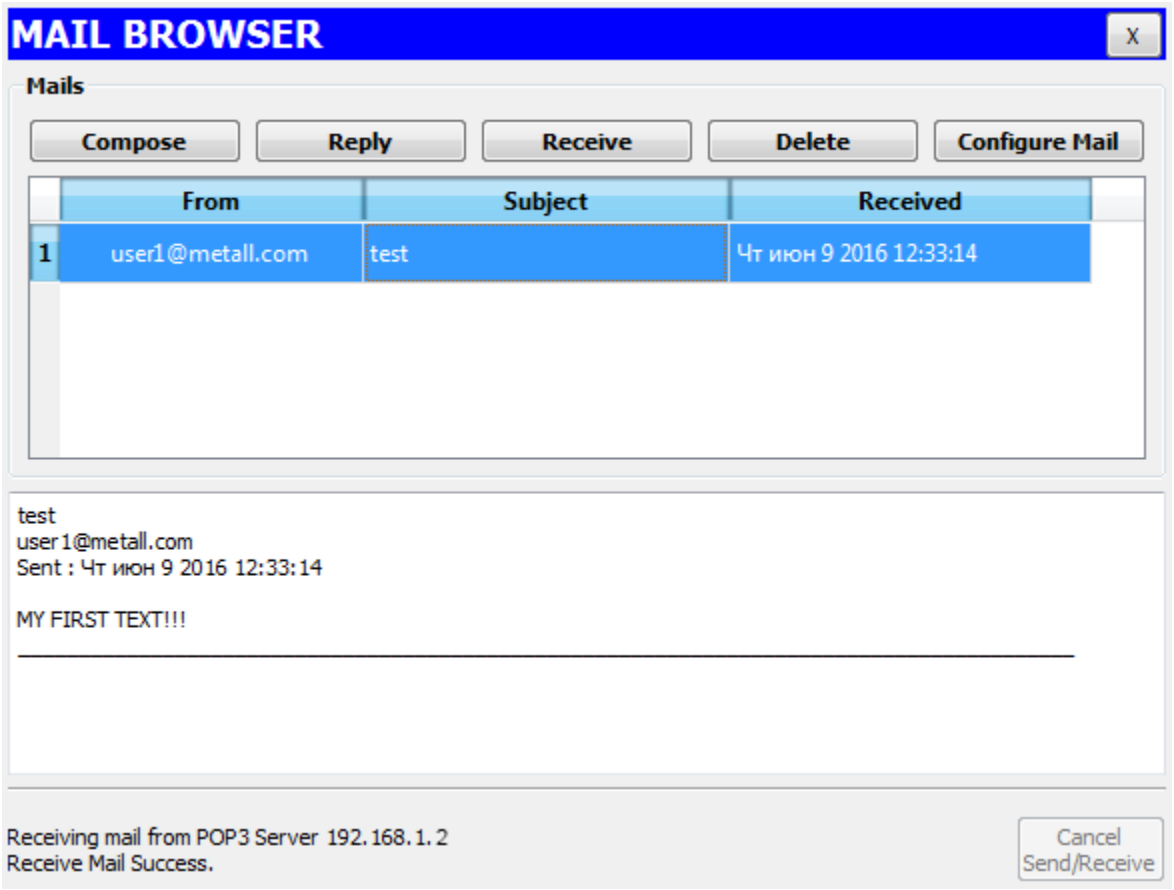


Рис. 8.3. Перелік отриманих повідомлень

Завдання для індивідуальної роботи

1. Додайте до робочого поля програми Packet Tracer два стаціонарні комп'ютери (PC0, PC1), два ноутбуки (Laptop0, Laptop1), два комутатори 2960-24TT (Switch0, Switch1), роутер Generic Router-PT-Empty (Router0) та два сервери Generic Server-PT (email_A, email_Б).

2. Додайте два Gigabit Ethernet-модуля PT-ROUTER-NM-1CGE до роутера для підключення мережі.

3. Об’єднайте всі пристрої за допомогою витої пари. Порти підключення роутера та комутаторів – GigabitEthernet, решти пристроїв з комутаторами – FastEthernet. Топологія мережевої моделі показана на рис. 8.4.

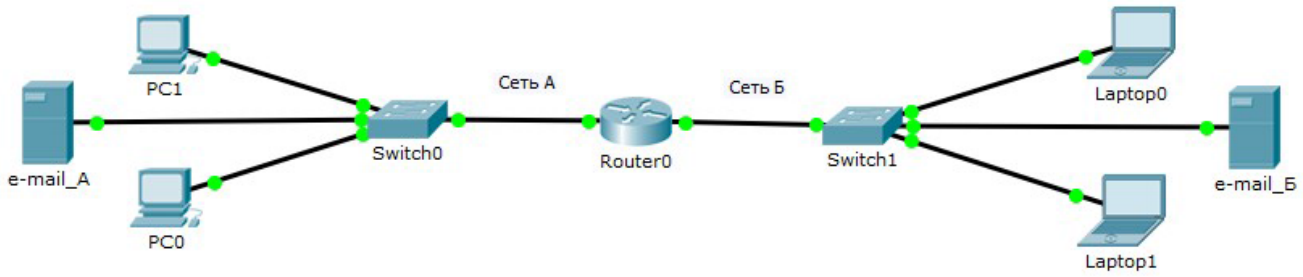


Рис. 8.4. Задання топологія мережі

4. Призначте статичні IP-адреси цільовим вузлам у мережах А та Б відповідно до зазначеного варіанту (табл. 8.1):

- призначте першу доступну адресу інтерфейсу роутера в мережах А і Б.
- призначте останні доступні адреси серверам у мережах А та Б.
- призначте другу доступну адресу в мережі А.
- комп’ютеру PC1 призначте третю доступну адресу в мережі А.
- призначте другу доступну адресу в мережі В для Laptop0.
- призначте третю доступну адресу в мережі В для Laptop1.

Таблиця 8.1. Параметри завдання мережної адреси

№ вар.	Адреса мережі А	Маска мережі А	Адреса мережі Б	Маска мережі Б
1	14.67.11.128	255.255.255.192	51.18.41.160	255.255.255.224
2	14.67.12.128	255.255.255.224	51.18.42.160	255.255.255.240
3	14.67.13.128	255.255.255.128	51.18.43.160	255.255.255.248
4	14.67.14.128	255.255.255.192	51.18.44.160	255.255.255.224
5	14.67.15.128	255.255.255.224	51.18.45.160	255.255.255.240
6	14.67.16.128	255.255.255.128	51.18.46.160	255.255.255.248
7	14.67.17.128	255.255.255.192	51.18.47.160	255.255.255.224
8	14.67.18.128	255.255.255.224	51.18.48.160	255.255.255.240
9	14.67.19.128	255.255.255.128	51.18.49.160	255.255.255.248
10	14.67.20.128	255.255.255.192	51.18.50.160	255.255.255.224

5. Перевірте працездатність мережі – пропінгуйте з PC0 решту вузлів мережі.

6. Згідно з таблицею 8.2 створіть на серверах email_A та email_B поштові сервера з доменними іменами і додайте до них по два облікові записи. Для кожного запису придумайте свій пароль.

7. Налаштуйте поштові скриньки на всіх цільових вузлах відповідно до таблиці 8.2.

8. Перевірте відправку пошти:

- відправте тестові листи з PC0 на всі інші поштові скриньки;

- відправте тестові листи з Laptop0 на всі інші поштові скриньки.

9. Перевірте прийом листів на всіх пристроях.

10. У режимі моделювання надішліть тестовий електронний лист з PC1 на Laptop1. Відстежуйте рух пакетів за протоколами SMTP та POP3 під час надсилання і отримання листа.

Таблиця 8.2. Параметри завдання імені домену

№ вар.	Домен сервера email_A	Обліковий запис PC0	Обліковий запис PC1	Домен сервера email_Б	Обліковий запис Laptop0	Обліковий запис Laptop1
1	Albania.com	Tirana	Durres	Chad.net	Koumra	Mongo
2	Algeria.com	Algiers	Oran	Pakistan.net	Islamabad	Karachi
3	Chad.com	Bangor	Fada	Peru.net	Lima	Arequipa
4	Angola.com	Luanda	Huambo	Cyprus.net	Nicosia	paphos
5	Ecuador.com	Quito	Loja	Sudan.net	Khartoum	Omdurma
6	Iran.com	Ahar	Kilan	Taiwan.net	Kaohsiung	Taipei
7	India.com	Mumbai	Delhi	Fiji.net	Suva	Lami
8	Cameroon.com	Douala	Yaounde	Vietnam.net	Hanoi	Haiphong
9	Chile.com	Santiago	Arica	Yemen.net	Aden	Sana
10	Cuba.com	Havana	Holguin	Zimbabwe.net	Harare	Bulaway

Вимоги до звіту

1. Зображення топології мережі.

2. Зображення команди ipconfig кожного цільового вузла.

3. Зображення команди ping між комп'ютером PC0 та іншими цільових вузлів.

4. Зображення вікна конфігурації кожної поштової скриньки відповідно до п.7.

5. Зображення вікна панелі моделювання відповідно до п.10. Зображення структури пакета і його проходження через рівні мережевої моделі OSI.

6. Загальні висновки по роботі.

Контрольні запитання

1. Що таке електронна пошта?

2. Для чого використовуються поштові скриньки?

3. Які кроки є в процесі налаштування клієнтського програмного забезпечення для роботи з електронною поштою?

4. У чому різниця між поштовими протоколами?

ЛАБОРАТОРНА РОБОТА № 9
НАСТРОЮВАННЯ ТА ВИКОРИСТАННЯ СЛУЖБИ DHCP

Мета роботи: ознайомитись з технологією DHCP, принципом його роботи протоколу DHCP, навчитись використанні технологію DHCP.

Теоретичні відомості

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) – це мережевий протокол, який дозволяє комп'ютерам автоматично отримують IP-адресу та інші параметри, що необхідні для роботи в мережі TCP/IP. Цей протокол працює за моделлю «клієнт-сервер». Для автоматичної конфігурації комп'ютер-клієнт на етапі налаштування мережевого пристрою звертається до так званого DHCP-сервера і отримує від нього необхідні параметри. Мережний адміністратор може задати діапазон адрес, які розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі і зменшує кількість помилок. Протокол DHCP використовується в більшість мереж TCP/IP.

DHCP є розширенням протоколу BOOTP, який використовувався раніше забезпечення бездискових робочих станцій IP-адресами, при їх завантаженні. DHCP підтримує зворотну сумісність з BOOTP.

Протокол DHCP надає три способи розподілу IP-адрес:

1) Ручний розподіл. За допомогою цього методу адміністратор мережі співставляє апаратній адресі (для мереж Ethernet це MAC-адреса) кожного клієнтського комп'ютера певну IP-адресу. Цей спосіб виділення адрес відрізняється від ручної конфігурації кожного комп'ютера лише том, що інформація про адресу зберігається централізовано (на DHCP-сервері) і, отже, її легше змінювати, коли виникає така потреба

2) Автоматичний розподіл. За допомогою цього методу кожному комп'ютеру для постійного використання виділяється довільна IP-адреса з діапазону, визначеного адміністратором.

3*) Динамічний розподіл.* Цей метод схожий на автоматичний розподіл, за винятком того, що адреса не видається комп'ютеру для постійного користування,

а на певний період. Це називається орендою. Після закінчення терміну оренди IP-адреса знову вважається вільною, і клієнт зобов'язаний запросити новий (віна може бути такою ж). Крім того, клієнт сам може відмовитися від отриманої адреси.

Деякі реалізації DHCP-сервісів здатні автоматично здатні оновлювати записи DNS, які відповідають клієнтським комп'ютерам, при виділенні їм нових адрес.

Процес отримання IP-адреси клієнтом з DHCP-сервера складається з чотирьох етапів.

1. Виявлення DHCP. Спочатку клієнт виконує запит через всю фізичну мережу, щоб виявити доступний DHCP-Сервері.

2. DHCP-пропозиція. Сервер отримує повідомлення від клієнта та визначає необхідну конфігурацію клієнта відповідно до вказаних мережним адміністратором настройок. Клієнт може отримати кілька різні пропозиції DHCP з різних серверів. З них він повинен обрати той, який йому підходить.

3. DHCP-запит. Вибравши одну з конфігурацій, пропонованих DHCP-серверами, клієнт надсилає DHCP-запит. Він розсилається широковещательно; при цьому до опцій що вказав клієнт в повідомленні, додається спеціальна опція – ідентифікатор сервера – адреса DHCP-сервера, вибраного клієнтом.

4. Підтвердження DHCP. Сервер підтверджує запит і відправляє підтвердження клієнту. Після цього клієнт повинен налаштувати мережевий інтерфейс за допомогою наданих параметрів.

Крім повідомлень, необхідних для отримання IP-адреси клієнтом, DHCP передбачає декілька додаткових повідомлень для виконання інших задач

1) Відмова DHCP. Якщо після отримання підтвердження від сервера клієнт виявляє, що адреса, вказана сервером, вже використовується в мережі, він транслює повідомлення про помилку DHCP, а потім процедура отримання IP-адреси повторюється. Використання IP-адреси для інших користувачем можна виявити відправивши запит ARP.

2) Повідомлення відміни DHCP. При отриманні такого повідомлення клієнт повинен повторити процедуру отримання адреси.

3) Звільнення DHCP. Клієнт може явно припинити оренду IP-адреси Для цього він надсилає повідомлення DHCP серверу, який надає йому цю адресу в оренду. На відміну від інших DHCP-повідомлень, це повідомлення не транслюється.

4) Відомості DHCP. Інформаційне повідомлення DHCP призначене для визначення додаткові параметри TCP/IP (наприклад, адреси маршрутизатора за замовчуванням, DNS-сервери і т. д.) тими клієнтами, які не потребують динамічної IP-адреси (тобто адреса яких налаштована вручну). Сервери відповідають на цей запит повідомленням-підтвердження без виділення IP-адреси.

Практична частина

Нехай є мережа 192.168.1.0 з маскою 255.255.255.0, що складається з трьох настільних комп'ютерів, трьох ноутбуків, комутатора, роутера і сервера. Необхідно настроїти DHCP-сервер і встановити автоматичне присвоєння IP-адрес ноутбукам.

1. Додаємо робоче поле програми Packet Tracer три стаціонарних комп’ютери (PC0 – PC2), три ноутбуки (Laptop0 – Laptop2), комутатор 2960-24TT (Switch0), роутер Generic Router-PT-Empty (Router0) і сервер Generic Server-PT (Server0).

2. Додаємо один Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE в роутер для підключення до мережі. Для цього відкрийте властивості Router0, на вкладка *Physical* на моделі роутера натискаємо кнопку живлення для завершення роботи, вибираємо вказаний модуль з'єднання та встановлюємо його в у вільний слот.

3. Підключаємо всі пристрої за допомогою крученої пари. Порти підключення роутера і комутатора – GigabitEthernet, інших пристроїв та комутатор – FastEthernet. Топологія мережевої моделі представлена на рис. 9.1.

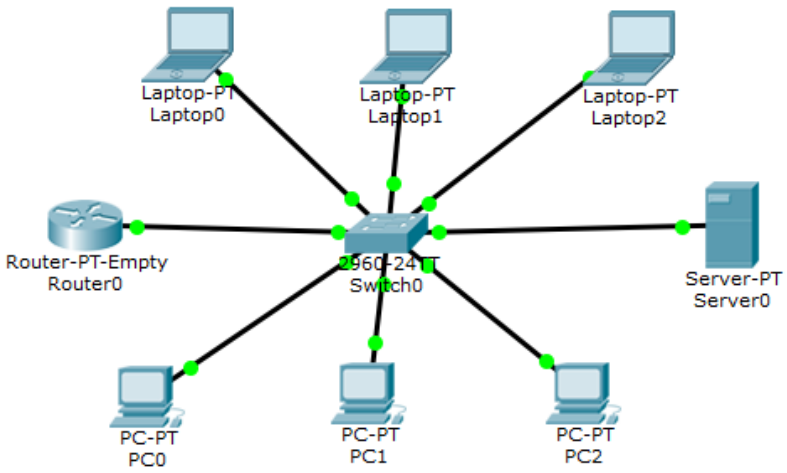


Рис. 9.1. Топологія мережі

4. Зберігаємо створену топологію.

5. Налаштовуємо елементи мережі. Резервуємо для маршрутизатора першу доступна IP-адресу, для сервера - другу, а стаціонарні комп'ютери будуть отримувати адреси послідовно починаючи з третьої доступної. Маска мережі для всіх пристроїв – 255.255.255.0.

6. Щоб налаштувати PC0, відкриваємо його властивості. На вкладці *Desktop* вибираємо параметр *IP Config* і для режиму отримання IP-адреси Static в поле IP-адреса водимо третю доступну мережеву адресу – 192.168.1.3, в поле *Subnet Mask* –255.255.255.192, а в поле за *Default Gateway* – першу доступну IP-адресу мережі, зарезервовану для роутера – 192.168.1.1. Інші настільні комп'ютери налаштовуємо аналогічно.

7. Налаштовуємо роутер. Для цього відкриємо його властивості, переходимо до вкладки *Config* та в підменю *INTERFACE* вибираємо модуль *GigabitEthernet0/0*, до якого підключено комутатор. У поле *IP Address* – вводимо першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – 255.255.0 та включаємо цей модуль – *Port Status* встановлено на значення On.

8. Щоб налаштувати сервер, відкриваємо його властивості, переходимо на вкладку *Config* та в підменю *INTERFACE* вибираємо модуль *FastEthernet0*. У поле *IP Address* – вводимо другу зарезервовану IP-адресу мережі – 192.168.1.2, в *Subnet Mask* – 255.255.255.0 та включаємо даний модель.

9. Настроюємо сервис DHCP. Для цього відкриємо вкладку *Services* виберемо підменю *DHCP*. Для включення перемикач *Service* встановлюємо в положення *On*. Призначимо ім'я пулу для роздачі адрес – у поле *Pool Name* введіть *APP_Pool;* в поле *Default Gateway* – IP-адресу роутера 192.168.1.1. Для автоматичного розподілу виділимо адреси починаючи з шостої доступної адреси мережі: в поле *Start IP Address* введемо 192.168.1.6; в поле У полі *Subnet Mask* – маску мережі 255.255.255.0; натискаємо кнопку *Add* і в в DHCP-таблиці зявиться відповідний запис.

9. Налаштуємо ноутбуки для автоматичного отримання IP-адреси. Для laptop0 даємо його властивості та на вкладці *Desktop* виберемо пункт *IP Config* та активуємо режим отримання IP-адреси DHCP. Через деякий час в полях *IP Address* та *Subnet Mask* з'являться мережеві параметри. У нашому випадку це перша IP-адреса, доступна для автоматичне призначення – 192.168.1.6 та маска мережі – 255.255.255.0.

Решта ноутбуків налаштовуємо аналогічно. Перевірити призначені адреси можна використавши засіб Inspect/Port Status Summary Table.

10. Перевірте працездатність мережі. Зайдемо на PC0 і пропінгуємо Laptop0. Результати виконання команди *ping*:

PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:

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

Approximate round trip times in milli-seconds:

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

Такий результат роботи вказує на те, що параметри мережних пристроїв є правильними.

Завдання для індивідуальної роботи

1. Створіть мережу відповідно до топології, показаної на рис. 9.1.

2. Призначте статичні IP-адреси цільовим вузлам відповідно до варіанту (табл. 9.1):

- призначте першу доступну адресу інтерфейсу роутера;
- призначити другу доступну адресу інтерфейсу сервера;
- призначте PC0 третю доступну адресу;;
- призначте PC1 четверту доступну адресу;
- призначте PC2 п'яту доступну адресу.

Таблиця 9.1. Параметри завдання

№ варіанту	**Адреса мережі**	**Маска мережі**
1	44.16.105.0	255.255.255.128
2	45.16.115.0	255.255.255.192
3	46.16.125.0	255.255.255.224
4	47.16.135.0	255.255.255.128
5	48.16.145.0	255.255.255.192
6	49.16.155.0	255.255.255.224
7	50.16.165.0	255.255.255.128
8	51.16.175.0	255.255.255.192
9	52.16.185.0	255.255.255.224
10	53.16.195.0	255.255.255.128

3. Налаштуйте Server0 сервіс DHCP.

4. У режимі симуляції налаштуйте Laptop0 на динамічне отримання IP-адреси. Відстеж рух пакетів за допомогою протоколу DHCP. Налаштуйте решту ноутбуків в мережі для динамічного отримання IP-адрес.

5. Перевірте настройки комп'ютера за допомогою команди *ipconfig /all.*

7. Перевірте працездатність мережі – пропінгуйте з першого стаціонарного комп’ютера всі вузли.

Вимоги до звіту

1. Скрін топології мережі.

2. Скрін результату виконання команди *ipconfig* кожного кінцевого вузла.

3. Скрін результату виконання команди *ping* між першим та іншими вузлами.

4. Скрін вікна панелі симуляції відповідно до пункту 4.

5. Загальні висновки по роботі.

Контрольні запитання

1. Що таке DHCP?

2. Для чого використовується DHCP?

3. Які етапи процесу отримання клієнтом IP-адреси з сервера DHCP?

4. Які повідомлення надсилає DHCP для виконання завдань, що не пов'язані з отриманням IP-адреси?

ЛАБОРАТОРНА РОБОТА № 10
НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ СЛУЖБИ DNS

Мета роботи: ознайомитись з принципом функціонування доменної системи імен (DNS), навчитися налаштовувати DNS-сервер.

Теоретичні відомості

DNS (англ. Domain Name System – система доменних імен) – комп'ютерна розподілена система для отримання інформації про домени. Найчастіше використовується для отримання IP-адреси за іменем хоста (комп'ютера або пристрою), отримання інформації про маршрутизацію пошти та обслуговуючих вузлів для протоколів у домені (SRV-запис).

Розподілена база даних DNS підтримується з допомогою єрархії DNS-серверів, що взаємодіють за певним протоколом.

Основою DNS є уявлення про ієрархічну структуру доменного імені та зон. Кожен сервер, відповідальний за ім'я, може делегувати відповідальність за подальшу частину домену іншому серверу, що дає можливість покласти відповідальність за актуальність інформації на сервери різних організацій, відповідальних тільки за «свою» частину доменного імені.

Домен (англ. domain – область) – це вузол у дереві імен разом з усіма підпорядкованими йому вузлами (якщо такі є), тобто іменована гілка або підгілка в дереві імен. Структура доменного імені відображає порядок слідування вузлів в ієрархії. Доменне ім'я читається зліва направо від низькорівневих доменів до доменів верхнього рівня (за зростанням значимості): зверху знаходиться кореневий домен (не має ідентифікатора), далі йдуть домени першого рівня (доменні зони), потім – домени другого, третього і наступних рівнів. (наприклад, для адреси *zu.edu.ua.* домену першого рівня *ua*, другого – *edu*, третього – *ua*.

Піддомен (англ. subdomain) – підпорядкований домен (наприклад, *edu.ua* піддомен домену *ua*, а *zu.edu.ua* – піддомен домену *edu.ua.* Теоретично такий поділ може мати до 127 рівнів, а кожна мітка може містити до 63 символів, поки загальна довжина доменного імені разом із крапками не досягне 254 символів. На практиці реєстратори доменних імен використовують більш суворі

обмеження. Наприклад, якщо у вас є домен форми, mydomain.ua то можна створити для нього різні піддомени виду mysite1.mydomain.ua виду, mysite2.mydomain.ua і ін.

DNS-сервер – спеціалізоване ПЗ для обслуговування DNS, а також комп'ютер, на якому це програмне забезпечення працює. DNS-сервер може відповідати за певні зони та/або може перенаправляти запити вище стоячим серверам.

DNS-клієнт – спеціалізована бібліотека (або програма) для робота з DNS. У деяких випадках DNS-сервер діє як DNS-клієнт.

DNS-запит – запит від клієнта (або сервера) до сервера. Запит може бути рекурсивним або не рекурсивним.

Термін *рекурсія* в DNS відноситься до алгоритму поведінки DNS-сервера, при якій сервер виконує від імені клієнта пошук інформації по всій системі DNS, при необхідності звертаючись до інших DNS-серверів. При відповіді на нерекурсивний запит або при забороні виконати рекурсивний запит, DNS-сервер або повертає дані про зону, за яку він відповідає, або повертає помилку. Налаштування нерекурсивного сервера, коли при відповіді видаються адреси серверів, які володіють більшим об’ємом інформації про запитувану зону, ніж сервер що відповідає (адреси кореневих серверів), є некоректними і такий сервер може бути використаним для організації DoS-атак.

У разі рекурсивного запиту DNS-сервер опитує сервери (у порядку спадання рівня зони в імені), поки відповідь не буде знайдена або не виявиться, що домену не існує. На практиці пошук починається з найближчих до шуканого DNS-серверів. Якщо інформацію про них є у кеші і не застаріла, сервер може не запитувати інші DNS-сервери.

Іноді допускається, що б запитаний сервер передавав рекурсивний запит на DNS-сервер «вищестоячому» і чекав готову відповідь.

При рекурсивній обробці запитів всі відповіді проходять через DNS-сервер, і він отримує можливість кешувати їх. Повторно запитувати на ті ж імена

зазвичай не виходять за межі кешу сервера. Допустимий час збереження відповідей в кеші надходить разом з відповіддю (поле TTL рекурсивного запису).

Рекурсивні запити вимагають від сервера більше ресурсів (і створюють більше трафіку), тому зазвичай беруться з «відомих» серверу вузлів (наприклад, провайдер надає можливість робити рекурсивні запити тільки до своїх клієнтів, в корпоративній мережі рекурсивні запити приймаються тільки з локального сегмента). Нерекурсивні запити, як правило, приймаються з усіх вузлів мережі (відповідь надається лише на запити про зону, розміщену на вузлі, на DNS-запити про інші зони зазвичай повертають адреси інших серверів).

DNS використовується в основному для перетворення символьних імен в IP-адреси, але він також може виконувати і зворотний процес. Для цього використовуються вже наявні засоби DNS.

Ім'я та IP-адреса не ідентичні – одна IP-адреса може мати кілька імен, що дозволяє підтримувати на одному комп'ютері багато веб-сайтів (це називається віртуальним хостингом). Зворотне теж можливе – одному імені може відповідати кілька IP-адрес. Це дозволяє балансувати навантаження.

Практична частина

Нехай існує мережа 192.168.1.0 з мережною маскою 255.255.255.0, що складається з двох настільних комп'ютерів, двох ноутбуків, комутатора та сервер. Потрібно настроїти DNS-сервер.

1. Додаємо на робочу область програми Packet Tracer два стаціонарних комп'ютер (PC0 і PC1), два ноутбуки (Laptop0 і Laptop1), комутатор 2960-24TT (Switch0) і сервер Generic Server-PT (Server0)

2. Всі пристрої підключаємо до комутатора витою парою. Порти підключення – FastEthernet. Топологія мережевої моделі представлена на рис. 10.1.

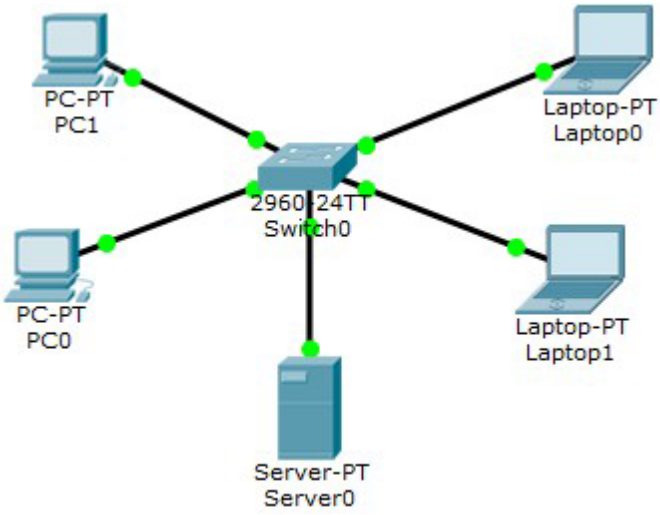


Рис. 10.1. Топологія мережі

3. Зберігаємо створену топологію.

4. Налаштовуємо елементи мережі. Зарезервуємо для сервера першу доступну IP-адресу, а комп’ютерам будемо надавати адреси послідовно починаючи з другої доступної. Мережна маска для всіх пристроїв – 255.255.255.0. Даємо комп’ютерам імена, які будемо використання в запитах замість IP-адрес: PC0 – APP1, PC1 – APP2, Laptop0 – APP3, Laptop1 – APP4.

5. Щоб налаштувати PC0, відкриємо його властивості та на вкладці *Desktop* виберемо пункт *IP Config* та для режиму отримання IP-адреси *Static* в поле *IP Address* введемо другу доступну мережеву адресу – 192.168.1.2, в поле *Subnet Mask* – маску мережі 255.255.255.192, а в поле DNS-сервер вкажемо першу доступна IP-адресу мережі, зарезервовану для сервера – 192.168.1.1. Ім'я комп'ютера можна змінити на вкладці *Config* в підменю *Global Setting* – у полі *Display Name* введемо APP1. Аналогічно налаштовуємо решту комп’ютерів.

6. Налаштуємо сервер. Для цього відкриємо його властивості, перейдемо на вкладку *Config* та в підменю *INTERFACE* виберемо модуль *FastEthernet0*. У поле *IP Address* введемо першу зарезервовану IP-адресу мережі – 192.168.1.1, в поле *Subnet Mask* – маску мережі 255.255.255.0 та включимо даний модуль (*Port Status* встановимо в *On*.

7. Налаштуємо службу DNS. Перейдемо на вкладку *Services* та виберемо підменю *DNS*. Щоб увімкнути сервіс перемикач *DNS Service* встановимо в

положення *On.* Щоб додати перший комп'ютер в DNS-таблицю у поле *Name* внесемо APP1, а в поле *Address* його IP-адресу – 192.168.1.2 та натиснемо кнопку *Add*. В У таблиці DNS з'явиться відповідний запис. Інші пристрої додаємо аналогічно.

8. Перевірте працездатність мережі. Для цього перейдемо до комп'ютера APP1 та пропінгуємо ноутбук APP4. Для цього відкриємо властивості APP1, та на вкладці *Desktop* виберемо пункт *Command Promt* і у командний рядок, що відкриється, введемо команду *ping* і символьне ім'я ноутбука (APP4). Нижче наведено результати виконання команди *ping:*

PC>ping APP4

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Reply from 192.168.1.5: bytes=32 time=1ms TTL=128

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.5:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

Такий результат роботи вказує на те, що параметри мережних пристроїв є правильними.

Завдання для індивідуальної роботи

1. Створіть мережу відповідно до топології, показаної на рис. 10.1.

2. Встановіть всі ПК та ноутбуки довільні імена за типом: "ім'я-ПК" (наприклад, «Алекс-ПК»).

3. Призначте адреси цільовим вузлам відповідно до вказаного варіанту (таблиця 10.1):

- призначте першу доступну адресу в мережі інтерфейсу DNS-сервера;
- призначте PC0 другу доступну адресу;
- призначте PC1 третю доступну адресу;

- призначте останню доступну адресу laptop0;

- призначте передостанню доступну адресу laptop1.

Таблиця 10.1. Параметри завдання

№ варіанту	**Адреса мережі**	**Маска мережі**
1	100.10.15.0	255.255.255.240
2	100.11.15.0	255.255.255.128
3	100.12.15.0	255.255.255.0
4	100.13.15.0	255.255.255.240
5	100.14.15.0	255.255.255.128
6	100.15.15.0	255.255.255.0
7	100.16.15.0	255.255.255.240
8	100.17.15.0	255.255.255.128
9	100.18.15.0	255.255.255.0
10	100.19.15.0	255.255.255.240

4. Налаштуйте на Server0 службу DNS.

5. Перевірте роботоздатність мережі та DNS-сервера пропінгувавши з першого компютера решту вузлів. В якості аргумента команди ping використовуйте символьні імена.

6. У режимі симуляції надішліть запит з символьним іменем з PC0 на Laptop0. Відстежте рух пакетів по протоколах DNS і ICMP.

Вимоги до звіту

1. Зображення топології мережі.

2. Скрін вікна з результатами виконання команди ipconfig зкожного вузла.

3. Скріни вікон з результатами виконання команди ping між першим та іншими вузлами.

4. Зображення вікна *Simulation Panel* відповідно до пункту 6 завдання.

5. Загальні висновки по роботі.

Контрольні запитання

1. Що таке DNS?

2. Для чого використовується DNS?

3. Як спілкуватися в мережі, яка не має DNS-сервера?

4. Що містить таблиця DNS?

5. Що робить локальний DNS-сервер, якщо він не може знайти відповідності у своїй таблиці?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна:

1. Платтнер Б., Чернега В. Безпровідні локальні комп'ютерні мережі: навч. посібник. К.: Кондор, 2018. – 238 с.

2. Микитишин А. Г., Митник М. М., Стухляк П .Д. Комп'ютерні мережі: навч. посібник. для технічних спеціальностей ВНЗ. К.: Магнолія 2006, 2018. – 256 с.

3. Рамський Ю. С. Адміністрування комп'ютерних мереж та систем: навч. посібник. К. : Богдан, 2010. – 196 с.

4. Ахрамович В. М. Комп'ютерні мережі: навч. посібник. К. : ДП «Інформ.-аналіт. агенство», 2010. – 352 с.

5. Комп'ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] – Вінниця: ВНТУ, 2013. – 371 с.

6. Комп'ютерні мережі та комунікації : навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків : НТУ "ХПІ", 2011. – 224 с.

7. Організація комп'ютерних мереж : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

8. Одом Ю. Офіційний посібник Cisco з підготовки до CCENT/CCNA ICNDl 100-101 Acad. Ед.: транс. з англійською мовою / W. Odom. – М.: ТОВ «І. Д. Вільямс», 2015. – 912 с.

9. Бейцун С.В., Кулинич М.В. Моделирование компьютерных сетей: Учебное пособие. – Днепропетровск: НМетАУ, 2016. – 96 с.

Додаткова:

1. Щедріна О. І., Агутін М. М. Інтернет-технології в бізнесі: навч. посібник. – К.: КНЕУ, 2012. – 303 с.

2. Габрусєв В. Ю. Вивчаємо комп'ютерні мережі. – К.: Вид. дім "Шкільний світ", 2005. – 128 с.

3. Комп'ютерні мережі: навч. посіб. для техн. спец. вищ. навч. закл. Кн. 1 / А. Г. Микитишин [та ін.]; М-во освіти і науки України. - Львів : Магнолія 2006, 2017. – 255 с.

4. Дибкова, Л. М. Інформатика і комп'ютерна техніка: навч. посіб. / Л. М. Дибкова. - 2-е вид., переробл. і доповн. - К.: Академвидав, 2007. – 415 с.

5. Швиденко М. З., Матус Ю. В. Комп’ютерні мережні технології. / Навч.-метод. Посібник. – Київ. – ТОВ “Авета”, - 2008.

6. Вікіпедія – вільна енциклопедія [Електроні ресурс]. – Режим доступу: http://wikipedia.org.

Укладачі:
ЯЦЕНКО Олександр Сергійович
ЯЦЕНКО Оксана Іванівна

Комп’ютерні мережі

Частина 1

Моделювання комп’ютерних мереж

Лабораторний практикум

Оформлення випускних відомостей здійснюється видавництвом:

Підп. до друку __.___.2022.

Формат 60х84/16. Папір офсетний Гарнітура Times New Roman Cyr. Друк різографічний.

Ум. друк. арк.____ Обл.-вид. арк. _____

Наклад 50 пр.

Зам. № _____

Видавництво Житомирського державного університету імені Івана Франка

10008, м. Житомир, вул. Велика Бердичівська, 40

Свідоцтво суб’єкта видавничої справи:

ЖТ № 10 від 07.12.2004 р.

електронна пошта (E-mail): zu@zu.edu.ua