Міністерство освіти і науки України

Центральноукраїнський національний технічний університет

О.К. Дідик, О.М. Сербул, І.А. Березюк

ТЕЛЕКОМУНІКАЦІЇНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ

Навчальний посібник

Кропивницький 2023 р.

УДК 004.716

Рекомендовано Вченою радою Центральноукраїнського національного технічного університету як навчальний посібник для студентів денної та заочної форми навчання першого (бакалаврського) освітнього рівня галузі знань 17 – «Електроніка та телекомунікації» спеціальності 174 – «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» у вищих навчальних закладах III-IV рівня акредитації.

(Протокол №9 від 29.05.2023 р.)

Рецензенти:

В.О. Кондратець – доктор техн. наук, професор, академік Академії інженерних наук України, професор кафедри автоматизації виробничих процесів Центральноукраїнського національного технічного університету,

О.А. Смірнов доктор техн. наук, професор, член Експертної ради МОН з експертизи проектів наукових робіт за напрямом 05 – електроніка, радіотехніка та телекомунікації, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Телекомунікаційні та інформаційні мережі: Навчальний посібник. / Дідик О.К., Сербул О.М., Березюк І.А., Центральноукраїнський національний технічний університет. – Кропивницький: ЦНТУ, 2023 – 124 с.

Навчальний посібник укладено у відповідності до змісту навчальної дисципліни «Телекомунікаційні та інформаційні мережі», містить опис варіантів структурної побудови та архітектурного описання, технологій і протоколів сучасних телекомунікаційних та інформаційних мереж.

ЗМІСТ

ВСТУП

Дисципліна «Телекомунікаційні та інформаційні мережі» вивчається студентами спеціальності 174 – Автоматизація, комп’ютерноінтегровані технології та робототехніка. Метою її вивчення є формування у студентів здібностей самостійно, творчо застосовувати на практиці теоретичні знання, отримані як при вивченні даної дисципліни, так і при вивченні дисциплін «Теорія інформації», «Основи збору передачі та обробки інформації», «Основи комп'ютерної схемотехніки» та «Операційні системи». Даний посібник укладено на основі багаторічної розробки та удосконалення навчально-методичного комплексу дисципліни “Телекомунікаційні та інформаційні мережі” [3, 6]. У процесі опрацювання матеріалів за посібником студенти отримують можливість придбати теоретичні та практичні навички в області прийняття технічно обґрунтованих рішень при комплексній розробці обчислювальних мереж з обліком їх апаратної і програмної складових.

Вивчення теоретичного матеріалу охоплює огляд топологій комп’ютерних мереж, аналіз способів адресації мереж TCP/IP, аналіз способів маршрутизації, огляд протоколів DNS та DHCP, огляд технологій Ethernet та Wi-Fi. Опрацювання практичних завдань дозволить здобувачам здійснювати вибір топології мережі та додаткових мережних пристроїв, розподіляти адресний простір та налаштовувати вузли мережі, організувати маршрутизацію, налаштовувати мережі Internet, описувати функціонування мережних пристроїв під час відображення Web-сторінки, розробляти структурні електричні схеми обчислювальної мережі та налаштовувати всі її елементи, оформляти графічні матеріали та технічну документацію за результатами проектування.

Підсумком вивчення матеріалів за даним посібником є набуття здобувачами вміння розробляти локальну мережу невеликого підприємства, у якого кожен підрозділ розміщений в окремому кабінеті і має певний набір обладнання не з’єднаного локальною мережею, логічно структурувати локальну мережу для підрозділів, створенням власної підмережі, підключати дану локальну мережу до глобальної мережі Internet, за умови отримання підприємством у провайдера виділеного пулу адрес.

1. Мережний симулятор Cisco Packet Tracer"

Симулятор Cisco Packet Tracer дозволяє проектувати свої власні мережі, створюючи і відправляючи різноманітні пакети даних, зберігати і коментувати свою роботу. З його допомогою можна вивчати і використовувати такі мережні пристрої, як комутатори другого і третього рівнів, робочі станції, визначати типи зв'язків між ними і з'єднувати їх. Після того, як мережа спроектована, можна приступати до конфігурації вибраних пристроїв за допомогою термінального доступу або командного рядка.

Відмінною особливістю даного симулятора є наявність у ньому "Режиму симуляції". У даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно [1, 2] Ця можливість дозволяє наочно продемонструвати, з якого інтерфейсу в даний момент часу переміщається пакет, який протокол використовується і т.д.

Однак, це не всі переваги Packet Tracer: у "Режимі симуляції" є можливість не лише відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний.

Всі параметри і команди Packet Tracer відображаються із рядка меню (рис. 1.1):

- команди меню ***File*** дозволяють створити новий проект, відкрити збережений проект, зберегти проект, роздрукувати та вийти з програми.

- команди меню ***Edit*** (правка) дозволяють вирізати, копіювати і відміняти події;

- у вікні ***Options*** (параметри) можливо змінювати налаштування Packet Tracer (*Options → Preferences*).

В основній панелі інструментів знаходяться ярлики команд, такі як ***New*** (створити), ***Open*** (відкрити), ***Save*** (зберегти), ***Cut*** (вирізати), ***Paste*** (вставити) та ***Zoom*** (масштабування). Тут також знаходяться ярлик ***Custom Device*** (користувацький пристрій), що дозволяє створювати користувальницькі конфігурації апаратного забезпечення.

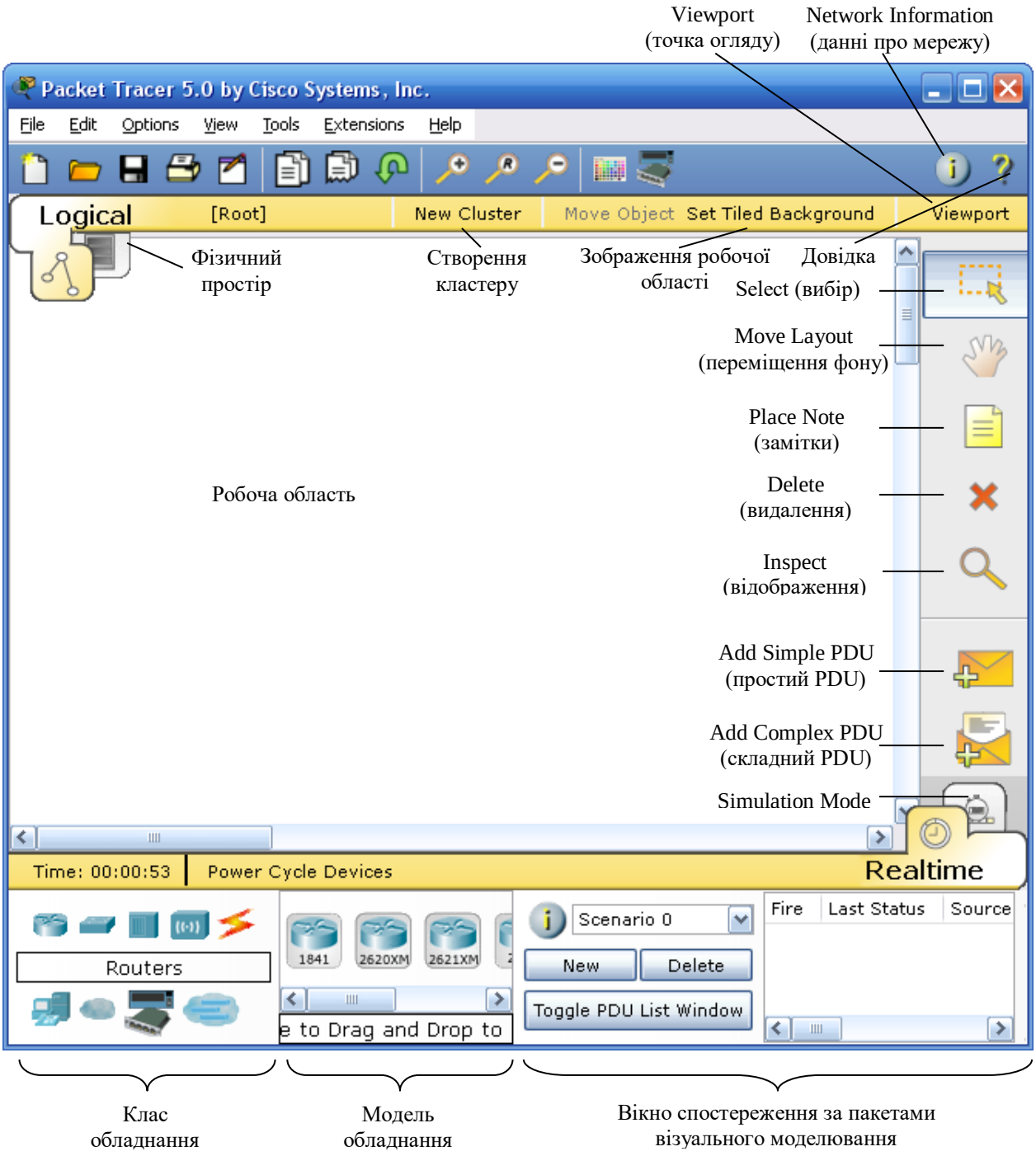


Рисунок 1.1 – Вікно програми Packet Tracer.

Інформацію про топологію мережі можна ввести у вікні ***Network Information*** (данні про мережу).

Ярлик довідки знаходиться поряд з кнопкою ***Network Information***.

З допомогою кнопки ***Set Tiled Background*** (фон) можливо змінювати фонове зображення робочої області.

Параметр ***New Cluster*** (створити кластер) дозволяє групувати пристрої та економити робочу область.

Параметр ***Viewport*** (точка огляду) дозволяє масштабувати представлені мережі.

Вкладка фізичного простору дозволяє перейти у вікно фізичної області, де вказано розміри логічної топології мережі. Воно створює відчуття простору та дозволяє відобразити знаходження пристроїв та мереж [3].

В загальній панелі інструментів знаходяться всі команди, що використовуються в робочому полі Packet Tracer (рис. 1):

- ***Select*** (вибір) дозволяє перетягувати, виділяти і вибирати пристрої та бездротові канали;

- ***Move Layout*** (переміщення фону) дозволяє переміщувати робочу область;

- ***Place Note*** (замітки) дозволяє робити замітки в робочій області:

- ***Delete*** (видалення) дозволяє видаляти пристрої та бездротові канали;

- ***Inspect*** (відображення) дозволяє проглядати різні таблиці пристроїв;

- ***Add Simple PDU*** (добавити простий PDU) дозволяє формувати простий пакет ICMP даних між двома вузлами;

- ***Add Complex PDU*** (добавити складний PDU) дозволяє формувати складний пакет ICMP даних між пристроями.

- ***Power Cycle Devices*** кнопка вмикання та вимикання всіх пристроїв в робочій області.

Вкладка Simulation Mode дозволяє перейти в режим моделювання. Цей режим дозволяє відслідковувати мережний трафік в повільному, детальному режимі.

У вікні "Клас обладнання" відображається дев’ять класів. Докладніше про головні класи:

Роутер (маршрутизатор) – мережний пристрій, на підставі інформації про топологію мережі і певних правил приймає рішення про пересилання пакетів мережного рівня (рівень 3 моделі OSI) між різними сегментами мережі. Зазвичай маршрутизатор використовує адресу одержувача, вказану в пакетах даних, і

визначає за таблицею маршрутизації шлях, за яким слід передати дані. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, пакет відкидається. В Packet Tracer у вікні моделей роутери відрізняються лише набором інтерфейсів і можливістю встановлення плат розширення.

Світч (комутатор) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегменту мережі (рівень 2 моделі OSI). Світч відрізняється від роутера тим, що не може поєднувати різні мережі (роз'єми всі однакові). Комутатор зберігає в пам'яті таблицю комутації (зберігається в асоціативній пам'яті), в якій вказується відповідність MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі інформація, що поступає на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри (фрейми) і, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача не асоціюється з яким-небудь портом комутатора, то кадр буде відправлений на всі порти. З часом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується. Варто відзначити малу латентність (затримку) і високу швидкість пересилання на кожному порту інтерфейсу. В Packet Tracer принципової різниці між моделями комутатора немає але в моделі 3560 існує багаторівнева комутація.

Хаб (концентратор) – мережний пристрій, призначений для об'єднання кількох пристроїв Ethernet в спільний сегмент мережі. Пристрої підключаються за допомогою витої пари, коаксіального кабелю чи оптоволокна. Концентратор працює на фізичному рівні мережевої моделі OSI, повторює надісланий на один порт сигнал, на всі активні порти. У разі надходження сигналу на два і більше портів одночасно, виникає колізія, і передані кадри даних втрачаються. Таким чином, всі підключені до концентратора пристрої знаходяться в одному домені колізій. На відміну від хабу, світч запам'ятовує MAC-адреси комп'ютерів в кеші і

посилає тільки в порт, відповідний MAC-адресі одержувача. Крім того, пакети буферизуються, що виключає колізії.

Кабелі (з'єднувачі) в Packet Tracer є декількох типів:

- автоматичний – програма автоматично підбирає потрібний тип кабелю (для новачків);

- консольний – з'єднує комп'ютер – роутер;

- прямий патч-корд – з'єднує: комп'ютер – світч та роутер – світч;

- кросовий патч-корд – з'єднує комп'ютер – комп'ютер, світч – світч, роутер–роутер та роутер – комп'ютер;

Кінцеві пристрої – в Packet Tracer це комп'ютер, сервер, принтер та телефон.

Практичне завдання 1.

1. Запустити Cisco Packet Tracer.

2. У вікні "Клас обладнання" вибрати піктограму ***End Devices*** (Кінцеві пристрої), а у вікні "Модель обладнання" клацнути ЛК миші на ***PC-PT*** (Комп'ютер), а потім клацнути ЛК миші в робочій області, з'явиться один комп'ютер.

3. Встановити ще один комп'ютер в робочій області.

4. З'єднати два комп'ютери між собою автоматичним або кросовим патч-корд кабелем (при використанні кабелю кросовий патч-корд вибирати гніздо FastEthernet), як це показано на рис. 1.2.

5. Надати першому комп'ютеру IP- адресу та маску мережі. Клацнути ЛК миші по комп'ютеру. З'явилося вікно, в якому потрібно вибрати вкладку ***Desktop***, а в ній вибрати піктограму ***IP Configuration***.

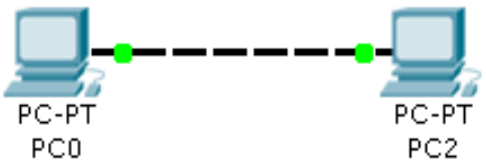


Рисунок 1.2 – Два комп'ютера з'єднані кабелем.

6. В рядку IP Adress задати адресу комп'ютера в форматі ***192.168.0.*****[**варіант по списку**]**.

7. В рядку Subnet Mask клацнути ЛК миші і програма сама впише потрібне значення.

8. Задати другому комп'ютеру IP- адресу в форматі ***192.168.0.*****[**варіант по списку+1**]** аналогічно пунктам 5 – 7.

9. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP- адреса комп'ютера PC2]

10. В правому нижньому куту програми натиснути на піктограму ***Simulation Mode*** (Shift + S). З'явиться вікно, з допомогою якого відбувається симуляція мережі.

11. Натиснути ЛК миші на простий ***ping***-запит (Закритий конверт), курсор змінить свою форму. Далі клацнути на перший комп'ютер, а потім на другий. В результаті на першому комп'ютері буде намальовано конверт.

12. У вікні симуляції натиснути на кнопку ***Auto Capture/Play***, що запустить симуляцію мережі.

13. Поспостерігати за пакетом та пояснити хід цієї передачі.

14. Зберегти файл та продемонструвати викладачеві.

Питання для самоконтролю.

1. Які пристрої знаходяться в стимуляторі Packet Tracer?
2. Що відбувається в "Режимі симуляції"?
3. Що називається маршрутизатором?
4. Що називається комутатором?
5. Що називається концентратором?
6. Які кабелі є в стимуляторі Packet Tracer?

2. Колізія. Методи боротьби з нею (метод доступу CSMA/CD)

Колізія – це нормальна ситуація в роботі мереж Ethernet. Колізію породжує одночасна передача даних декількома вузлами. Для виникнення колізії не обов'язково, щоб кілька станцій почали передачу абсолютно одночасно, така ситуація малоймовірна. Набагато ймовірніше, що колізія виникає через те, що один вузол починає передачу раніше іншого, але до іншого вузла сигнали першого просто не встигають дійти за той час, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії – це наслідок розподіленого характеру мережі [4].

Метод доступу CSMA/CD. Щоб коректно обробити колізію, усі станції одночасно спостерігають за сигналами, які виникають на кабелі. Якщо передані сигнали і сигнали, що спостерігаються, відрізняються, то фіксується виявлення колізії (collision detection, CD). Для збільшення імовірності якнайшвидшого виявлення колізії всіма станціями мережі, станція, яка знайшла колізію, перериває передачу свого кадру (у довільному місці, можливо, і не на межі байта) і підсилює ситуацію колізії посилкою в мережу спеціальної послідовності з 32 біт, названою jam-послідовністю.

Після цього передавальна станція, що знайшла колізію, зобов'язана припинити передачу і зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища і передачі кадру. Випадкова пауза вибирається за наступним алгоритмом:

Пауза = L x (інтервал відстрочки),

де інтервал відстрочки дорівнює 512 бітовим інтервалам (у технології Ethernet прийнято всі інтервали вимірювати в бітових інтервалах; бітовий інтервал позначається, як bt і відповідає часу між появою двох послідовних біт даних на кабелі; для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс чи 100 нс); L представляє собою ціле число, обране з рівною імовірністю з діапазону [0, 2N], де N – номер повторної спроби передачі даного кадру: 1, 2,…, 10.

Після 10-ї спроби інтервал, з якого вибирається пауза, не збільшується. Таким чином, випадкова пауза може приймати значення від 0 до 52,4 мс.

Якщо 16 послідовних спроб передачі кадру викликають колізію, то передавач повинен припинити спроби і відкинути цей кадр. З опису методу доступу видно, що він носить імовірнісний характер, і ймовірність успішного одержання у своє розпорядження загального середовища залежить від завантаженості мережі, тобто від інтенсивності виникнення у станціях потреби передачі кадрів. При розробці цього методу наприкінці 70-х років передбачалося, що швидкість передачі даних у 10 Мбіт/с дуже висока порівняно з потребами комп'ютерів у взаємному обміні даними, тому завантаження мережі буде завжди невеликим [3, 4]. Це припущення залишається іноді справедливим і донині, однак з'явилися додатки, що працюють у реальному масштабі часу з мультимедійною інформацією, що дуже завантажують сегменти Ethernet. При цьому колізії виникають набагато частіше. При значній інтенсивності колізій корисна пропускна здатність мережі Ethernet різко падає, тому що мережа майже постійно зайнята повторними спробами передачі кадрів. Для зменшення інтенсивності виникнення колізій потрібно або зменшити трафік, скоротивши, наприклад, кількість вузлів у сегменті, або підвищити швидкість протоколу, наприклад перейти на Fast Ethernet.

Слід зазначити, що метод доступу CSMA/CD загалом не гарантує станції, що вона коли-небудь зможе одержати доступ до середовища. Звичайно, при невеликому завантаженні мережі ймовірність такої події невелика, але при коефіцієнті використання мережі, що наближається до 1, така подія стає дуже ймовірною. Цей недолік методу випадкового доступу – плата за його надзвичайну простоту, яка зробила технологію Ethernet дуже недорогою. Інші методи доступу – маркерний доступ мереж Token Ring і FDDI, метод Demand Priority мереж 100VG-AnyLAN – позбавлені цього недоліку [5].

Практичне завдання 2.

Потрібно створити локальну мережу, в яку будуть входити: два концентратори Hub-PT та п’ять комп’ютерів PC–PT та локальну мережу, в яку будуть входити: два комутатори 2960-24TT та п’ять комп’ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 2.1.

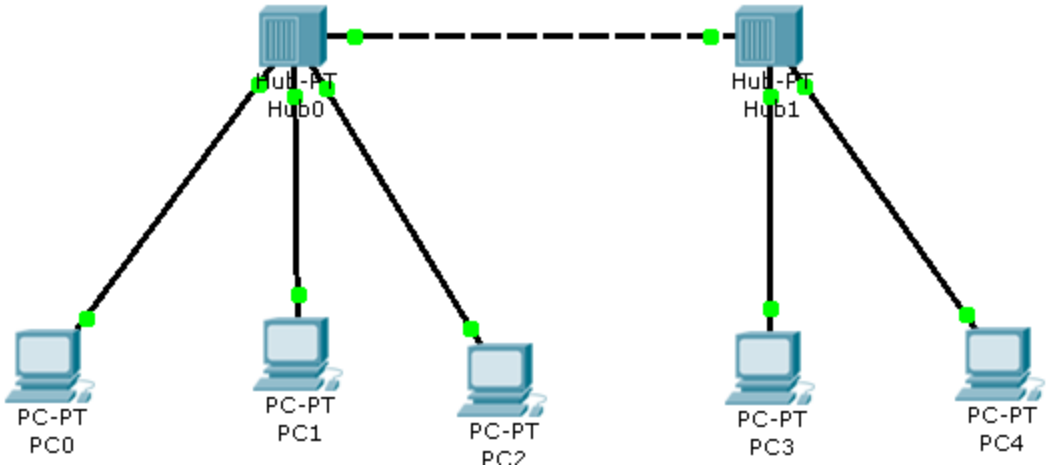


Рисунок 2.1 – Схема локальної мережі для завдання 2.

2. У вікні "Клас обладнання" вибрати піктограму ***End Devices*** (Кінцеві пристрої), з вікна "Модель обладнання" перетягнути п’ять ***PC-PT*** (Комп’ютер) в робоче поле.

3. У вікні "Клас обладнання" вибрати піктограму ***Hubs*** (Концентратори), з вікна "Модель обладнання" перетягнути два ***Hub-PT*** (Концентратор) в робоче поле.

4. З’єднати два концентратори між собою автоматичним або кросовим патч-корд кабелем, а комп’ютер з концентратором з’єднати з допомогою кабеля з прямим з’єднанням контактів, як це показано на рис. 2.1.

5. Задати для кожного комп’ютера IP-адресу та маску підмережі згідно варіанту обраного з табл.. 2.1 варіанту.

6. В правому нижньому куту програми натиснути на піктограму ***Simulation Mode*** (Shift + S). З’явиться вікно, з допомогою якого відбувається симуляція мережі.

7. Натиснути ЛК миші на простий ping-запит (Закритий конверт), курсор змінить свою форму. Далі клацнути на ***PC0-PC4***. Потім знову натиснути на простий ping-запит потім ***PC3-PC1***.

8. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі.

9. Поспостерігати за пакетом та пояснити хід цієї передачі.

10. В середовищі Packet Tracer побудувати мережу, що показана на рис. 2.2.

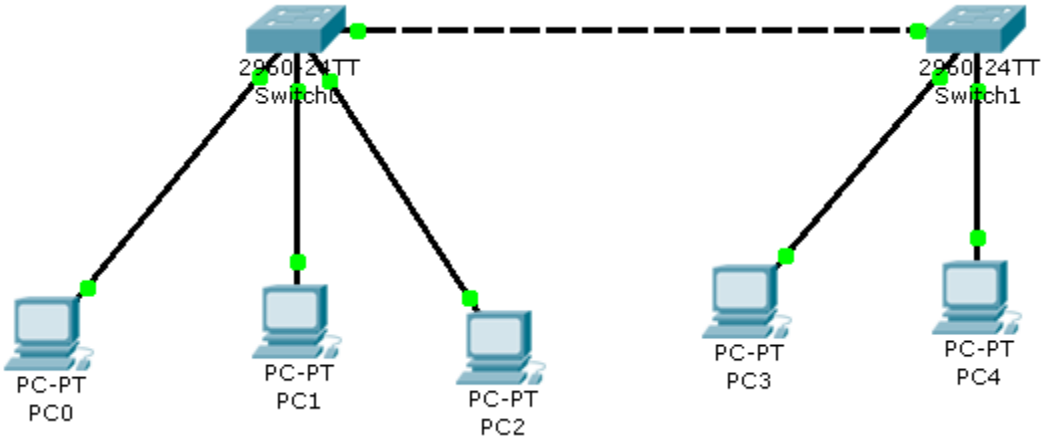


Рисунок 2.2 – Схема локальної мережі для завдання 2.

11. Всі дії проводяться аналогічно тільки замість концентраторів необхідно встановити комутатори. У вікні "Клас обладнання" вибрати піктограму ***Switches*** (Комутатори), з вікна "Модель обладнання" перетягнути два 2960-24TT (Комутатор) в робоче поле.

12. З'єднати складові мережі, як показано на рис. 4, та задати для кожного комп'ютера IP-адресу та маску підмережі згідно обраного з табл.. 2.1 варіанту.

13. В правому нижньому куту програми натиснути на піктограму ***Simulation Mode*** (Shift + S). З'явиться вікно, з допомогою якого відбувається симуляція мережі.

14. Натиснути ЛК миші на простий ping-запит (Закритий конверт), курсор змінить свою форму. Далі клацнути на ***PC0-PC4***. Потім знову натиснути на простий ping-запит потім ***PC3-PC1***.

15. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі.

16. Поспостерігати за пакетом та пояснити хід цієї передачі.

Таблиця 2.1 Варіанти до практичного завдання 2.

№ варіанту	IP-адреса комп'ютера	№ варіанту	IP-адреса комп'ютера	№ варіанту	IP-адреса комп'ютера
1	172.10.1.1 172.10.1.2 172.10.1.3 172.10.1.4 172.10.1.5	6	172.15.1.1 172.15.1.2 172.15.1.3 172.15.1.4 172.15.1.5	11	172.20.1.1 172.20.1.2 172.20.1.3 172.20.1.4 172.20.1.5
2	172.11.1.1 172.11.1.2 172.11.1.3 172.11.1.4 172.11.1.5	7	172.16.1.1 172.16.1.2 172.16.1.3 172.16.1.4 172.16.1.5	12	172.21.1.1 172.21.1.2 172.21.1.3 172.21.1.4 172.21.1.5
3	172.12.1.1 172.12.1.2 172.12.1.3 172.12.1.4 172.12.1.5	8	172.17.1.1 172.17.1.2 172.17.1.3 172.17.1.4 172.17.1.5	13	172.22.1.1 172.22.1.2 172.22.1.3 172.22.1.4 172.22.1.5
4	172.13.1.1 172.13.1.2 172.13.1.3 172.13.1.4 172.13.1.5	9	172.18.1.1 172.18.1.2 172.18.1.3 172.18.1.4 172.18.1.5	14	172.23.1.1 172.23.1.2 172.23.1.3 172.23.1.4 172.23.1.5
5	172.14.1.1 172.14.1.2 172.14.1.3 172.14.1.4 172.14.1.5	10	172.19.1.1 172.19.1.2 172.19.1.3 172.19.1.4 172.19.1.5	15	172.24.1.1 172.24.1.2 172.24.1.3 172.24.1.4 172.24.1.5

Питання для самоконтролю.

1. Що спричиняє колізію?

2. Дати характеристику методу доступу CSMA/CD.

3. Які пристрої використовувались при виконанні практичного завдання?

4. Чому при використанні комутатора не відбувається колізії?

3. Основи роботи з інтерфейсом обладнання Cisco

Маршрутизатор (роутер) та комутатор (світч) конфігуруються у командному рядку операційної системи Cisco IOS. Підключення здійснюється через Telnet на IP-адресу будь-якого з інтерфейсів або за допомогою будь-якої термінальної програми через послідовний порт комп'ютера, пов'язаний з консольним портом маршрутизатора (комутатора) [6].

При роботі в командному рядку Cisco IOS існує декілька контекстів (режимів вводу команд).

Контекст користувача відкривається при підключенні до маршрутизатора (комутатора). У цей же контекст командний рядок автоматично переходить при тривалій відсутності введення в контексті адміністратора. У контексті користувача доступні тільки прості команди (деякі базові операції для моніторингу), які не впливають на конфігурацію маршрутизатора (комутатора). Вид запрошення командного рядка:

Router> (для маршрутизатора)

або

Switch> (для комутатор)

Контекст адміністратора відкривається командою ***enable***, поданою в контексті користувача. У контексті адміністратора доступні команди, що дозволяють отримати повну інформацію про конфігурацію маршрутизатора (комутатора) та його стан, команди переходу в режим конфігурування, команди збереження та завантаження конфігурації. Вид запрошення командного рядка:

Router# (для маршрутизатора)

або

Switch# (для комутатора)

Зворотний перехід в контекст користувача проводиться по команді ***disable*** або після закінчення встановленого часу не активності. Завершення сеансу роботи – команда ***exit.***

Глобальний контекст конфігурування відкривається командою ***config terminal*** ("конфігурувати через термінал "), поданий в контексті адміністратора. Глобальний контекст конфігурування містить, як безпосередньо команди конфігурування маршрутизатора (комутатора), так і команди переходу в контексти конфігурування підсистем маршрутизатора (комутатора).

Вид запрошення командного рядка в контекстах конфігурування, які будуть зустрічатися найбільш частіше:

Router (config) #	глобальний
Router (config-if) #	інтерфейсу
Router (config-router) #	динамічної маршрутизації
Router (config-line) #	термінальної лінії

ВАЖЛИВО! Студент повинен запам’ятати вигляд запрошень командного рядка у всіх вищевказаних контекстах і правила переходу з контексту в контекст. Надалі приклади команд завжди будуть даватися разом із запрошеннями, з яких студент повинен визначати контекст, в якому подається команда. Приклади не будуть містити вказівок, як потрапити в необхідний контекст.

Вихід із глобального контексту конфігурації в контекст адміністратора, а також вихід з будь-якого підконтексту конфігурації в контекст верхнього рівня проводиться командою ***exit*** або ***Ctrl-Z***. Крім того, команда ***end***, подана в будь-якому із контекстів конфігурування негайно завершує процес конфігурації і повертає оператора в контекст адміністратора.

ВАЖЛИВО! Будь-яка команда конфігурації вступає в дію негайно після введення, а не після повернення в контекст адміністратора.

Спрощена схема контекстів представлена на рис. 3.1 [7].

Всі команди і параметри можуть бути скорочені (наприклад, "**enable**" – "**en**", "**configure terminal**" – "**conf t**"); якщо скорочення виявиться неоднозначним, маршрутизатор (комутатор) повідомить про це, а після натискання табуляції видасть варіанти, що відповідають введеному фрагменту.

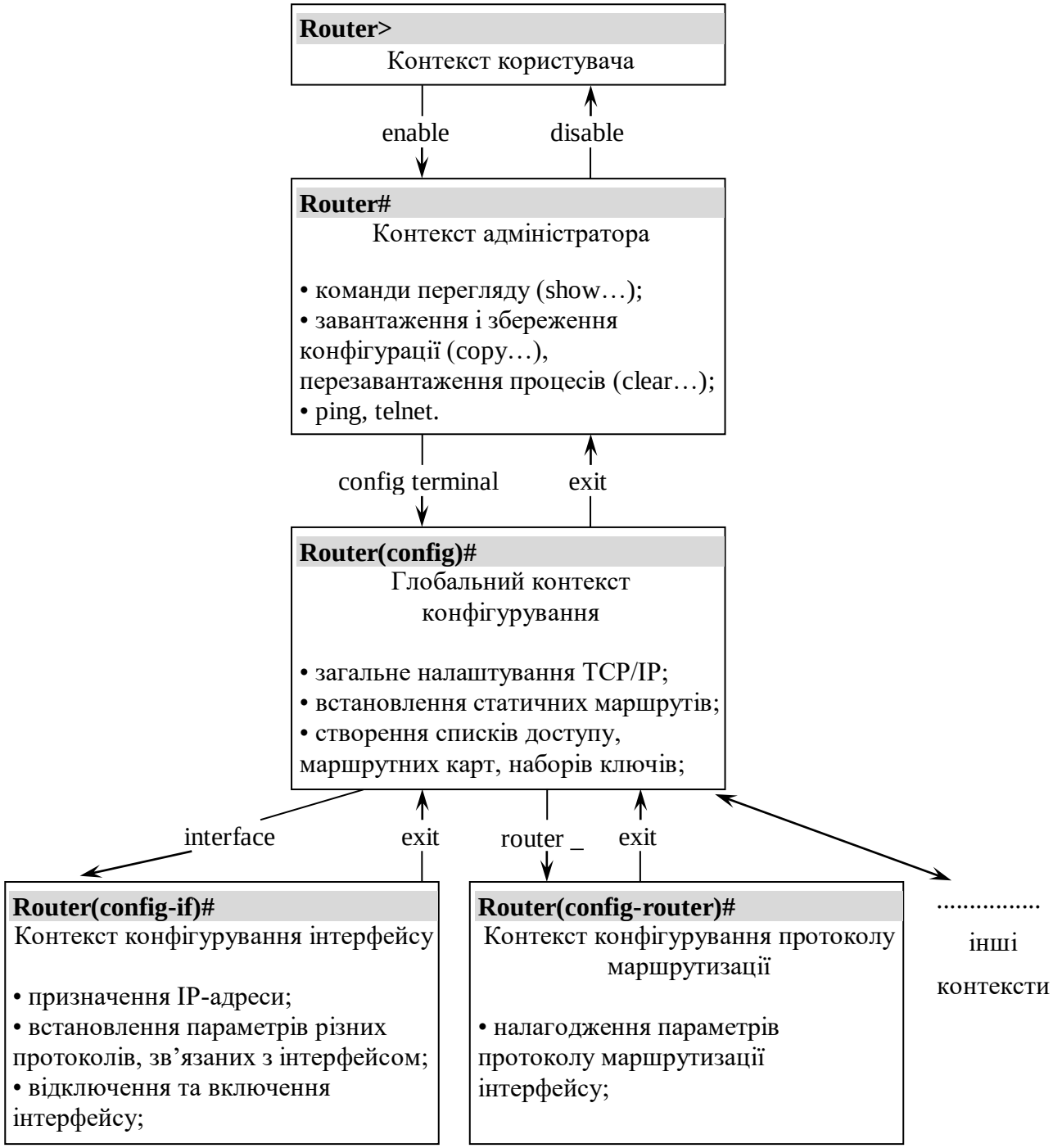


Рисунок 3.1 – Схема контекстів маршрутизатора Cisco IOS.

У будь-якому місці командного рядка для отримання допомоги може бути використаний знак питання:

Router #? список всіх команд даного контексту з коментарями;

Router # co? список всіх слів у цьому контексті введення, що починаються на "co" – немає пробілу перед "?";

Router # conf? список всіх параметрів, які можуть слідувати за командою config – перед "?" є пробіл.

Команда ***Hostname*** використовується для зміни імені використовуємого пристрою. Команда працює як для маршрутизатора, так і для комутатора.

Формат команди:

hostname *ім'я пристрою*

Приклад виконання команди:

Router(config)#hostname R1

R1(config)#

З прикладу видно, що маршрутизатор змінив своє ім'я з Router на R1.

Для встановлення паролю на привілейований режим (режим адміністратора) у маршрутизаторі, використовується команда ***Enable password***, а у комутаторі – команда ***Enable secret***.

Формат команди для маршрутизатора:

Enable password *пароль*

Формат команди для комутатора:

Enable secret *пароль*

Приклад виконання команди для маршрутизатора:

Router(config)#enable password 123

Приклад виконання команди для комутатора:

Router(config)#enable secret 123

Після того, як було встановлено пароль, при спробі входу в привілейований режим, маршрутизатор (комутатор) буде вимагати ввести цей пароль, в іншому випадку вхід буде неможливим.

Команда ***ip address*** використовується для надання інтерфейсу унікального імені, як для маршрутизатора, так і для комутатора.

Кожен інтерфейс повинен володіти своєю унікальною ip-адресою – інакше взаємодію пристроїв з даного інтерфейсу не зможе бути здійснено. Ця команда використовується для завдання ip-адреси обраному інтерфейсу.

Формат команди:

ip address *IP-адреса та маска під мережі*

Формат команди:

Switch(config)#interface vlan1

Switch(config-if)#ip address 172.16.10.5 255.255.0.0

Результат можна перевірити командою:

Switch#show interface vlan1

Практичне завдання 3.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис.2.

2. З розділу Switches (комутатори) добавити в робочу область три комутатора типу 2950–24. Далі з розділу End Devices (кінцеві пристрої) добавити чотири комп'ютера PC–PT.

3. З'єднати всі пристрої, як це показано на рис. 3.2, кабелями з розділу Connections: з прямим з'єднанням контактів (Copper Straight–Through) – комп'ютери з комутаторами, а з перехресним з'єднанням контактів (Copper Cross–Over) – комутатори між собою. У всіх пристроях використовувати гніздо FastEthernet.

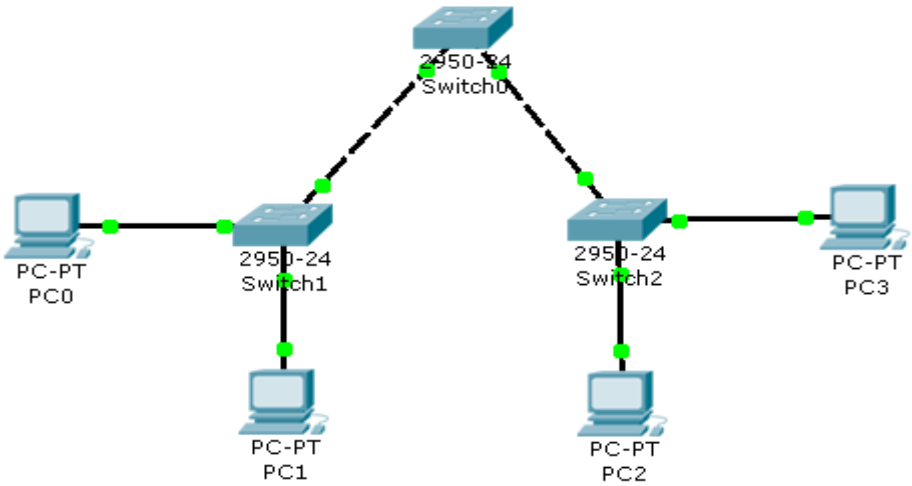


Рисунок 3.2 – Схема мережі складена з 4-х комп'ютерів та 3-х комутаторів.

4. Щоб розпочати конфігурацію комутатора необхідно клацнути ЛК миші по комутатору і перейти на вкладку ***CLI***.

5. Змінити імена комутаторам Cisco, використовуючи команду.

6. Забезпечити парольний доступ до привілейованого режиму на комутаторах.

7. Задати IP-адреси та маски комутаторам.

8. Задати IP-адреси та маски мереж персональним комп'ютерам.

9. Переконатися, що всі параметри були задані вірно.

10. Переключитися в режим симуляції та відправити пакети згідно варіанту.

Таблиця 3.1 Варіанти до практичного завдання 3.

№ варіанту	Ім'я комутатора	Пароль комутатора	IP-адреса та маска комутатора	IP-адреса комп'ютера	Переслати пакет з комп. на комп.
1	2	3	4	5	6
1	White1 White2 White3	111	172.10.1.11 255.255.0.0 172.10.1.12 255.255.0.0 172.10.1.13 255.255.0.0	172.10.1.1 172.10.1.2 172.10.1.3 172.10.1.4	з 172.10.1.1 на 172.10.1.3
2	Black1 Black2 Black3	222	172.11.1.11 255.255.0.0 172.11.1.12 255.255.0.0 172.11.1.13 255.255.0.0	172.11.1.1 172.11.1.2 172.11.1.3 172.11.1.4	з 172.11.1.1 на 172.11.1.4
3	Green1 Green2 Green3	333	172.12.1.11 255.255.0.0 172.12.1.12 255.255.0.0 172.12.1.13 255.255.0.0	172.12.1.1 172.12.1.2 172.12.1.3 172.12.1.4	з 172.12.1.2 на 172.12.1.3
4	Yellow1 Yellow2 Yellow3	444	172.13.1.11 255.255.0.0 172.13.1.12 255.255.0.0 172.13.1.13 255.255.0.0	172.13.1.1 172.13.1.2 172.13.1.3 172.13.1.4	з 172.13.1.2 на 172.13.1.4
5	Blue1 Blue2 Blue3	555	172.14.1.11 255.255.0.0 172.14.1.12 255.255.0.0 172.14.1.13 255.255.0.0	172.14.1.1 172.14.1.2 172.14.1.3 172.14.1.4	з 172.14.1.1 на 172.14.1.3

1	2	3	4	5	6
6	Gold1 Gold2 Gold3	666	172.15.1.11 255.255.0.0 172.15.1.12 255.255.0.0 172.15.1.13 255.255.0.0	172.15.1.1 з 172.15.1.2 172.15.1.3 на 172.15.1.4	172.15.1.1
7	Brown1 Brown2 Brown3	777	172.16.1.11 255.255.0.0 172.16.1.12 255.255.0.0 172.16.1.13 255.255.0.0	172.16.1.1 з 172.16.1.2 172.16.1.3 на 172.16.1.4	172.16.1.2 172.16.1.3
8	Cream1 Cream2 Cream3	888	172.17.1.11 255.255.0.0 172.17.1.12 255.255.0.0 172.17.1.13 255.255.0.0	172.17.1.1 з 172.17.1.2 172.17.1.3 на 172.17.1.4	172.17.1.2 172.17.1.4
9	Cyan1 Cyan2 Cyan3	999	172.18.1.11 255.255.0.0 172.18.1.12 255.255.0.0 172.18.1.13 255.255.0.0	172.18.1.1 з 172.18.1.2 172.18.1.3 на 172.18.1.4	172.18.1.1 172.18.1.3
10	Grey1 Grey2 Grey3	121	172.19.1.11 255.255.0.0 172.19.1.12 255.255.0.0 172.19.1.13 255.255.0.0	172.19.1.1 з 172.19.1.2 172.19.1.3 на 172.19.1.4	172.19.1.1 172.19.1.4
11	Magenta1 Magenta2 Magenta3	212	172.20.1.11 255.255.0.0 172.20.1.12 255.255.0.0 172.20.1.13 255.255.0.0	172.20.1.1 з 172.20.1.2 172.20.1.3 на 172.20.1.4	172.20.1.2 172.20.1.3
12	Orange1 Orange2 Orange3	131	172.21.1.11 255.255.0.0 172.21.1.12 255.255.0.0 172.21.1.13 255.255.0.0	172.21.1.1 з 172.21.1.2 172.21.1.3 на 172.21.1.3	172.21.1.2 172.21.1.4
13	Red1 Red2 Red3	313	172.22.1.11 255.255.0.0 172.22.1.12 255.255.0.0 172.22.1.13 255.255.0.0	172.22.1.1 з 172.22.1.2 172.22.1.3 на 172.22.1.4	172.22.1.1 172.22.1.3

1	2	3	4	5	6
14	Ping1 Ping2 Ping3	141	172.23.1.11 255.255.0.0 172.23.1.12 255.255.0.0 172.23.1.13 255.255.0.0	 172.23.1.1 172.23.1.2 172.23.1.3 172.23.1.4	 з 172.23.1.1 на 172.23.1.4
15	Silver1 Silver2 Silver3	414	172.24.1.11 255.255.0.0 172.24.1.12 255.255.0.0 172.24.1.13 255.255.0.0	 172.24.1.1 172.24.1.2 172.24.1.3 172.24.1.4	 з 172.24.1.2 на 172.24.1.3

Питання для самоконтролю.

1.Яку потрібно застосувати команду, щоб зайти в контекст адміністратора?

2.Як відрізнити контекст адміністратора від контексту користувача?

3.Яка команда дозволяє зайти в глобальний контекст конфігурування?

4.Що робить команда Hostname?

4. Планування структури локальної мережі та підключення пристроїв

Сервери – це високопродуктивні комп’ютери, які використовуються на підприємствах і в інших організаціях (рис. 4.1). Сервери обслуговують багатьох кінцевих користувачів або клієнтів.

Веб-сервер – це сервер, приймаючий HTTP-запити від клієнтів, зазвичай веб-браузерів, який видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. Веб-сервер – це основа Всесвітньої павутини [7, 8].

Апаратне забезпечення оптимізоване для швидкого відгуку на кілька мережевих запитів. У серверах встановлюється декілька центральних процесорів (ЦП), велика кількість оперативної пам’яті (ОЗП) і кілька жорстких дисків великої ємності, з яких можна дуже швидко отримувати інформацію.

Рисунок 4.1 – Вигляд сервера.

Часто сервер виконує дуже важливі функції і повинен бути постійно доступний користувачам. Тому їх компоненти і підсистеми часто дублюються, щоб уникнути збоїв. Крім того, зазвичай виконується автоматичне або ручне створення резервних копій даних. Зазвичай сервери встановлюють у безпечних місцях з контрольованим доступом.

Доступ до сервера, як правило, здійснюється дистанційно через мережу, тому клавіатуру і монітор до сервера підключають не завжди і лише з метою локального управління сервером. У деяких випадках використовується клавіатура і монітор іншого пристрою [8].

Зазвичай сервер діє, як сховище файлів, електронної пошти, веб-сторінок, завдань друку і т.д.

Бездротовий маршрутизатор LinkSys WRT300N – пристрій «три-в-одному»: маршрутизатор, точка доступу та 4-х портовий full-duplex 10/100 комутатор (рис. 4.2).

Рисунок 4.2 – Вигляд бездротового маршрутизатора
LinkSys WRT300N.

В точці доступу стандарту 802.11n (MIMO) використовуються чотири новітні технології, застосування яких забезпечує збільшення швидкості в 12 разів у порівнянні зі стандартом Wireless-G (802.11g). Технологія Wireless-N дозволяє одночасно працювати в Інтернеті, дивитися відео високої роздільної здатності, слухати потокову музику, організовувати спільний доступ до файлів, здійснювати телефонні дзвінки через Інтернет і брати участь в мережевих іграх [9].

Завдяки застосуванню нової технології передачі сигналу, зона охоплення в мережі Wireless-N в 4 рази перевищує зони охоплення мереж, побудованих за попередніми технологіями, що дозволило збільшити силу сигналу, практично усунути мертві зони і забезпечити безперервний зв’язок в будь-якій точці будинку або офісу, навіть якщо раніше вона була там недоступною. Найбільш зручна особливість устаткування Linksys для мереж Wireless-N полягає в тому, що воно володіє сумісністю з усім існуючим устаткуванням стандартів Wireless-B і Wireless-G.

Практичне завдання 4.

В завданні потрібно підключити до локальній мережі два комп'ютера та веб-сервер. Для перевірки мережі потрібно створити в Packet Tracer прототип.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис.3.

2. З розділу ***Wireless Devices*** (бездротові пристрої) добавити в робочу область маршрутизатор ***Linksys-WRT300N***. Далі з розділу ***End Devices*** (кінцеві пристрої) добавити два комп'ютера ***PC–PT*** та сервер ***Server–PT***.

3. З'єднати всі пристрої, як це показано на рис. 4.3, кабелем з прямим з'єднанням контактів (***Copper Straight–Through***) з розділу ***Connections***. У всіх пристроях використовувати гніздо ***FastEthernet***.

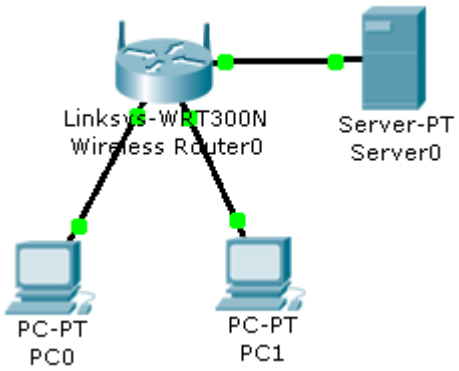


Рисунок 4. 3 – Схема мережі складена з двох комп'ютерів, сервера та бездротового маршрутизатора.

4. Вибрати кожен пристрій та присвоїти йому шлюз, IP-адресу та маску мережі згідно свого варіанту. Всі IP-адреси будуть знаходитись в одній і тій же мережі.

4.1 Клацнути ЛК миші по серверу, перейти на вкладку ***Config***, на лівій панелі натиснути кнопку ***Settings*** та в рядку ***Gateway*** ввести шлюз. Потім в лівій панелі натиснути кнопку ***FastEthernet*** і в рядку ***IP Address*** ввести IP-адресу сервера, а в рядку ***Subnet Mask*** ввести маску (формується автоматично, потрібно лише поставити в рядок курсор). (Дані шлюзу, IP-адреси та маски можна ввести і тим способом, який використовувався в практичному завданні 1).

4.2 Аналогічно ввести дані для комп'ютерів.

5. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP-адреса комп'ютера PC1]

PC>ping [IP-адреса сервера Server0]

6. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

7. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити маршрут від комп'ютера ***PC0*** і до сервера ***Server0***.

8. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі та дозволить прослідкувати за ходом запиту.

9. Зберегти файл та продемонструвати викладачеві.

Таблиця 4.1 Варіанти до практичного завдання 4.

№ варіанту	Шлюз	IP-адреса комп'ютера PT0	IP-адреса комп'ютера PT1	IP-адреса серверу Server0
1	192.168.1.1	192.168.1.10	192.168.1.11	192.168.1.12
2	192.168.1.2	192.168.1.20	192.168.1.21	192.168.1.22
3	192.168.1.3	192.168.1.30	192.168.1.31	192.168.1.32
4	192.168.1.4	192.168.1.40	192.168.1.41	192.168.1.42
5	192.168.1.5	192.168.1.50	192.168.1.51	192.168.1.52
6	192.168.1.6	192.168.1.60	192.168.1.61	192.168.1.62
7	192.168.1.7	192.168.1.70	192.168.1.71	192.168.1.72
8	192.168.1.8	192.168.1.80	192.168.1.81	192.168.1.82
9	192.168.1.9	192.168.1.90	192.168.1.91	192.168.1.92
10	192.168.1.10	192.168.1.100	192.168.1.101	192.168.1.102
11	192.168.1.11	192.168.1.110	192.168.1.111	192.168.1.112
12	192.168.1.12	192.168.1.120	192.168.1.121	192.168.1.122
13	192.168.1.13	192.168.1.130	192.168.1.131	192.168.1.132
14	192.168.1.14	192.168.1.140	192.168.1.141	192.168.1.142
15	192.168.1.15	192.168.1.150	192.168.1.151	192.168.1.152

Примітка. Шлюз використовується один і той самий, що для сервера, що для комп'ютерів. При завданні маски (чи то комп'ютера, чи то сервера) в рядку маска сама формується автоматично, але перед цим потрібно задати IP-адресу.

Питання для самоконтролю

1. Для яких цілей потрібен сервер?
2. В яких цілях використовується пристрій LinkSys WRT300N?
3. Які пристрої використовувались в мережі?

5. Конфігурування DHCP на мультифункціональному пристрої

Список користувачів локальної мережі часто змінюється. З'являються нові користувачі з ноутбуками, які потрібно підключити. Інші встановлюють нові робочі станції. Щоб кожної станції не доводилося вручну присвоювати IP-адреси, найпростіше це зробити автоматично. Для цього використовується протокол під назвою *Dynamic Host Configuration Protocol* (DHCP) [9, 10].

DHCP передбачає механізм автоматичного присвоєння інформації про адресу, наприклад, IP-адреси, маски підмережі, шлюзу за замовчуванням та інших параметрів.

Це найбільш бажаний спосіб привласнення IP-адрес вузлів у великій мережі, оскільки він полегшує роботу фахівців служби підтримки і практично усуває можливість помилки.

Інші переваги DHCP полягають в тому, що адреси присвоюються вузлам сайту тимчасово. Якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання. Це особливо корисно для мобільних користувачів, які то підключаються, то відключаються.

Коли відбувається підключення до бездротової мережі в аеропорту або магазині, доступ в Інтернет забезпечує DHCP (рис. 5.1). При вході в зону зв'язку встановлений на ноутбуці клієнт DHCP зв'язується з локальним сервером DHCP через бездротове з'єднання. Сервер DHCP присвоює ноутбука IP-адресу.

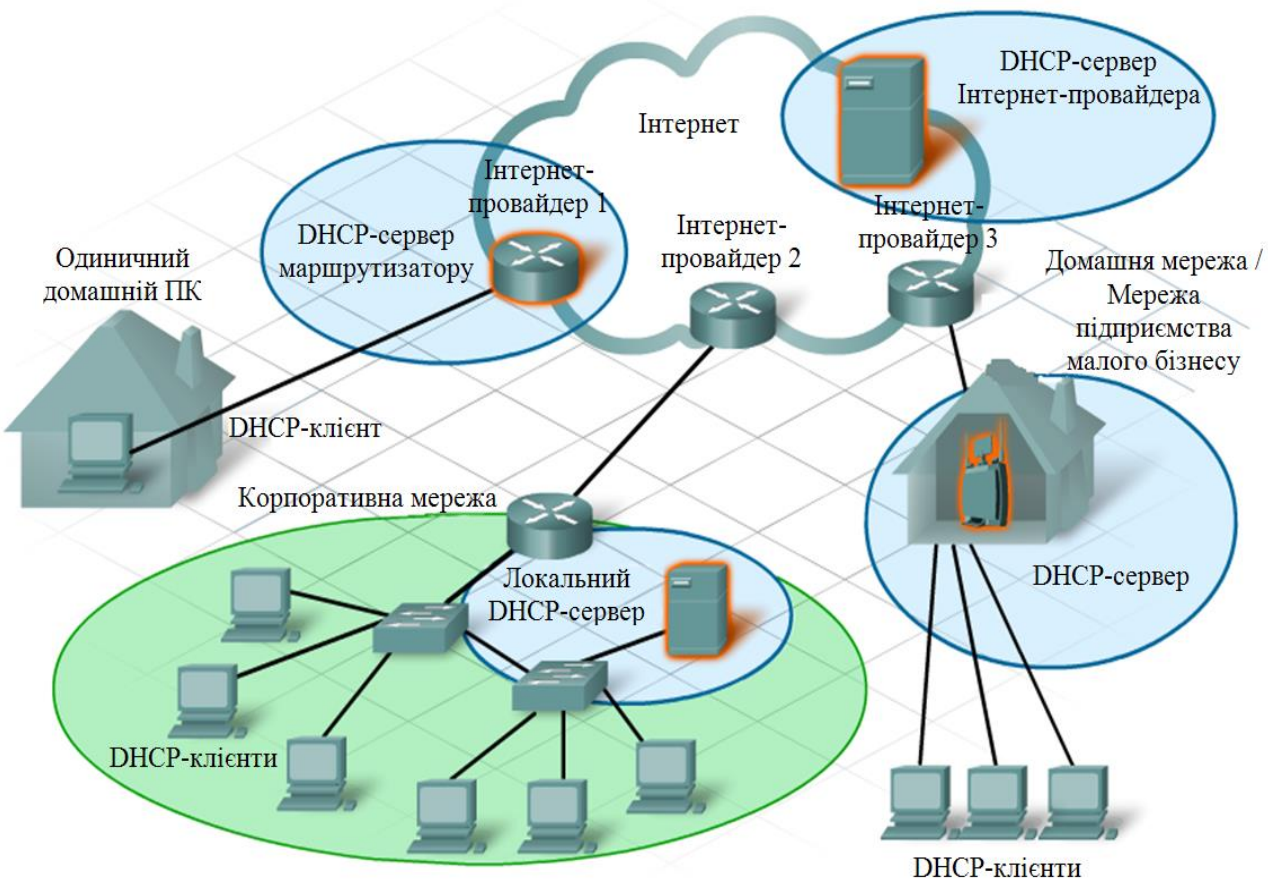


Рисунок 5.1 – Схема забезпечення доступу через DHCP протокол.

В якості серверів DHCP можуть виступати найрізноманітніші пристрої за умови, що на них встановлено службове програмне забезпечення DHCP. У більшості середніх і великих мереж сервер DHCP – це локальний виділений сервер на базі ПК.

У домашніх мережах він зазвичай знаходиться в Інтернет-провайдера. Вузол з домашньої мережі отримує налаштування IP безпосередньо від Інтернет-провайдера [10].

У багатьох домашніх і невеликих корпоративних мережах для підключення до модему Інтернет-провайдера використовується вбудований маршрутизатор. У даному випадку він виступає в якості клієнта і сервера DHCP. Як клієнт він отримує налаштування IP від Інтернет-провайдера, а потім, вже як сервер DHCP, передає їх внутрішніх вузлів локальної мережі.

Крім серверів на базі ПК і вбудованих маршрутизаторів, послуги DHCP можуть надаватись клієнтам і іншим мережевим пристроям, наприклад, виділені маршрутизатори.

При першому налагодженні в якості клієнта DHCP у вузлі немає IP-адреси, маски підмережі та шлюзу за замовчуванням. Він отримує ці дані від сервера DHCP, локального або який належить Інтернет-провайдеру. На сервері DHCP налаштовується діапазон, або пул, IP-адрес, які можна привласнити клієнтам DHCP.

Практичне завдання 5.

В завданні потрібно підключити три ПК до Linksys–WRT300N. Всі три комп'ютери повинні автоматично отримати IP-адресу від пристрою Linksys.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 5.2.

1.1 З розділу ***Wireless Devices*** (бездротові пристрої) добавити в робочу область маршрутизатор ***Linksys-WRT300N***. Далі з розділу ***End Devices*** (кінцеві пристрої) добавити три комп'ютера ***PC–PT***.

1.2 З'єднати комп'ютери з Linksys-WRT300N, як це показано на схемі, кабелем з прямим з'єднанням контактів (***Copper Straight–Through***) з розділу ***Connections***. У всіх пристроях використовувати гніздо ***FastEthernet***.

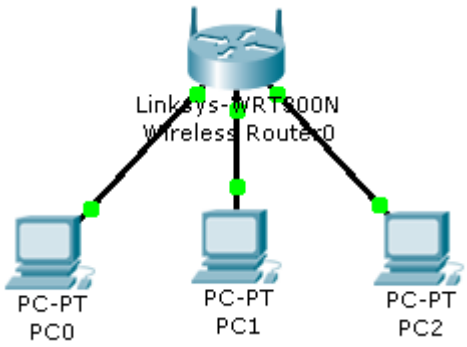


Рисунок 5.2 – Схема мережі складена з трьох комп'ютерів та бездротового маршрутизатора.

2. Шляхом натиснення ЛК миші на Linksys-WRT300N, викликати вікно конфігурацій пристрою.

3. Перейти на вкладку конфігурацій (***Config***) та в рядку ***Display Name*** ввести нове ім’я маршрутизатора згідно свого варіанту.

4. Перейти на вкладку графічного користувальницького інтерфейсу (***GUI***), а в нижніх вкладках – на вкладку ***Setup*** (повинна бути за замовчуванням).

5. В рядку ***IP Address*** змінити IP-адресу пристрою Linksys-WRT300N на ту що відповідає варіанту, та зберегти налаштунки шляхом натиснення на кнопку ***Save Settings*** внизу сторінки.

6. Якщо всі дії було виконано вірно, то в рядку ***Start IP Address*** будуть наступні дані: [перші три числа IP-адреси варіанта] та число 100.

7. Змінити число 100 на відповідне число варіанта, це буде кінцівка IP-адреси, що присвоюється першому ПК.

8. В рядку ***Maximum number of Users*** ввести максимальну кількість ПК, згідно варіанту, що можуть підключатись до Linksys-WRT300N та знову зберегти всі параметри натисненням кнопки ***Save Settings***.

9. Закрити вікно конфігурацій Linksys-WRT300N.

10. Відкрити вікно конфігурацій першого комп’ютера та перейти на вкладку ***Config***. В лівій панелі вкладки натиснути на кнопку ***FastEthernet*** та поставити крапку навпроти рядка ***DHCP***. Зверніть увагу, що IP-адреса та маска підмережі з’явились автоматично.

11. Виконати аналогічні дії для інших двох комп’ютерів, що вказані в пункту 10.

12. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп’ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP-адреса комп’ютера PC1]

PC>ping [IP-адреса комп’ютера PC2]

13. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

14. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити маршрут від комп'ютера ***PC0*** і до комп'ютера ***PC2***.

15. В панелі симуляції натиснути на кнопку ***Auto Capture / Play***, та спостерігати за діями у вікні симуляції і командному рядку першого комп'ютера. (**Примітка**. Щоб прискорити швидкість переміщення пакету, можна скористатися повзунком швидкості на панелі симуляції).

16. Зберегти файл та продемонструвати викладачеві.

Таблиця 5.1 Варіанти до практичного завдання 5.

№ варіанту	Ім'я Linksys–WRT300N	IP-адреса Linksys–WRT300N	Кінцівка IP-адреси, що буде автоматично присвоюватись першому ПК	Число, що відповідає максимальній кількості ПК
1	White	192.168.1.15	5	10
2	Black	192.168.2.14	7	12
3	Green	192.168.3.13	9	15
4	Yellow	192.168.4.12	10	17
5	Blue	192.168.5.11	12	19
6	Gold	192.168.6.10	15	20
7	Brown	192.168.7.9	17	22
8	Cream	192.168.8.8	19	23
9	Cyan	192.168.9.7	20	25
10	Grey	192.168.10.6	22	27
11	Magenta	192.168.11.5	25	29
12	Orange	192.168.12.4	27	30
13	Red	192.168.13.3	29	32
14	Ping	192.168.14.2	30	35
15	Silver	192.168.15.1	32	37

Питання для самоконтролю

1. Для чого використовується протокол DHCP?
2. Які функції виконує пристрій Linksys–WRT300N?
3. Які дані автоматично отримував кожен комп'ютер мережі?

6. Міжмережні пристрої

Маршрутизатор з інтегрованими службами – призначений для використання у середніх і великих організаціях, головних офісах великих підприємств і на кордоні агрегування трафіку перед WAN (WAN – глобальна мережа – мережа обміну даними, що обслуговує користувачів на великій території). Також може використовуватися, як велика платформа інтернет-доступу.

Маршрутизатор забезпечує високу продуктивність і відповідає вимогам великомасштабних мереж. ***Cisco 1841*** – це маршрутизатори орієнтовані насамперед на компанії з великими та середніми офісами (рис. 6.1). Гнучкість у налаштуванні зробили дані моделі популярним рішенням для реалізації підключення до корпоративних мереж і Інтернету. Cisco 1841 збільшили продуктивність більш ніж у п’ять разів, зберігши при цьому мультисервісну архітектуру. Подібний прогрес став можливим багато в чому завдяки розміщенню роз’ємів для карт HWIC, які у свою чергу, дають можливість встановлювати більш сучасні моделі HWIC карт (наприклад, чотирьохпортовий EtherSwitch HWIC).

Cisco 1841 сумісний з модулями AIM, HWIC і VWIC, а також з модулями WAN-інтерфейсів для маршрутизаторів Cisco 1700 (підтримується більш ніж тридцять карт, однак WIC / VIC / VWIC будуть працювати тільки в режимі передачі даних). Він має вбудовані засоби апаратного прискорення шифрування трафіку, можливість подальшого збільшення продуктивності шифрування – шляхом встановлення опционального модуля VPN; функціональність системи запобігання вторгнень та міжмережевого екрану [11].

Рисунок 6.1 – Вигляд маршрутизатора серії Cisco 1841.

Cisco EtherSwitch HWIC-4ESW – це інтерфейсна плата (рис. 6.2), що представляють собою комутатор Ethernet 10/100BaseT рівня 2 з підтримкою маршрутизації рівня 3. (Маршрутизація рівня 3 переадресовується на мережевий вузол і безпосередньо на комутаторі не виконується.) Трафік між різними мережами VLAN на комутаторі здійснюється на платформі маршрутизатора.

Рисунок 6.2 – Вигляд інтерфейсної плати Cisco EtherSwitch HWIC-4ESW.

Будь-який порт інтерфейсної плати Cisco EtherSwitch HWIC можна налаштувати для використання в якості об’єднавчого порту зв’язку з іншою інтерфейсною платою Cisco EtherSwitch HWIC або мережевим модулем EtherSwitch в цій же системі.

Cisco WIC-1T – це інтерфейсна плата маршрутизатора (рис. 6.3), що забезпечує один порт послідовного з’єднання для віддалених офісів або застарілих послідовних пристроїв мережі, такі як синхронний Data Link Control (SDLC) концентратор, системи сигналізації, а також пакетів по SONET (POS) пристроїв.

Рисунок 6.3 – Вигляд інтерфейсної плати Cisco WIC-1T.

Точка доступу або ***точка бездротового доступу*** – центральний пристрій бездротової мережі (рис. 6.4), що використовується для організації з'єднання між бездротовими клієнтами, а також для з'єднання дротового і бездротового сегментів, виконуючи функції моста між ними. Точка доступу під'єднується до концентратора, комутатора або проводового маршрутизатора та надсилає безпроводові сигнали. Це дає можливість комп'ютерам і пристроям підключатися до проводової мережі з використанням безпроводового зв'язку. Дія точки доступу подібна до роботи вишки мобільного зв'язку: можна переміщатися з одного розташування до іншого без втрати безпроводового доступу до мережі. Якщо підключитися до Інтернету за допомогою публічної безпроводової мережі в аеропорту, кафе або готелі, підключення зазвичай відбувається через точку доступу [11, 12].

Рисунок 6.4 – Вигляд точки доступу Access Point PT

Практичне завдання 6.

В завданні потрібно створити локальну мережу, в яку будуть входити: маршрутизатор з інтегрованими службами 1841, маршрутизатор Router-PT, точка доступу AccessPoint PT та два комп'ютера PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 6.5.

1.1 З розділу ***Wireless Devices*** (бездротові пристрої) добавити в робочу область точку доступу ***AccessPoint PT***. Далі з розділу ***End Devices*** (кінцеві

пристрої) добавити два комп'ютера ***PC–PT*** і з розділу ***Router*** (маршрутизатори) добавити маршрутизатор ***1841*** та маршрутизатор ***Router-PT***.

1.2 З'єднати точку доступу ***AccessPoint PT*** з маршрутизатором ***1841***, як це показано на схемі, кабелем з перехресним з'єднанням контактів (***Copper Cross–Over***) з розділу ***Connections***. В точці доступу використовувати гніздо ***Port 0***, а в маршрутизаторі ***FastEthernet0/0*** (не перейматись, що індикатори зв'язку будуть червоними, це через те що інтерфейс FastEthernet0/0 вимкнутий).

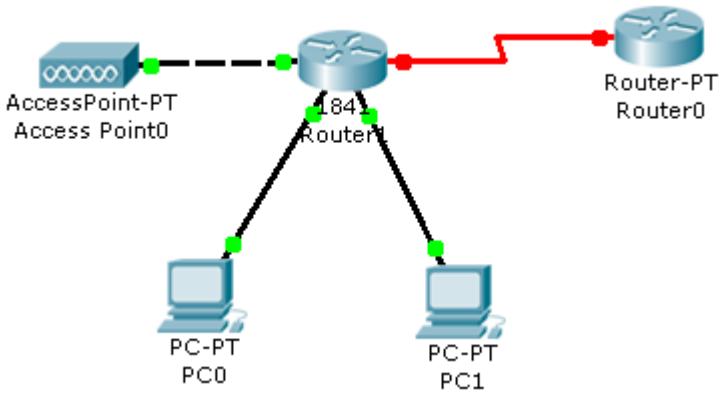


Рисунок 6.5 – Схема локальної мережі складена з двох комп'ютерів, двох маршрутизаторів та точки доступу.

2. Шляхом натиснення ЛК миші на маршрутизаторі 1841, викликати вікно конфігурації пристрою.

3. На вкладці "Вид фізичного пристрою" (Physical) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

4. В лівій частині вікна натиснути на кнопку ***HWIC-4ESW***, після чого в низу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний лівий роз'єм маршрутизатора (тягнути курсором потрібно зображення плати).

5. Знову натиснути на кнопку ***WIC-1T*** в лівій частині вікна та перетягнути плату у вільний роз'єм маршрутизатора.

6. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

7. Після того, як було подано живлення потрібно зачекати секунд 20 (вступають в дію налаштунки) та перейти на вкладку "Конфігурація" (***Config***), щоб увімкнути всі інтерфейси маршрутизатора. Для цього потрібно натиснути на кожен інтерфейс в лівій частині вікна (інтерфейсів всього 7, а саме: FastEthernet0/0, FastEthernet0/1, Serial0/0/0, FastEthernet0/1/0, FastEthernet0/1/1, FastEthernet0/1/2, FastEthernet0/1/3) та поставити відмітку ***ON*** навпроти рядка ***Port Status***. По закінченню вмикання інтерфейсів – закрити вікно конфігурацій маршрутизатора.

8. В робочій області повинен налагодитись зв'язок між маршрутизатором 1841 та точкою доступу AccessPoint PT (індикатори зв'язку світяться зеленим кольором).

9. З'єднати два маршрутизатора між собою кабелем ***Serial-DTE*** з розділу ***Connections***. В маршрутизаторі 1841 використовувати гніздо ***Serial0/0/0***, а в маршрутизаторі Router-PT – ***Serial2/0***.

10. Надати комп'ютерам IP-адреси та маски підмережі, що задані в таблиці варіантів.

11. З'єднати комп'ютери з маршрутизатором 1841, як це показано на рисунку 5, кабелем з прямим з'єднанням контактів (***Copper Straight–Through***) з розділу ***Connections***. Для першого з'єднання в маршрутизаторі 1841 використовувати гніздо ***FastEthernet0/1/0***, а в комп'ютері PT0 – ***FastEthernet***; для другого з'єднання – в маршрутизаторі 1841 використовувати гніздо ***FastEthernet0/1/1***, а в комп'ютері PT1 – ***FastEthernet.***

12. Щоб переконатись, що мережа працює, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP-адреса комп'ютера PC1]

13. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

14. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити маршрут від комп'ютера ***PC0*** до комп'ютера ***PC1***.

15. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі та дозволить прослідкувати за ходом запиту.

16. Зберегти файл та продемонструвати викладачеві.

Таблиця 6.1 Варіанти до практичного завдання 6.

№ варіанту	IP-адреса комп'ютера PT0	IP-адреса комп'ютера PT1
1	192.168.1.10	192.168.1.11
2	192.168.1.20	192.168.1.21
3	192.168.1.30	192.168.1.31
4	192.168.1.40	192.168.1.41
5	192.168.1.50	192.168.1.51
6	192.168.1.60	192.168.1.61
7	192.168.1.70	192.168.1.71
8	192.168.1.80	192.168.1.81
9	192.168.1.90	192.168.1.91
10	192.168.1.100	192.168.1.101
11	192.168.1.110	192.168.1.111
12	192.168.1.120	192.168.1.121
13	192.168.1.130	192.168.1.131
14	192.168.1.140	192.168.1.141
15	192.168.1.150	192.168.1.151

Питання для самоконтролю.

1. Для чого використовуються маршрутизатори з інтегрованими службами?

2. На які масштаби мереж розрахований маршрутизатор Cisco 1841?

3. Дати характеристику платам маршрутизації, що використовувались при виконанні даного завдання.

4. Які кабелі застосовувались при виконанні завдання?

7. Значення та принцип використання шлюзу

Шлюз – пристрій (апаратний чи програмний), використовується для передачі інформації між підмережами, які використовують різні протоколи(пр. локальна та глобальна мережа).

Як шлюз може використовуватись маршрутизатор або комп'ютер з двома мережевими картами, кожна з яких під'єднань до підмережі. В кожному комп'ютері необхідно вказати адресу шлюзу, і коли потрібно буде передати інформацію в іншу підмережу, то він передає дані на шлюз, а той в свою чергу на відповідний комп'ютер [13].

Головна задача мережевого шлюзу – конвертувати протоколи між мережами.

В основному шлюз працює повільніше ніж мости, комутатори і звичайні маршрутизатори. Говорячи простою мовою, мережевий шлюз – це точка, яка служить виходом в іншу мережу.

Практичне завдання 7.

В завданні необхідно створити дві під мережі які будуть об'єднані з допомогою мережевого шлюзу. Для цього використовується: вісім комп'ютерів PC–PT(по чотири на кожну підмережу), два комутатори 2950-24 (об'єднують кожну підмережу), та маршрутизатор з інтегрованими службами 1841(виконує роль шлюзу).

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 7.1.

1.1 З розділу ***Switches*** (комутатори) добавити в робочу область два комутатори серії ***2950-24***. Далі з розділу ***End Devices*** (кінцеві пристрої) добавити вісім комп'ютерів ***PC–PT***, з розділу ***Router*** (маршрутизатори) добавити маршрутизатор серії ***1841***.

1.2 З’єднати пристрої, як це показано на схемі, кабелем з прямим з’єднанням контактів (***Copper Straight–Through***) з розділу ***Connections***.

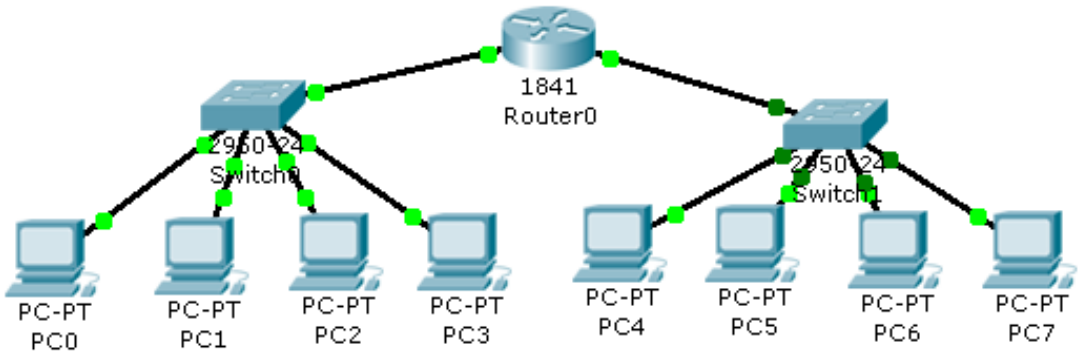


Рисунок 7.1 – Схема двох локальних мереж об’єднаних за допомогою шлюзу.

2. Натиснути ЛК миші на маршрутизатор та перейти до вкладки ***Config***, перейти в розділу ***INTERFACE***.

2.1 Натиснути на клавішу ***FastEhernet 0/0***. В рядку ***Port Status*** поставити відмітку ***ON*** та вказати IP-адресу та маску підмережі згідно варіанту.

2.2 Натиснути на клавішу ***FastEhernet 0/1***. В рядку ***Port Status*** поставити відмітку ***ON*** та вказати IP-адресу та маску підмережі згідно варіанту.

3. Натиснути ЛК миші на комп’ютер та перейти до вкладки ***Desktop***, натиснути на піктограму ***IP Configuration***. Задати IP-адресу, маску підмережі та шлюз згідно варіанту (цей пункт повторити з кожним комп’ютером).

4. Щоб переконатись, що мережа працює, потрібно зробити тестування. Клацнути ЛК миші по комп’ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP-адреса комп’ютера PC1]

PC>ping [IP-адреса комп’ютера PC6]

5. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

6. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити маршрут від комп'ютера ***PC0*** до комп'ютера ***PC6***.

7. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі та дозволить прослідкувати за ходом запиту.

8. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC7*]

9. Протестувати мережу в режимі моделювання ***Simulation Mode*** та подивитися, як відбувається обмін пакетами за допомогою ***ping-запиту***.

10. Зберегти файл та продемонструвати викладачеві.

Таблиця 7.1 Варіанти до практичного завдання 7.

№ варіанту	IP-адреса, маска та шлюз PC-PT0	IP-адреса, маска та шлюз PC-PT1	IP-адреса, маска та шлюз PC-PT2	IP-адреса, маска та шлюз PC-PT3	IP-адреса, маска та шлюз PC-PT4	IP-адреса, маска та шлюз PC-PT5
1	2	3	4	5	6	7
1	192.168.1.2 255.255.255.0 192.168.1.1	192.168.1.3 255.255.255.0 192.168.1.1	192.168.1.4 255.255.255.0 192.168.1.1	192.168.1.5 255.255.255.0 192.168.1.1	192.168.2.2 255.255.255.0 192.168.1.1	192.168.2.3 255.255.255.0 192.168.1.1
2	192.168.3.2 255.255.255.0 192.168.3.1	192.168.3.3 255.255.255.0 192.168.3.1	192.168.3.4 255.255.255.0 192.168.3.1	192.168.3.5 255.255.255.0 192.168.3.1	192.168.4.2 255.255.255.0 192.168.4.1	192.168.4.3 255.255.255.0 192.168.4.1
3	192.168.5.2 255.255.255.0 192.168.5.1	192.168.5.3 255.255.255.0 192.168.5.1	192.168.5.4 255.255.255.0 192.168.5.1	192.168.5.5 255.255.255.0 192.168.5.1	192.168.6.2 255.255.255.0 192.168.6.1	192.168.6.3 255.255.255.0 192.168.6.1
4	192.168.7.2 255.255.255.0 192.168.7.1	192.168.7.3 255.255.255.0 192.168.7.1	192.168.7.4 255.255.255.0 192.168.7.1	192.168.7.5 255.255.255.0 192.168.7.1	192.168.8.2 255.255.255.0 192.168.8.1	192.168.8.3 255.255.255.0 192.168.8.1
5	192.168.9.2 255.255.255.0 192.168.9.1	192.168.9.3 255.255.255.0 192.168.9.1	192.168.9.4 255.255.255.0 192.168.9.1	192.168.9.5 255.255.255.0 192.168.9.1	192.168.10.2 255.255.255.0 192.168.10.1	192.168.10.3 255.255.255.0 192.168.10.1
6	192.168.11.2 255.255.255.0 192.168.11.1	192.168.11.3 255.255.255.0 192.168.11.1	192.168.11.4 255.255.255.0 192.168.11.1	192.168.11.5 255.255.255.0 192.168.11.1	192.168.12.2 255.255.255.0 192.168.12.1	192.168.12.3 255.255.255.0 192.168.12.1
7	192.168.13.2 255.255.255.0 192.168.13.1	192.168.13.3 255.255.255.0 192.168.13.1	192.168.13.4 255.255.255.0 192.168.13.1	192.168.13.5 255.255.255.0 192.168.13.1	192.168.14.2 255.255.255.0 192.168.14.1	192.168.14.3 255.255.255.0 192.168.14.1

1	2	3	4	5	6	7
8	192.168.15.2 255.255.255.0 192.168.15.1	192.168.15.3 255.255.255.0 192.168.15.1	192.168.15.4 255.255.255.0 192.168.15.1	192.168.15.5 255.255.255.0 192.168.15.1	192.168.16.2 255.255.255.0 192.168.16.1	192.168.16.3 255.255.255.0 192.168.16.1
9	192.168.17.2 255.255.255.0 192.168.17.1	192.168.17.3 255.255.255.0 192.168.17.1	192.168.17.4 255.255.255.0 192.168.17.1	192.168.17.5 255.255.255.0 192.168.17.1	192.168.18.2 255.255.255.0 192.168.18.1	192.168.18.3 255.255.255.0 192.168.18.1
10	192.168.19.2 255.255.255.0 192.168.19.1	192.168.19.3 255.255.255.0 192.168.19.1	192.168.19.4 255.255.255.0 192.168.19.1	192.168.19.5 255.255.255.0 192.168.19.1	192.168.20.2 255.255.255.0 192.168.20.1	192.168.20.3 255.255.255.0 192.168.20.1
11	192.168.21.2 255.255.255.0 192.168.21.1	192.168.21.3 255.255.255.0 192.168.21.1	192.168.21.4 255.255.255.0 192.168.21.1	192.168.21.5 255.255.255.0 192.168.21.1	192.168.22.2 255.255.255.0 192.168.22.1	192.168.22.3 255.255.255.0 192.168.22.1
12	192.168.23.2 255.255.255.0 192.168.23.1	192.168.23.3 255.255.255.0 192.168.23.1	192.168.23.4 255.255.255.0 192.168.23.1	192.168.23.5 255.255.255.0 192.168.23.1	192.168.24.2 255.255.255.0 192.168.24.1	192.168.24.3 255.255.255.0 192.168.24.1
13	192.168.25.2 255.255.255.0 192.168.25.1	192.168.25.3 255.255.255.0 192.168.25.1	192.168.25.4 255.255.255.0 192.168.25.1	192.168.25.5 255.255.255.0 192.168.25.1	192.168.26.2 255.255.255.0 192.168.26.1	192.168.26.3 255.255.255.0 192.168.26.1
14	192.168.27.2 255.255.255.0 192.168.27.1	192.168.27.3 255.255.255.0 192.168.27.1	192.168.27.4 255.255.255.0 192.168.27.1	192.168.27.5 255.255.255.0 192.168.27.1	192.168.28.2 255.255.255.0 192.168.28.1	192.168.28.3 255.255.255.0 192.168.28.1
15	192.168.29.2 255.255.255.0 192.168.20.1	192.168.29.3 255.255.255.0 192.168.29.1	192.168.29.4 255.255.255.0 192.168.29.1	192.168.29.5 255.255.255.0 192.168.29.1	192.168.30.2 255.255.255.0 192.168.30.1	192.168.30.3 255.255.255.0 192.168.30.1

Продовження таблиці 7.1 Варіанти до практичного завдання 7.

№ варіанту	IP-адреса, маска та шлюз PC-PT6	IP-адреса, маска та шлюз PC-PT7	IP-адреса та маска FastEthernet 0/0 Використовувати також як шлюз для комп'ютерів PT0 – PT3	IP-адреса та маска FastEthernet 0/1 Використовувати також як шлюз для комп'ютерів PT4 – PT7
1	2	3	4	5
1	192.168.2.4 255.255.255.0 192.168.1.1	192.168.2.5 255.255.255.0 192.168.1.1	192.168.1.1 255.255.255.0	192.168.2.1 255.255.255.0
2	192.168.4.4 255.255.255.0 192.168.4.1	192.168.4.5 255.255.255.0 192.168.4.1	192.168.3.1 255.255.255.0	192.168.4.1 255.255.255.0
3	192.168.6.4 255.255.255.0 192.168.6.1	192.168.6.5 255.255.255.0 192.168.6.1	192.168.5.1 255.255.255.0	192.168.6.1 255.255.255.0
4	192.168.8.4 255.255.255.0 192.168.8.1	192.168.8.5 255.255.255.0 192.168.8.1	192.168.7.1 255.255.255.0	192.168.8.1 255.255.255.0

1	2	3	4	5
7	192.168.14.4 255.255.255.0 192.168.14.1	192.168.14.5 255.255.255.0 192.168.14.1	192.168.13.1 255.255.255.0	192.168.14.1 255.255.255.0
5	192.168.10.4 255.255.255.0 192.168.10.1	192.168.10.5 255.255.255.0 192.168.10.1	192.168.9.1 255.255.255.0	192.168.10.1 255.255.255.0
6	192.168.12.4 255.255.255.0 192.168.12.1	192.168.12.5 255.255.255.0 192.168.12.1	192.168.11.1 255.255.255.0	192.168.12.1 255.255.255.0
8	192.168.16.4 255.255.255.0 192.168.16.1	192.168.16.5 255.255.255.0 192.168.16.1	192.168.15.1 255.255.255.0	192.168.16.1 255.255.255.0
9	192.168.18.4 255.255.255.0 192.168.18.1	192.168.18.5 255.255.255.0 192.168.18.1	192.168.17.1 255.255.255.0	192.168.18.1 255.255.255.0
10	192.168.20.4 255.255.255.0 192.168.20.1	192.168.20.5 255.255.255.0 192.168.20.1	192.168.19.1 255.255.255.0	192.168.20.1 255.255.255.0
11	192.168.22.4 255.255.255.0 192.168.22.1	192.168.22.5 255.255.255.0 192.168.22.1	192.168.21.1 255.255.255.0	192.168.22.1 255.255.255.0
12	192.168.24.4 255.255.255.0 192.168.24.1	192.168.24.5 255.255.255.0 192.168.24.1	192.168.23.1 255.255.255.0	192.168.24.1 255.255.255.0
13	192.168.26.4 255.255.255.0 192.168.26.1	192.168.26.5 255.255.255.0 192.168.26.1	192.168.25.1 255.255.255.0	192.168.26.1 255.255.255.0
14	192.168.28.4 255.255.255.0 192.168.28.1	192.168.28.5 255.255.255.0 192.168.28.1	192.168.27.1 255.255.255.0	192.168.28.1 255.255.255.0
15	192.168.30.4 255.255.255.0 192.168.30.1	192.168.30.5 255.255.255.0 192.168.30.1	192.168.29.1 255.255.255.0	192.168.30.1 255.255.255.0

Питання для самоконтролю.

1. Для чого використовується шлюз?

2. Скільки підмереж використовувались в завданні? Дайте розширену відповідь.

3. Які пристрої застосовувались в завданні?

8. Конфігурування маршрутизатора Cisco в якості сервера DHCP

Маршрутизатор з підтримкою Cisco IOS можна зробити сервером DHCP. Це спростить процес управління мережевими IP-адресами. При зміні параметрів конфігурації IP, адміністраторові потрібно буде оновити лише один, центральний, маршрутизатор.

Протокол DHCP вже розглядався при виконанні попередніх завдань. Він призначений для автоматичного надання вузлам IP-адреси.

Для налагодження DHCP маршрутизатора, потрібно проробити такі дії:

- Створити пул адрес DHCP;
- Вказати IP-адресу сервера DNS;
- Вказати під мережу (шлюз);
- Виключити IP-адреси;
- Перевірити конфігурацію.

Практичне завдання 8.

В завданні потрібно створити локальну мережу, в яку будуть входити: маршрутизатор з інтегрованими службами 1841, два принтери Printer-PT, два комутатори 2960-24TT, два сервера Server-PT та п’ять комп’ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 8.1.

1.1 З розділу ***Switches*** (комутатори) добавити в робочу область два комутатори серії ***2960-24TT***. Далі з розділу ***End Devices*** (кінцеві пристрої) добавити п’ять комп’ютерів ***PC–PT***, два сервери ***Server-PT*** та два принтери ***Printer-PT*** і з розділу ***Router*** (маршрутизатори) добавити маршрутизатор серії ***1841***.

1.2 З’єднати пристрої, як це показано на схемі, кабелем з прямим з’єднанням контактів (***Copper Straight–Through***) з розділу ***Connections***, а також з’єднати консольним кабелем (***Console***) комп’ютер ***PC0*** та маршрутизатор ***Router1*** використовуючи гніздо на комп’ютері ***RS 232***, а на маршрутизаторі ***Console***.

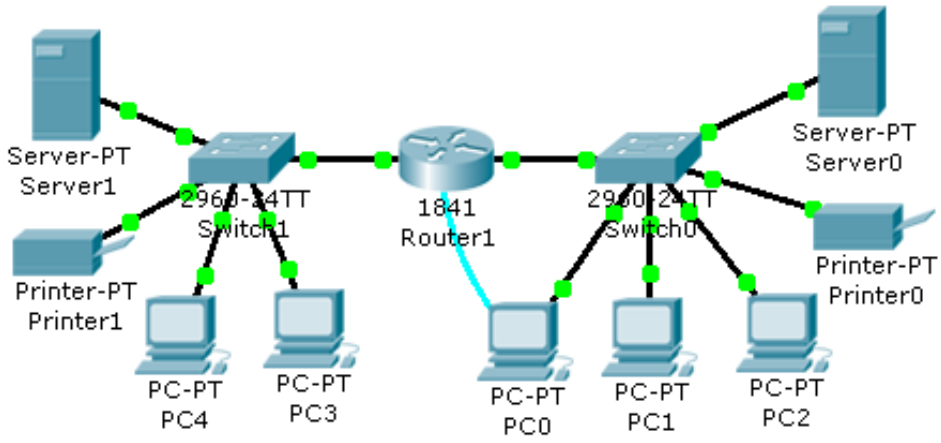


Рисунок 8.1 – Схема локальної мережі складена з маршрутизатора, двох комутаторів, двох серверів, двох принтерів та п’яти комп’ютерів.

2. З комп’ютера користувача ***PC0*** в програмі емуляції терміналу підключіться до консолі маршрутизатора користувача ***Route1*** шляхом:

- натиснення ЛК миші на комп’ютер;
- перейти на вкладку робочого столу (***Desktop***);
- натиснути на піктограму ***Terminal***;
- клацнути ЛК миші на кнопку ***OK***.

3. Метод конфігурування маршрутизатора вже розглядався при виконанні попередніх завдань але там використовувалась конфігурація через командний рядок, а в даному завданні – через термінал.

4. Перейти в глобальний контекст конфігурування командами ***enable*** та ***configure terminal***:

Router> enable

Router#configure terminal

5. За допомогою відомої команди ***hostname*** змінити ім’я маршрутизатора на те що вказане в таблиці варіантів.

6. Активувати та надати інтерфейсам ***FastEhernet 0/0***, ***FastEhernet 0/1*** відповідні IP-адреси і маски підмережі, що вказані в таблиці варіантів. Приклад конфігурації FastEhernet 0/1:

…

Router(config)#interface fastethernet 0/0

Router(config-if)#ip address [*IP-адреса інтерфейса, що вказана у варіанті*] [*маска підмережі, що вказана у варіанті*]

Примітка: квадратні дужки не використовуються

Router(config-if)#no shutdown

Примітка: команда ***no shutdown*** *використовується для активації інтерфейсу.*

Router(config-if)# exit

Аналогічно конфігурується інтерфейс FastEthernet 0/1.

7. Наступним кроком буде конфігурування послуги DHCP. Це робиться наступною групою команд:

…

Router(config)#ip dhcp pool pool1

Примітка: створення пул адрес DHCP з ім'ям pool1

Router(dhcp-config)#network [*діапазон мережевих адрес, що вказано у варіанті*]

Примітка: створення діапазону мережевих адрес для пулу DHCP.

Router(dhcp-config)#dns-server [*IP-адреса сервера DNS, що вказано у варіанті*]

Router(dhcp-config)#default-route [*IP-адреса шлюзу, що вказано у варіанті*]

Router(dhcp-config)#exit

Router(config)#ip dhcp excluded-address [*початковий та кінцевий адреси, що виключаються з пулу адрес, вказано у варіанті*]

Примітка: ці адреси не будуть надаватися послугою, їх може призначити тільки адміністратор.

Аналогічно сконфігурувати пул 2.

8. Увійти в конфігурацію кожного комп'ютера та включити послугу DHCP шляхом:

- натиснення ЛК миші на комп'ютер;
- перейти на вкладку робочого столу (***Desktop***);

- натиснути на піктограму ***IP Configuration***;
- відмітити крапкою рядок DHCP.

В результаті повинно автоматично відобразитись IP-адреса, маска підмережі, шлюз і DNS сервер.

9. Аналогічно провести налагодження інших комп'ютерів.

10. Щоб налагодити принтер, то потрібно:

- клацнути ЛК миші на принтер;
- перейти на вкладку конфігурації (***Config***);
- відмітити крапкою рядок DHCP.

11. Що стосується серверів, то їх налагодити автоматично не можна. Тому їх конфігурації потрібно задати:

- натиснення ЛК миші на сервер;
- перейти на вкладку робочого столу (***Desktop***);
- натиснути на піктограму ***IP Configuration***;
- задати параметри відповідно до варіанту.

12. Щоб переконатись, що мережа працює, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [IP-адреса комп'ютера PC3]

PC>ping [IP-адреса принтера Printer1]

13. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

14. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити такі три маршрути:

- комп'ютер PC0 – комп'ютер PC3;
- комп'ютер PC0 – принтер Printer0;
- комп'ютер PC4 – сервер Server1.

Можна створити свої маршрути, щоб перевірити мережу.

15. Зберегти файл та продемонструвати викладачеві.

Таблиця 8.1 Варіанти до практичного завдання 8.

№ варіанту	Ім'я комутатора	IP-адреса та маска FastEthernet 0/0	IP-адреса та маска FastEthernet 0/1	Діапазон мережевих адрес для pool1	Діапазон мережевих адрес для pool2	IP-адресу сервера DNS використовувати для pool1 і pool2
1	White	192.168.1.1 255.255.255.0	192.168.2.1 255.255.255.0	192.168.1.0 255.255.255.0	192.168.2.0 255.255.255.0	192.168.1.10
2	Black	192.168.3.1 255.255.255.0	192.168.4.1 255.255.255.0	192.168.3.0 255.255.255.0	192.168.4.0 255.255.255.0	192.168.3.10
3	Green	192.168.5.1 255.255.255.0	192.168.6.1 255.255.255.0	192.168.5.0 255.255.255.0	192.168.6.0 255.255.255.0	192.168.5.10
4	Yellow	192.168.7.1 255.255.255.0	192.168.8.1 255.255.255.0	192.168.7.0 255.255.255.0	192.168.8.0 255.255.255.0	192.168.7.10
5	Blue	192.168.9.1 255.255.255.0	192.168.10.1 255.255.255.0	192.168.9.0 255.255.255.0	192.168.10.0 255.255.255.0	192.168.9.10
6	Gold	192.168.12.1 255.255.255.0	192.168.13.1 255.255.255.0	192.168.12.0 255.255.255.0	192.168.13.0 255.255.255.0	192.168.12.10
7	Brown	192.168.14.1 255.255.255.0	192.168.15.1 255.255.255.0	192.168.14.0 255.255.255.0	192.168.15.0 255.255.255.0	192.168.14.10
8	Cream	192.168.16.1 255.255.255.0	192.168.17.1 255.255.255.0	192.168.16.0 255.255.255.0	192.168.17.0 255.255.255.0	192.168.16.10
9	Cyan	192.168.18.1 255.255.255.0	192.168.19.1 255.255.255.0	192.168.18.0 255.255.255.0	192.168.19.0 255.255.255.0	192.168.18.10
10	Grey	192.168.20.1 255.255.255.0	192.168.21.1 255.255.255.0	192.168.20.0 255.255.255.0	192.168.21.0 255.255.255.0	192.168.20.10
11	Magenta	192.168.22.1 255.255.255.0	192.168.23.1 255.255.255.0	192.168.22.0 255.255.255.0	192.168.23.0 255.255.255.0	192.168.22.10
12	Orange	192.168.24.1 255.255.255.0	192.168.25.1 255.255.255.0	192.168.24.0 255.255.255.0	192.168.25.0 255.255.255.0	192.168.24.10
13	Red	192.168.26.1 255.255.255.0	192.168.27.1 255.255.255.0	192.168.26.0 255.255.255.0	192.168.27.0 255.255.255.0	192.168.26.10
14	Ping	192.168.28.1 255.255.255.0	192.168.29.1 255.255.255.0	192.168.28.0 255.255.255.0	192.168.29.0 255.255.255.0	192.168.27.10
15	Silver	192.168.30.1 255.255.255.0	192.168.31.1 255.255.255.0	192.168.30.0 255.255.255.0	192.168.31.0 255.255.255.0	192.168.30.10

Продовження таблиці 8.1 Варіанти до практичного завдання 8.

№ варіанту	IP-адреса шлюзу для pool1	IP-адреса шлюзу для pool2	Початкова та кінцева адреса, що виключа-ються з пулу адрес pool1	Початкова та кінцева адреса, що виключа-ються з пулу адрес pool2	IP-адреса, маска та шлюз серверу Server0	IP-адреса, маска та шлюз серверу Server1
1	**2**	**3**	**4**	**5**	**6**	**7**
1	192.168.1.1	192.168.2.1	192.168.1.2 192.168.1.5	192.168.2.2 192.168.2.5	192.168.1.20 255.255.255.0 192.168.1.1	192.168.2.20 255.255.255.0 192.168.2.1
2	192.168.3.1	192.168.4.1	192.168.3.2 192.168.3.5	192.168.4.2 192.168.4.5	192.168.3.20 255.255.255.0 192.168.3.1	192.168.4.20 255.255.255.0 192.168.4.1

1	2	3	4	5	6	7
3	192.168.5.1	192.168.6.1	192.168.5.2 192.168.5.5	192.168.6.2 192.168.6.5	192.168.5.20 255.255.255.0 192.168.5.1	192.168.6.20 255.255.255.0 192.168.2.1
4	192.168.7.1	192.168.8.1	192.168.7.2 192.168.7.5	192.168.8.2 192.168.8.5	192.168.7.20 255.255.255.0 192.168.7.1	192.168.6.20 255.255.255.0 192.168.6.1
5	192.168.9.1	192.168.10.1	192.168.9.2 192.168.9.5	192.168.10.2 192.168.10.5	192.168.9.20 255.255.255.0 192.168.9.1	192.168.10.20 255.255.255.0 192.168.10.1
6	192.168.12.1	192.168.13.1	192.168.12.2 192.168.12.5	192.168.13.2 192.168.13.5	192.168.12.20 255.255.255.0 192.168.12.1	192.168.13.20 255.255.255.0 192.168.13.1
7	192.168.14.1	192.168.15.1	192.168.14.2 192.168.14.5	192.168.15.2 192.168.15.5	192.168.14.20 255.255.255.0 192.168.14.1	192.168.15.20 255.255.255.0 192.168.15.1
8	192.168.16.1	192.168.17.1	192.168.16.2 192.168.16.5	192.168.17.2 192.168.17.5	192.168.16.20 255.255.255.0 192.168.16.1	192.168.17.20 255.255.255.0 192.168.17.1
9	192.168.18.1	192.168.19.1	192.168.18.2 192.168.18.5	192.168.19.2 192.168.19.5	192.168.18.20 255.255.255.0 192.168.18.1	192.168.19.20 255.255.255.0 192.168.19.1
10	192.168.20.1	192.168.21.1	192.168.20.2 192.168.20.5	192.168.21.2 192.168.21.5	192.168.20.20 255.255.255.0 192.168.20.1	192.168.21.20 255.255.255.0 192.168.21.1
11	192.168.22.1	192.168.23.1	192.168.22.2 192.168.22.5	192.168.23.2 192.168.23.5	192.168.22.20 255.255.255.0 192.168.22.1	192.168.23.20 255.255.255.0 192.168.23.1
12	192.168.24.1	192.168.25.1	192.168.24.2 192.168.24.5	192.168.25.2 192.168.25.5	192.168.24.20 255.255.255.0 192.168.24.1	192.168.25.20 255.255.255.0 192.168.25.1
13	192.168.26.1	192.168.27.1	192.168.26.2 192.168.26.5	192.168.27.2 192.168.27.5	192.168.26.20 255.255.255.0 192.168.26.1	192.168.27.20 255.255.255.0 192.168.27.1
14	192.168.28.1	192.168.29.1	192.168.28.2 192.168.28.5	192.168.29.2 192.168.29.5	192.168.28.20 255.255.255.0 192.168.28.1	192.168.29.20 255.255.255.0 192.168.29.1
15	192.168.30.1	192.168.31.1	192.168.30.2 192.168.30.5	192.168.31.2 192.168.31.5	192.168.30.20 255.255.255.0 192.168.30.1	192.168.31.20 255.255.255.0 192.168.31.1

Питання для самоконтролю.

1. Для чого потрібний протокол DHCP?
2. Які дані автоматично отримує комп’ютер?

9. Статична маршрутизація

Статична маршрутизована IP-мережа не використовує протоколи маршрутизації, оскільки вся інформація про маршрутизації зберігається в статичній таблиці на кожному маршрутизаторі [14]. Щоб будь-які два довільних хоста в мережі могли взаємодіяти між собою, кожен маршрутизатор повинен мати таку таблицю маршрутів.

Статичне маршрутизоване IP-середовище найкраще підходить для невеликої мережі, що рідко змінюється структурою, в якій відсутні альтернативні маршрути. Статичне маршрутизоване середовище може застосовуватися для:

- мережі малого підприємства;
- мережі домашнього офісу;
- філіалу з однією мережею.

Замість реалізації протоколу маршрутизації через вузько-смуговий канал зв'язку, одиночний маршрут за замовчуванням на маршрутизаторі філіалу гарантує, що весь трафік, не призначений для комп'ютера в мережі філіалу, буде направлений в основний офіс.

Переваги статичної маршрутизації:

- легкість налагодження і конфігурації в малих мережах;
- відсутність додаткових накладних витрат (через відсутність протоколів маршрутизації);
- миттєва готовність (не потрібен інтервал для конфігурування/ підстроювання);
- низьке навантаження на процесор маршрутизатора;
- передбачуваність в кожен момент часу.

Недоліки статичної маршрутизації:

Відсутність відмовостійкості. Якщо в силу будь-яких причин один із маршрутизаторів виходить з ладу або стає недоступним комунікаційний канал, статичний маршрутизатор не зможе якось відреагувати на несправність [13]. Більше того, інші маршрутизатори в мережі не будуть знати про несправності і

будуть продовжувати передавати дані по недоступному маршруту. У мережах малого офісу (наприклад, з двома маршрутизаторами і трьома мережами, з'єднаними в ЛВС) подібні ситуації можуть вирішуватися адміністратором оперативно. У великих мережах більш кращим виявляється використання спеціальних протоколів маршрутизації;

Непродуктивні адміністративні витрати. Якщо додається нова підмережа або видаляється з міжмережевого середовища існуюча, маршрути до неї повинні бути вручну додані або видалені. Якщо додається новий маршрутизатор, то він повинен бути правильно налаштований для маршрутизації в міжмережевому середовищі.

Практичне завдання 9.

В завданні потрібно створити локальну мережу, в яку будуть входити: два маршрутизатори з інтегрованими службами 1841, два комутатори 2960-24TT та чотири комп'ютера PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 9.1 (обов'язково дотримуйтесь схеми при з'єднанні інтерфейсів). Маршрутизатори з'єднати між собою кабелем з перехресним з'єднанням контактів, а всі інші пристрої – кабелем з прямим з'єднанням контактів.

2. Надати кожному комп'ютеру IP-адресу, маску підмережі та шлюз, що вказані у таблиці варіантів.

3. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

4. Перейти на вкладку "Конфігурація" (***Config***), щоб увімкнути та налагодити відповідні інтерфейси. Для цього потрібно натиснути на інтерфейс ***FastEthernet0/0***, задати IP адресу, маску підмережі, що вказані в таблиці варіантів та поставити відмітку ***ON*** навпроти рядка ***Port Status***. Аналогічно налаштувати інтерфейс ***FastEthernet0/1***.

5. Провести такі самі налаштунки на маршрутизаторі ***Router1***.

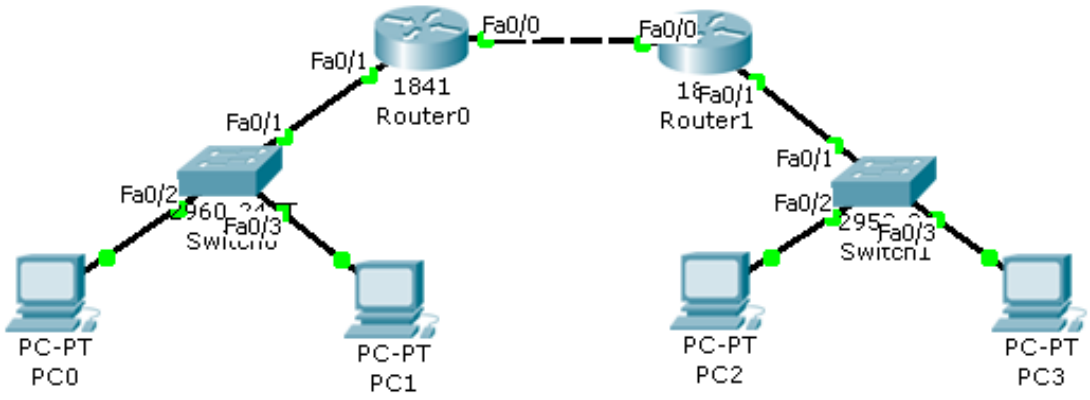


Рисунок 9.1 – Схема локальної мережі складена з двох маршрутизаторів, двох комутаторів та чотирьох комп'ютерів.

6. Для конфігурації статичної маршрутизації необхідно викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** де прописати:

…

Router(config)#ip route [*IP-адреса інтерфейсу FastEthernet0/1 маршрутизатора Router1 в форматі* ***X.X.X.0***] [маска підмережі] FastEthernet0/0

Примітка: вказується невідома мережа до якої потрібний доступ, маска підмережі та ім'я інтерфейсу маршрутизатора Router0 з яким буде зв'язок; FastEthernet0/0 інтерфейс через який відбувається зв'язок

7. Аналогічно налаштувати маршрутизатор ***Router1***.

8. Щоб подивитися на результат сконфігурованої статичної маршрутизації необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router #show ip route

Аналогічно перевірити інший маршрутизатор, а дані протоколу та таблиці маршрутизації занотувати.

9. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC3*]

Для більшої впевненості роботи мережі надіслати з інших комп'ютерів ***ping***-запити.

10. Відкрити режим моделювання (клацнути ЛК миші на кнопку ***Simulation Mode***).

11. Вибрати простий ***ping-запит*** (піктограма закритого конверту) та створити маршрут від комп'ютера ***PC0*** до комп'ютера ***PC2***.

12. У вікні симуляції натиснути на кнопку ***Auto Capture / Play***, що запустить симуляцію мережі та дозволить прослідкувати за ходом запиту.

13. Зберегти файл та продемонструвати викладачеві.

Таблиця 9.1 Варіанти до практичного завдання 9.

№ варіанту	Router0		Router1	
	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1
1	**2**	**3**	**4**	**5**
1	209.165.1.1 255.255.255.0	192.168.1.1 255.255.255.0	209.165.1.2 255.255.255.0	192.168.10.1 255.255.255.0
2	209.165.2.1 255.255.255.0	192.168.2.1 255.255.255.0	209.165.2.2 255.255.255.0	192.168.20.1 255.255.255.0
3	209.165.3.1 255.255.255.0	192.168.3.1 255.255.255.0	209.165.3.2 255.255.255.0	192.168.30.1 255.255.255.0
4	209.165.4.1 255.255.255.0	192.168.4.1 255.255.255.0	209.165.4.2 255.255.255.0	192.168.40.1 255.255.255.0
5	209.165.5.1 255.255.255.0	192.168.5.1 255.255.255.0	209.165.5.2 255.255.255.0	192.168.50.1 255.255.255.0
6	209.165.6.1 255.255.255.0	192.168.6.1 255.255.255.0	209.165.6.2 255.255.255.0	192.168.60.1 255.255.255.0
7	209.165.7.1 255.255.255.0	192.168.7.1 255.255.255.0	209.165.7.2 255.255.255.0	192.168.70.1 255.255.255.0
8	209.165.8.1 255.255.255.0	192.168.8.1 255.255.255.0	209.165.8.2 255.255.255.0	192.168.80.1 255.255.255.0
9	209.165.9.1 255.255.255.0	192.168.9.1 255.255.255.0	209.165.9.2 255.255.255.0	192.168.90.1 255.255.255.0
10	209.165.10.1 255.255.255.0	192.168.10.1 255.255.255.0	209.165.10.2 255.255.255.0	192.168.100.1 255.255.255.0
11	209.165.11.1 255.255.255.0	192.168.11.1 255.255.255.0	209.165.11.2 255.255.255.0	192.168.110.1 255.255.255.0
12	209.165.12.1 255.255.255.0	192.168.12.1 255.255.255.0	209.165.12.2 255.255.255.0	192.168.120.1 255.255.255.0

1	2	3	4	5
13	209.165.13.1 255.255.255.0	192.168.13.1 255.255.255.0	209.165.13.2 255.255.255.0	192.168.130.1 255.255.255.0
14	209.165.14.1 255.255.255.0	192.168.14.1 255.255.255.0	209.165.14.2 255.255.255.0	192.168.140.1 255.255.255.0
15	209.165.15.1 255.255.255.0	192.168.15.1 255.255.255.0	209.165.15.2 255.255.255.0	192.168.150.1 255.255.255.0

Продовження таблиці 9.1 Варіанти до практичного завдання 9.

№ варіанту	IP-адреса та маска PC0	IP-адреса та маска PC1	IP-адреса та маска PC2	IP-адреса та маска PC3	Шлюз для комп'ютерів PC0 та PC1	Шлюз для комп'ютерів PC2 та PC3
1	192.168.1.2 255.255.255.0	192.168.1.3 255.255.255.0	192.168.10.2 255.255.255.0	192.168.10.3 255.255.255.0	192.168.1.1	192.168.10.1
2	192.168.2.2 255.255.255.0	192.168.2.3 255.255.255.0	192.168.20.2 255.255.255.0	192.168.20.3 255.255.255.0	192.168.2.1	192.168.20.1
3	192.168.3.2 255.255.255.0	192.168.3.3 255.255.255.0	192.168.30.2 255.255.255.0	192.168.30.3 255.255.255.0	192.168.3.1	192.168.30.1
4	192.168.4.2 255.255.255.0	192.168.4.3 255.255.255.0	192.168.40.2 255.255.255.0	192.168.40.3 255.255.255.0	192.168.4.1	192.168.40.1
5	192.168.5.2 255.255.255.0	192.168.5.3 255.255.255.0	192.168.50.2 255.255.255.0	192.168.50.3 255.255.255.0	192.168.5.1	192.168.50.1
6	192.168.6.2 255.255.255.0	192.168.6.3 255.255.255.0	192.168.60.2 255.255.255.0	192.168.60.3 255.255.255.0	192.168.6.1	192.168.60.1
7	192.168.7.2 255.255.255.0	192.168.7.3 255.255.255.0	192.168.70.2 255.255.255.0	192.168.70.3 255.255.255.0	192.168.7.1	192.168.70.1
8	192.168.8.2 255.255.255.0	192.168.8.3 255.255.255.0	192.168.80.2 255.255.255.0	192.168.80.3 255.255.255.0	192.168.8.1	192.168.80.1
9	192.168.9.2 255.255.255.0	192.168.9.3 255.255.255.0	192.168.90.2 255.255.255.0	192.168.90.3 255.255.255.0	192.168.9.1	192.168.90.1
10	192.168.10.2 255.255.255.0	192.168.10.3 255.255.255.0	192.168.100.2 255.255.255.0	192.168.100.3 255.255.255.0	192.168.10.1	192.168.100.1
11	192.168.11.2 255.255.255.0	192.168.11.3 255.255.255.0	192.168.110.2 255.255.255.0	192.168.110.3 255.255.255.0	192.168.11.1	192.168.110.1
12	192.168.12.2 255.255.255.0	192.168.12.3 255.255.255.0	192.168.120.1 255.255.255.0	192.168.120.3 255.255.255.0	192.168.12.1	192.168.120.1
13	192.168.13.2 255.255.255.0	192.168.13.3 255.255.255.0	192.168.130.2 255.255.255.0	192.168.130.3 255.255.255.0	192.168.13.1	192.168.130.1
14	192.168.14.2 255.255.255.0	192.168.14.3 255.255.255.0	192.168.140.2 255.255.255.0	192.168.140.3 255.255.255.0	192.168.14.1	192.168.140.1
15	192.168.15.2 255.255.255.0	192.168.15.3 255.255.255.0	192.168.150.2 255.255.255.0	192.168.150.3 255.255.255.0	192.168.15.1	192.168.150.1

Питання для самоконтролю.

1. Для яких мереж краще використовувати статичну маршрутизацію?

2. Які переваги у статичній маршрутизації?

3. Які недоліки у статичній маршрутизації?

10. Налагодження протоколу маршрутизації RIP

Протокол обміну інформацією про маршрутизацію (Routing Information Protocol, RIP) розроблявся, як механізм, за допомогою якого маршрутизатори можуть обмінюватися інформацією про оновлення таблиць маршрутизації [8]. Цей механізм спочатку передбачався для використання в мережах відносно невеликого розміру (це вірно для RIP версії 1).

Протокол RIP використовує таку схему побудови таблиці маршрутизації – спочатку таблиця маршрутизації кожного маршрутизатора включає в себе маршрути тільки для тих підмереж, що фізично під'єднанні до маршрутизатора. Використовуючи протокол RIP, маршрутизатор періодично відправляє іншим маршрутизаторам оголошення, що містять інформацію про вміст власної таблиці маршрутизації. RIP версії 1 використовує для передачі оголошень широкомовні IP-пакети. RIP версії 2 дозволяє використовувати для оголошень також пакети групового мовлення. Кожен маршрутизатор розсилає подібні оголошення періодично з інтервалом у 30 секунд.

Маршрутизатори, що використовують протокол RIP, можуть також повідомляти інформацію про маршрутизації за допомогою тригерних оновлень. Тригерні оновлення ініціюються, коли відбувається зміна топології мережі і надсилається оновлена інформація про маршрутизацію, яка відображає ці зміни. Тригерні оновлення відбуваються миттєво, отже, інформація про маршрутизації оновиться раніше, ніж відбудеться наступне періодичне оголошення. Наприклад, коли маршрутизатор виявляє встановлення нового з'єднання або відмову сусіднього маршрутизатора, він модифікує власну таблицю маршрутизації і розсилає оновлені маршрути. Кожен маршрутизатор, який одержує тригерне оновлення, змінює власну таблицю маршрутизації і поширює зміну [8, 9].

Основна перевага RIP полягає в простоті розгортання та конфігурування. Як недолік RIP версії 1 можна відзначити наявність жорсткого обмеження на розмір мережі. Протокол RIP може бути використаний в мережі, в якій два хоста розділені не більше ніж 15 маршрутизаторами. Іншими словами, маршрутизатор,

що використовує протокол RIP для побудови таблиці маршрутизації, "знає" тільки про тих підмережах, що розташовані на відстані не більше 15 переходів. Підмережі, розташовані на відстані 16 або більше пересилань, вважаються недосяжними.

Оскільки глобальні IP-мережі стають все більше і більше, періодичні RIP-оголошення кожного маршрутизатора можуть викликати надмірний трафік. В якості іншого недоліку протоколу RIP можна відзначити високий час оновлення. У ситуації, коли в структурі мережі відбуваються зміни, може пройти кілька хвилин, перше ніж усі корпоративні маршрутизатори отримають інформацію про зміну та переконфігурують власні таблиці маршрутизації. За той час, як відбувається реконфігурування маршрутизаторів, можуть утворитися цикли маршрутизації, що призведуть до втрати або неможливості доставки даних. В умовах підвищених вимог до надійності каналу даних існуючих можливостей протоколу RIP може бути недостатньо.

RIP версії 2 підтримує оголошення, що розсилаються за допомогою групових розсилок, просту аутентифікацію за допомогою пароля, а також дає можливість гнучкої настройки при роботі в середовищах з підмережами і в CIDR-середовищах (Classless Inter Domain Routing, Безкласова міждоменна маршрутизація).

Використання в мережі протоколу маршрутизації RIP виправдано у разі невеликої мережі з динамічно змінною структурою, що має кілька можливих маршрутів.

Практичне завдання 10.

В завданні потрібно створити локальну мережу, в яку будуть входити: два маршрутизатори з інтегрованими службами 1841, два комутатори 2960-24TT, та чотири комп’ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 10.1 (обов’язково дотримуйтесь схеми при з’єднанні інтерфейсів). Маршрутизатори з’єднати між собою кабелем з перехресним з’єднанням контактів, а всі інші пристрої – кабелем з прямим з’єднанням контактів.

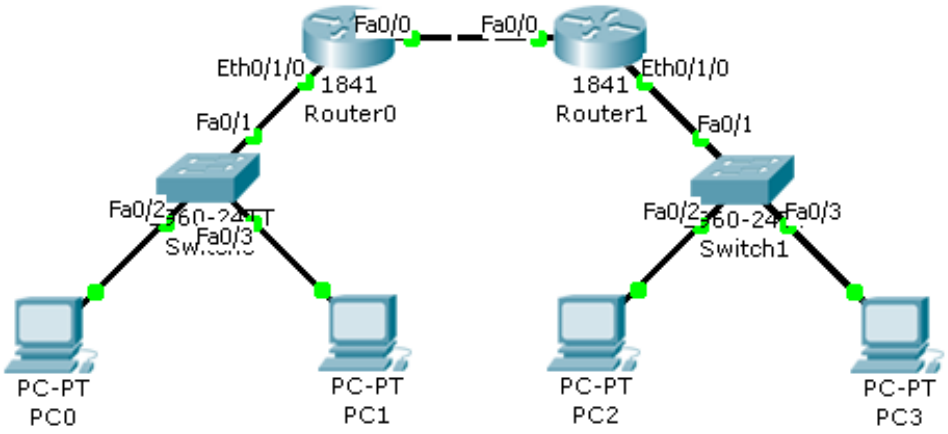


Рисунок 10.1 – Схема локальної мережі складена з двох маршрутизаторів, двох комутаторів та чотирьох комп’ютерів.

2. Надати кожному комп’ютеру IP-адресу, маску підмережі та шлюз, що вказані у таблиці варіантів.

3. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

4. На вкладці "Вид фізичного пристрою" (***Physical***) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

5. В лівій частині вікна натиснути на кнопку ***WIC-1ENET*** (плата, що має один роз’єм Ethernet), після чого в низу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний роз’єм маршрутизатора.

6. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

7. Після того, як було подано живлення потрібно зачекати секунд 20 (вступають в дію налаштунки) та перейти на вкладку "Конфігурація" (***Config***), щоб увімкнути та налагодити відповідні інтерфейси. Для цього потрібно натиснути на інтерфейс ***FastEthernet0/0***, задати IP адресу, маску підмережі, що вказані в таблиці варіантів та поставити відмітку ***ON*** навпроти рядка ***Port Status***. Аналогічно налаштувати інтерфейс ***Ethernet0/1/0***.

8. Провести такі самі налаштунки на маршрутизаторі ***Router1***.

9. Для конфігурації протоколу RIP необхідно викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** де прописати:

…

Router(config)#route rip

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Router(config-router)#network [*IP-адреса інтерфейсу Ethernet0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Примітка: в форматі ***X.X.X.0*** *– перші три X – це перші три числа IP-адреси інтерфейсу.*

10. Налаштувати протокол RIP можна і іншим чином, як це показано для ***Router1*** – викликати вікно конфігурації маршрутизатора ***Router1*** та перейти на вкладку "Конфігурація" (***Config***). В лівій панелі вікна натиснути на кнопку RIP, і навпроти рядка ***Network*** ввести IP-адресу інтерфейсу FastEthernet0/0 маршрутизатора Router1 в форматі ***X.X.X.0*** та натиснути кнопку ***Add***. Після цього знову навпроти рядка ***Network*** ввести IP-адресу інтерфейсу Ethernet0/1/0 маршрутизатора Router1 в форматі ***X.X.X.0*** та натиснути кнопку ***Add***.

11. Щоб подивитися на результат сконфігурованого протоколу RIP необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router#show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

Router#show ip route

Аналогічно перевірити інший маршрутизатор, а дані протоколу та таблиці маршрутизації занотувати.

12. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп’ютеру ***PC1*** та перейти на вкладку

робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC3*]

Можна протестувати і інші комп'ютери для більшої впевненості.

13. Зберегти файл та продемонструвати викладачеві.

Таблиця 10.1 Варіанти до практичного завдання 10.

№ варіанту	Router0		Router1	
	IP-адреса та маска інтерфейсу FastEhernet0/0	**IP-адреса та маска інтерфейсу Ehernet0/1/0**	**IP-адреса та маска інтерфейсу FastEhernet0/0**	**IP-адреса та маска інтерфейсу Ehernet0/1/0**
1	209.165.1.1 255.255.255.0	192.168.1.1 255.255.255.0	209.165.1.2 255.255.255.0	192.168.10.1 255.255.255.0
2	209.165.2.1 255.255.255.0	192.168.2.1 255.255.255.0	209.165.2.2 255.255.255.0	192.168.20.1 255.255.255.0
3	209.165.3.1 255.255.255.0	192.168.3.1 255.255.255.0	209.165.3.2 255.255.255.0	192.168.30.1 255.255.255.0
4	209.165.4.1 255.255.255.0	192.168.4.1 255.255.255.0	209.165.4.2 255.255.255.0	192.168.40.1 255.255.255.0
5	209.165.5.1 255.255.255.0	192.168.5.1 255.255.255.0	209.165.5.2 255.255.255.0	192.168.50.1 255.255.255.0
6	209.165.6.1 255.255.255.0	192.168.6.1 255.255.255.0	209.165.6.2 255.255.255.0	192.168.60.1 255.255.255.0
7	209.165.7.1 255.255.255.0	192.168.7.1 255.255.255.0	209.165.7.2 255.255.255.0	192.168.70.1 255.255.255.0
8	209.165.8.1 255.255.255.0	192.168.8.1 255.255.255.0	209.165.8.2 255.255.255.0	192.168.80.1 255.255.255.0
9	209.165.9.1 255.255.255.0	192.168.9.1 255.255.255.0	209.165.9.2 255.255.255.0	192.168.90.1 255.255.255.0
10	209.165.10.1 255.255.255.0	192.168.10.1 255.255.255.0	209.165.10.2 255.255.255.0	192.168.100.1 255.255.255.0
11	209.165.11.1 255.255.255.0	192.168.11.1 255.255.255.0	209.165.11.2 255.255.255.0	192.168.110.1 255.255.255.0
12	209.165.12.1 255.255.255.0	192.168.12.1 255.255.255.0	209.165.12.2 255.255.255.0	192.168.120.1 255.255.255.0
13	209.165.13.1 255.255.255.0	192.168.13.1 255.255.255.0	209.165.13.2 255.255.255.0	192.168.130.1 255.255.255.0
14	209.165.14.1 255.255.255.0	192.168.14.1 255.255.255.0	209.165.14.2 255.255.255.0	192.168.140.1 255.255.255.0
15	209.165.15.1 255.255.255.0	192.168.15.1 255.255.255.0	209.165.15.2 255.255.255.0	192.168.150.1 255.255.255.0

Продовження таблиці 10.1 Варіанти до практичного завдання 10.

№ варіанту	IP-адреса та маска PC0	IP-адреса та маска PC1	IP-адреса та маска PC2	IP-адреса та маска PC3	Шлюз для комп'ютерів PC0 та PC1	Шлюз для комп'ютерів PC2 та PC3
1	192.168.1.2 255.255.255.0	192.168.1.3 255.255.255.0	192.168.10.2 255.255.255.0	192.168.10.3 255.255.255.0	192.168.1.1	192.168.10.1
2	192.168.2.2 255.255.255.0	192.168.2.3 255.255.255.0	192.168.20.2 255.255.255.0	192.168.20.3 255.255.255.0	192.168.2.1	192.168.20.1
3	192.168.3.2 255.255.255.0	192.168.3.3 255.255.255.0	192.168.30.2 255.255.255.0	192.168.30.3 255.255.255.0	192.168.3.1	192.168.30.1
4	192.168.4.2 255.255.255.0	192.168.4.3 255.255.255.0	192.168.40.2 255.255.255.0	192.168.40.3 255.255.255.0	192.168.4.1	192.168.40.1
5	192.168.5.2 255.255.255.0	192.168.5.3 255.255.255.0	192.168.50.2 255.255.255.0	192.168.50.3 255.255.255.0	192.168.5.1	192.168.50.1
6	192.168.6.2 255.255.255.0	192.168.6.3 255.255.255.0	192.168.60.2 255.255.255.0	192.168.60.3 255.255.255.0	192.168.6.1	192.168.60.1
7	192.168.7.2 255.255.255.0	192.168.7.3 255.255.255.0	192.168.70.2 255.255.255.0	192.168.70.3 255.255.255.0	192.168.7.1	192.168.70.1
8	192.168.8.2 255.255.255.0	192.168.8.3 255.255.255.0	192.168.80.2 255.255.255.0	192.168.80.3 255.255.255.0	192.168.8.1	192.168.80.1
9	192.168.9.2 255.255.255.0	192.168.9.3 255.255.255.0	192.168.90.2 255.255.255.0	192.168.90.3 255.255.255.0	192.168.9.1	192.168.90.1
10	192.168.10.2 255.255.255.0	192.168.10.3 255.255.255.0	192.168.100.2 255.255.255.0	192.168.100.3 255.255.255.0	192.168.10.1	192.168.100.1
11	192.168.11.2 255.255.255.0	192.168.11.3 255.255.255.0	192.168.110.2 255.255.255.0	192.168.110.3 255.255.255.0	192.168.11.1	192.168.110.1
12	192.168.12.2 255.255.255.0	192.168.12.3 255.255.255.0	192.168.120.1 255.255.255.0	192.168.120.3 255.255.255.0	192.168.12.1	192.168.120.1
13	192.168.13.2 255.255.255.0	192.168.13.3 255.255.255.0	192.168.130.2 255.255.255.0	192.168.130.3 255.255.255.0	192.168.13.1	192.168.130.1
14	192.168.14.2 255.255.255.0	192.168.14.3 255.255.255.0	192.168.140.2 255.255.255.0	192.168.140.3 255.255.255.0	192.168.14.1	192.168.140.1
15	192.168.15.2 255.255.255.0	192.168.15.3 255.255.255.0	192.168.150.2 255.255.255.0	192.168.150.3 255.255.255.0	192.168.15.1	192.168.150.1

Питання для самоконтролю.

1. В яких цілях використовується протокол маршрутизації RIP?
2. Як відбувається побудова таблиці маршрутизації в протоколі RIP?
3. Які недоліки в протоколі маршрутизації RIP?

11. Налагодження протоколу маршрутизації IGRP та протоколу OSPF

Протокол маршрутизації IGRP

Протокол IGRP розроблений фірмою CISCO для своїх багатопротокольних маршрутизаторів в середині 80-х років [3]. IGRP являє собою протокол, який дозволяє великому числу маршрутизаторів координувати свою роботу. Основні переваги протоколу:

- стабільність маршрутів навіть у дуже великих і складних мережах;
- швидкий відгук на зміни топології мережі;
- мінімальна надмірність. Тому IGRP не вимагає додаткової пропускної здатності каналів для своєї роботи;
- поділ потоку даних між декількома паралельними маршрутами, приблизно рівних переваг;
- облік частоти помилок і рівня завантаження каналів;
- можливість реалізувати різні види сервісу для одного і того ж набору інформації.

На сьогодні реалізація протоколу орієнтована на TCP/IP. Проте, базова конструкція системи дозволяє використовувати IGRP і з іншими протоколами. IGRP має деяку схожість із старими протоколами, наприклад з RIP і Hello. Тут маршрутизатор обмінюється маршрутною інформацією тільки з безпосередніми сусідами. Тому завдання маршрутизації вирішується всією сукупністю маршрутизаторів, а не кожним окремо.

IGRP використовується в маршрутизаторах, які мають зв’язки з декількома мережами і виконують функції перемикачів пакетів. Коли якийсь об’єкт в одній мережі хоче послати пакет в іншу мережу, він повинен послати його відповідному маршрутизатору [4]. Якщо адресат знаходиться в одній з мереж, безпосередньо пов’язаної з маршрутизатором, він відправляє цей пакет за місцем призначення. Якщо ж адресат знаходиться в більш віддаленій мережі, маршрутизатор перешле

пакет іншому маршрутизатору, розташованому ближче до адресата. Тут також як і в інших протоколах для зберігання маршрутних даних використовуються спеціалізовані бази даних.

Протокол IGRP формує цю базу даних на основі інформації, яку він отримає від сусідніх маршрутизаторів. У найпростішому випадку знаходиться один шлях для кожної з мереж. Сегменти шляху характеризуються використовуваним мережним інтерфейсом, метрикою і маршрутизатором, куди слід спочатку послати пакет. Метрика – число, яке говорить про те, наскільки хороший цей маршрут. Це число дозволяє порівняти його з іншими маршрутами, що ведуть до того самого місця призначення і які забезпечують той же рівень QOS [5]. Передбачається можливість розділяти інформаційний потік між кількома доступними еквівалентними маршрутами. Користувач може сам розділити потік даних, якщо два або більше шляху виявилися майже рівними за метрикою, при цьому велика частина трафіку буде надіслана по шляху з кращою метрикою. Метрика, використовувана в IGRP, враховує:

- час затримки;
- пропускну здатність самого слабкого сегмента шляху (у бітах за секунду);
- завантаженість каналу (відносну);
- надійність каналу (визначається часткою пакетів, які досягли місця призначення непошкодженими).

Час затримки передбачається рівним часу, необхідного для досягнення місця призначення при нульовому завантаженні мережі. Додаткові затримки, пов’язані із завантаженням враховуються окремо.

Серед параметрів, які контролюються, але не враховуються метрикою, знаходяться – число кроків до мети і MTU (maximum transfer unit – розмір пакета пересилаємого без фрагментації). Розрахунок метрики виробляється для кожного сегмента шляху.

Час від часу кожен маршрутизатор широкомовно розсилає свою маршрутну інформацію всім сусіднім маршрутизаторам. Одержувач порівнює ці

дані з уже наявними і вносить, якщо потрібно, необхідні корекції. На підставі знову отриманої інформації можуть бути прийняті рішення про зміну маршрутів.

На початку 90-х років розроблена нова версія протоколу IGRP – EIGRP з поліпшеним алгоритмом оптимізації маршрутів, скороченим часом встановлення і масками субмереж змінної довжини. EIGRP підтримує багато протоколів мережевого рівня. Розсилка маршрутної інформації тут відбувається лише за зміни маршрутної ситуації. Протокол періодично розсилає сусіднім маршрутизаторам короткі повідомлення Hello [5]. Отримання відгуку означає, що сусід функціональний і можна здійснювати обмін маршрутною інформацією. Протокол EIGRP використовує таблиці сусідів (адреса і інтерфейс), топологічні таблиці (адреса місця призначення і список сусідів, що оголошують про доступність цієї адреси), стану і мітки маршрутів. Для кожного протокольного модуля створюється своя таблиця сусідів. Протоколом використовується повідомлення типу hello (мультикастна адресація), підтвердження (acknowledgent), актуалізація (update), запит (query; завжди мультикастний) і відгук (reply; надсилається відправнику запиту). Маршрути тут діляться на внутрішні і зовнішні – отримані від інших протоколів або записані в статичних таблицях.

Протокол маршрутизації OSPF

Протокол OSPF (Open Shortest Path First) розроблявся, як механізм, за допомогою якого маршрутизатори можуть обмінюватися інформацією про вміст таблиць маршрутизації у великому міжмережевому середовищі. Протокол OSPF є протоколом маршрутизації з оголошенням стану каналу зв’язку. В основі функціонування протоколу OSPF лежить алгоритм "першочергового виявлення найкоротшого шляху" (Shortest Path First, SPF), який використовується для обчислення маршрутів в таблиці маршрутизації. Використовуючи алгоритм SPF, маршрутизатор обчислює найкоротший шлях до всіх підмереж в міжмережевому середовищі. У маршрутах, розрахованих за допомогою алгоритму SPF, завжди відсутні цикли.

На відміну від протоколу RIP, протокол OSPF підтримує "карту" корпоративної мережі. Ця карта модифікується щоразу, коли відбувається будь-яка зміна в структурі мережі. Ця карта, що називається базою даних стану зв’язків (link state database), синхронізована для всіх OSPF-маршрутизаторів і використовується, щоб обчислити маршрути в таблиці маршрутизації. Зміни в структурі мережі призводять до негайного поширення відомостей про ці зміни на всі маршрутизатори, які у свою чергу, оновлюють власний примірник бази даних стану зв’язків. Оновлення бази даних станів зв’язків призводить до повторного перерахунку таблиці маршрутизації [7].

Починаючи свою роботу, кожен маршрутизатор сповіщає інші маршрутизатори про своє існування, відправляючи спеціальне повідомлення в усі доступні підмережі. Інші маршрутизатори отримують це повідомлення і оновлюють свій екземпляр бази даних про стан зв’язків. Фактично зазначена база даних і формується на підставі цих повідомлень.

Оскільки розмір бази даних станів зв’язків зростає, вимоги до обсягу пам’яті і час на обчислення маршруту збільшуються. Щоб вирішити цю проблему, OSPF розглядає міжмережеве середовище, як сукупність областей (під областю в даному випадку розуміється сукупність безперервних мереж), з’єднаних один з одним через деяку базову область (backbone area). Всі маршрутизатори, що належать до однієї області, мають ідентичні репліки баз даних стану зв’язків [2].

З метою ідентифікації областей, кожній з них виділяється спеціальний ідентифікатор (area ID), що представляє собою 32-розрядне число. Цей ідентифікатор записується так само, як і IP-адреса – у десятково-точковому форматі (тобто у вигляді чотирьох однобайтових чисел, розділених крапками). Ідентифікатор області ніяк не пов’язаний з IP-адресацією. Адміністратор може привласнювати ідентифікатори областям на свій розсуд, не озираючись на використовувані в мережі IP-адреси. При цьому одна область OSPF може включати до свого складу необмежену кількість підмереж (розмір області обмежується виключно розміром бази даних стану зв’язків).

Кожен маршрутизатор зберігає базу даних станів зв'язків тільки для тих областей, які під'єднані до маршрутизатора безпосередньо. Маршрутизатори, що з'єднують базову область з іншими областями, називаються прикордонними маршрутизаторами областей (Area Border Router, ABR). Прикордонні маршрутизатори накопичують зміни, отримані від інших маршрутизаторів області, і передають їх одним разом маршрутизаторам, розташованих в інших областях.

На рис. 11.1 показаний приклад поділу мережі на області у разі використання протоколу OSPF.

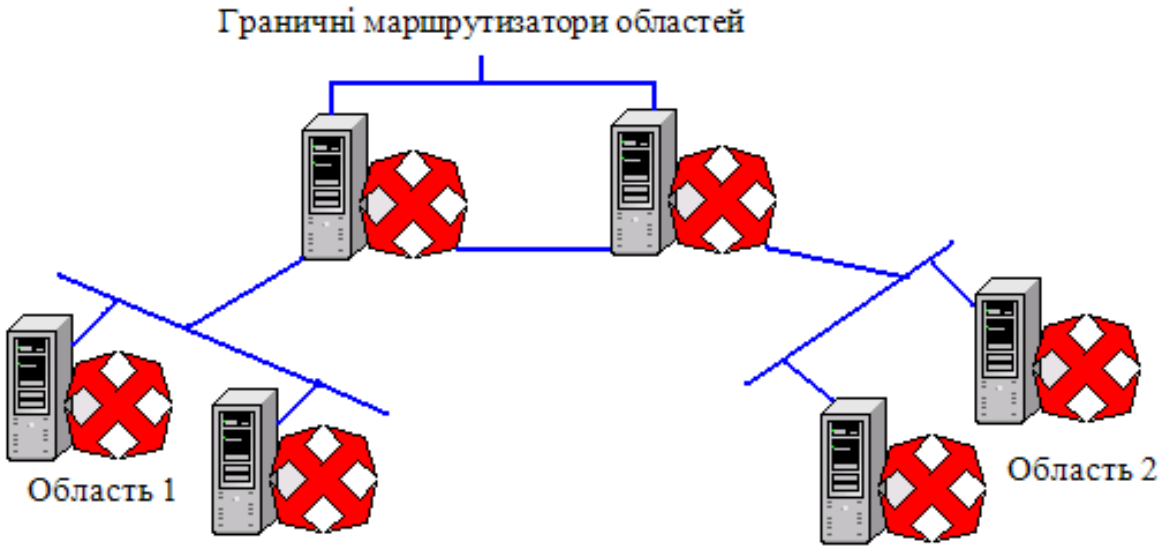


Рисунок 11.1 – Мережа з використанням протоколу OSPF.

Найбільша перевага протоколу OSPF полягає в тому, що він є високопродуктивним протоколом і призводить до незначних недоліків навіть у дуже великих міжмережевих конфігураціях. Як недолік протоколу OSPF можна відзначити певну складність його розгортання і конфігурації.

Переваги OSPF:

1. Для кожної адреси може бути декілька маршрутних таблиць, по одній на кожен вид IP-операції (TOS).

2. Кожному інтерфейсу присвоюється безрозмірний шлях, що враховує пропускну здатність, час транспортування повідомлення.

3. При існуванні еквівалентних маршрутів OSFP розподіляє потік рівномірно по цих маршрутах.

4. Підтримується адресацію субмереж (різні маски для різних маршрутів).

5. При зв'язку точка-точка не потрібно IP-адреси для кожного з кінців. (Економія адрес!)

6. Застосування мультикастінгу замість широкомовних повідомлень знижує завантаження не залучених сегментів.

Недоліки:

1. Важко отримати інформацію про перевагу каналів для вузлів, які підтримують інші протоколи, або зі статичної маршрутизацією.

2. OSPF є лише внутрішньою протоколом.

Практичне завдання 11.

В завданні потрібно створити локальну мережу, в яку будуть входити: три маршрутизатори з інтегрованими службами 1841, три комутатори 2950-24, та три комп'ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 11.2, але перш ніж з'єднувати пристрої кабелями, в маршрутизатор потрібно встановити плату ***WIC-1ENET*** (плата, що має один роз'єм Ethernet).

2. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

3. На вкладці "Вид фізичного пристрою" (***Physical***) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

4. В лівій частині вікна натиснути на кнопку ***WIC-1ENET***, після чого внизу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний роз'єм маршрутизатора.

5. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

6. Провести такі самі налаштунки на маршрутизаторі ***Router1*** та ***Router2***.

7. З'єднати всі пристрої між собою кабелями, при цьому обов'язково дотримуйтесь схеми при з'єднанні інтерфейсів. Маршрутизатори з'єднати між собою кабелем з перехресним з'єднанням контактів, а всі інші пристрої – кабелем з прямим з'єднанням контактів.

8. Надати кожному комп'ютеру IP-адресу, маску підмережі та шлюз, що вказані у таблиці варіантів.

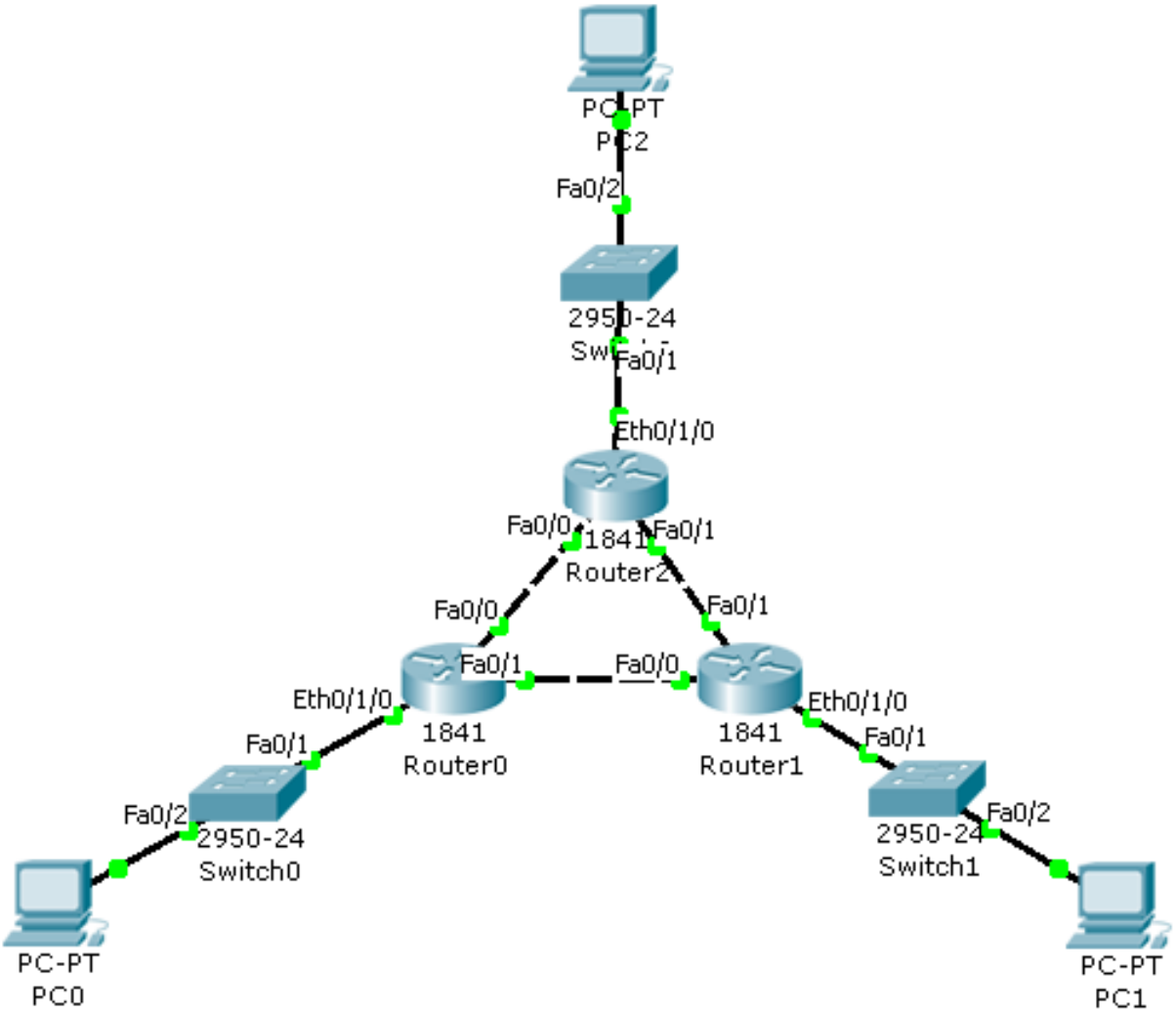


Рисунок 11.2 – Схема локальної мережі складена з трьох маршрутизаторів, трьох комутаторів та трьох комп'ютерів.

9. В маршрутизаторі ***Router0*** увійти у вікно конфігурування пристрою та перейти на вкладку "Конфігурація" (***Config***), щоб увімкнути та налагодити відповідні інтерфейси. Для цього потрібно натиснути на інтерфейс ***FastEthernet0/0***, задати IP адресу, маску підмережі, що вказані в таблиці варіантів та поставити відмітку ***ON*** навпроти рядка ***Port Status***. Аналогічно налаштувати інтерфейс ***FastEthernet0/1*** та ***Ethernet0/1/0***.

10. Провести такі самі налаштунки на маршрутизаторі ***Router1*** та ***Router2***.

11. Зберегти файл один раз з ім'ям ***Lab_11(IGRP)*** і один раз з ім'ям ***Lab_11(OSPF)***. Це робиться для того, щоб не будувати наступний раз мережу для налагодження протоколу.

12. Відкрити файл з ім'ям ***Lab_11(IGRP)***. Для конфігурації протоколу ***IGRP*** необхідно викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** де прописати:

…

Router(config)#router eigrp 200

Примітка: число 200 – це номер автономної системи, тобто сукупність мереж, які в подальшому будуть розумітись одним об'єктом.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Примітка: При введенні інформації раптово може виводитись повідомлення (це повідомлення говорить, що таку мережу знайдено) – не звертайте увагу на це повідомлення і продовжуйте вводити інформацію.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/1 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Router(config-router)#network [*IP-адреса інтерфейсу Ethernet0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Примітка: в форматі ***X.X.X.0*** *– перші три X – це перші три числа IP-адреси інтерфейсу.*

13. Самостійно налаштувати протокол ***IGRP*** на маршрутизаторі ***Router1*** та ***Router2***.

14. Щоб подивитися на результат сконфігурованого протоколу IGRP необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router#show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

Router#show ip route

Аналогічно перевірити інші маршрутизатори, а дані протоколу та таблиці маршрутизації занотувати.

15. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC1*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC2*]

Можна протестувати мережу і іншими способами для більшої впевненості.

16. Зберегти файл та продемонструвати викладачеві.

17. Відкрити файл з ім'ям ***Lab_11(OSPF)***. Для конфігурації протоколу ***OSPF*** необхідно викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** де прописати:

…

Router(config)#router ospf 200

Примітка: число 200 – це номер автономної системи, тобто сукупність мереж, які в подальшому будуть розумітись одним об'єктом.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Примітка: При введенні інформації раптово може виводитись повідомлення (це повідомлення говорить, що таку мережу знайдено) – не звертайте увагу на це повідомлення і продовжуйте вводити інформацію.

Примітка: 0.0.0.255 – перевернута маска (інверсна); area 15 – номер області.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/1 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Router(config-router)#network [*IP-адреса інтерфейсу Ethernet0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Примітка: в форматі ***X.X.X.0*** *– перші три X – це перші три числа IP-адреси інтерфейсу.*

18. Самостійно налаштувати протокол ***OSPF*** на маршрутизаторі ***Router1*** та ***Router2***.

19. Щоб подивитися на результат сконфігурованого протоколу OSPF необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router#show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

Router#show ip route

Аналогічно перевірити інші маршрутизатори, а дані протоколу та таблиці маршрутизації занотувати.

20. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC1*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC2*]

Можна протестувати мережу і іншими способами для більшої впевненості.

21. Зберегти файл та продемонструвати викладачеві.

Таблиця 11.1 Варіанти до практичного завдання 11.

№ варіанту	Router0			Router1		
	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1	IP-адреса та маска інтерфейсу Ehernet0/1/0	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1	IP-адреса та маска інтерфейсу Ehernet0/1/0
1	209.165.1.1 255.255.255.0	209.165.3.1 255.255.255.0	192.168.1.1 255.255.255.0	209.165.1.2 255.255.255.0	209.165.2.1 255.255.255.0	192.168.15.1 255.255.255.0
2	209.164.1.1 255.255.255.0	209.164.3.1 255.255.255.0	192.168.2.1 255.255.255.0	209.164.1.2 255.255.255.0	209.164.2.1 255.255.255.0	192.168.14.1 255.255.255.0
3	209.163.1.1 255.255.255.0	209.163.3.1 255.255.255.0	192.168.3.1 255.255.255.0	209.163.1.2 255.255.255.0	209.163.2.1 255.255.255.0	192.168.13.1 255.255.255.0
4	209.162.1.1 255.255.255.0	209.162.3.1 255.255.255.0	192.168.4.1 255.255.255.0	209.162.1.2 255.255.255.0	209.162.2.1 255.255.255.0	192.168.12.1 255.255.255.0
5	209.161.1.1 255.255.255.0	209.161.3.1 255.255.255.0	192.168.5.1 255.255.255.0	209.161.1.2 255.255.255.0	209.161.2.1 255.255.255.0	192.168.11.1 255.255.255.0
6	209.160.1.1 255.255.255.0	209.160.3.1 255.255.255.0	192.168.6.1 255.255.255.0	209.160.1.2 255.255.255.0	209.160.2.1 255.255.255.0	192.168.10.1 255.255.255.0
7	209.159.1.1 255.255.255.0	209.159.3.1 255.255.255.0	192.168.7.1 255.255.255.0	209.159.1.2 255.255.255.0	209.159.2.1 255.255.255.0	192.168.9.1 255.255.255.0
8	209.158.1.1 255.255.255.0	209.158.3.1 255.255.255.0	192.168.8.1 255.255.255.0	209.158.1.2 255.255.255.0	209.158.2.1 255.255.255.0	192.168.8.1 255.255.255.0
9	209.157.1.1 255.255.255.0	209.157.3.1 255.255.255.0	192.168.9.1 255.255.255.0	209.157.1.2 255.255.255.0	209.157.2.1 255.255.255.0	192.168.7.1 255.255.255.0
10	209.156.1.1 255.255.255.0	209.156.3.1 255.255.255.0	192.168.10.1 255.255.255.0	209.156.1.2 255.255.255.0	209.156.2.1 255.255.255.0	192.168.6.1 255.255.255.0
11	209.155.1.1 255.255.255.0	209.155.3.1 255.255.255.0	192.168.11.1 255.255.255.0	209.155.1.2 255.255.255.0	209.155.2.1 255.255.255.0	192.168.5.1 255.255.255.0
12	209.154.1.1 255.255.255.0	209.154.3.1 255.255.255.0	192.168.12.1 255.255.255.0	209.154.1.2 255.255.255.0	209.154.2.1 255.255.255.0	192.168.4.1 255.255.255.0
13	209.153.1.1 255.255.255.0	209.153.3.1 255.255.255.0	192.168.13.1 255.255.255.0	209.153.1.2 255.255.255.0	209.153.2.1 255.255.255.0	192.168.3.1 255.255.255.0
14	209.152.1.1 255.255.255.0	209.152.3.1 255.255.255.0	192.168.14.1 255.255.255.0	209.152.1.2 255.255.255.0	209.152.2.1 255.255.255.0	192.168.2.1 255.255.255.0
15	209.151.1.1 255.255.255.0	209.151.3.1 255.255.255.0	192.168.15.1 255.255.255.0	209.151.1.2 255.255.255.0	209.151.2.1 255.255.255.0	192.168.1.1 255.255.255.0

Продовження таблиці 11.1 Варіанти до практичного завдання 11.

№ варіанту	Router2			IP-адреса маска та шлюз PC0	IP-адреса маска та шлюз PC1	IP-адреса маска та шлюз PC2
	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1	IP-адреса та маска інтерфейсу Ehernet0/1/0			
1	2	3	4	5	6	7
1	209.165.3.2 255.255.255.0	209.165.2.2 255.255.255.0	192.168.10.1 255.255.255.0	192.168.1.2 255.255.255.0 192.168.1.1	192.168.15.2 255.255.255.0 192.168.15.1	192.168.10.2 255.255.255.0 192.168.10.1
2	209.164.3.2 255.255.255.0	209.164.2.2 255.255.255.0	192.168.20.1 255.255.255.0	192.168.2.2 255.255.255.0 192.168.2.1	192.168.14.2 255.255.255.0 192.168.14.1	192.168.20.2 255.255.255.0 192.168.20.1

1	2	3	4	5	6	7
3	209.163.3.2 255.255.255.0	209.163.2.2 255.255.255.0	192.168.30.1 255.255.255.0	192.168.3.2 255.255.255.0 192.168.3.1	192.168.13.2 255.255.255.0 192.168.13.1	192.168.30.2 255.255.255.0 192.168.30.1
4	209.162.3.2 255.255.255.0	209.162.2.2 255.255.255.0	192.168.40.1 255.255.255.0	192.168.4.2 255.255.255.0 192.168.4.1	192.168.12.2 255.255.255.0 192.168.12.1	192.168.40.2 255.255.255.0 192.168.40.1
5	209.161.3.2 255.255.255.0	209.161.2.2 255.255.255.0	192.168.50.1 255.255.255.0	192.168.5.2 255.255.255.0 192.168.5.1	192.168.11.2 255.255.255.0 192.168.11.1	192.168.50.2 255.255.255.0 192.168.50.1
6	209.160.3.2 255.255.255.0	209.160.2.2 255.255.255.0	192.168.60.1 255.255.255.0	192.168.6.2 255.255.255.0 192.168.6.1	192.168.10.2 255.255.255.0 192.168.10.1	192.168.60.2 255.255.255.0 192.168.60.1
7	209.159.3.2 255.255.255.0	209.159.2.2 255.255.255.0	192.168.70.1 255.255.255.0	192.168.7.2 255.255.255.0 192.168.7.1	192.168.9.2 255.255.255.0 192.168.9.1	192.168.70.2 255.255.255.0 192.168.70.1
8	209.158.3.2 255.255.255.0	209.158.2.2 255.255.255.0	192.168.80.1 255.255.255.0	192.168.8.2 255.255.255.0 192.168.8.1	192.168.8.2 255.255.255.0 192.168.8.1	192.168.80.2 255.255.255.0 192.168.80.1
9	209.157.3.2 255.255.255.0	209.157.2.2 255.255.255.0	192.168.90.1 255.255.255.0	192.168.9.2 255.255.255.0 192.168.9.1	192.168.7.2 255.255.255.0 192.168.7.1	192.168.90.2 255.255.255.0 192.168.90.1
10	209.156.3.2 255.255.255.0	209.156.2.2 255.255.255.0	192.168.100.1 255.255.255.0	192.168.10.2 255.255.255.0 192.168.10.1	192.168.6.2 255.255.255.0 192.168.6.1	192.168.100.2 255.255.255.0 192.168.100.1
11	209.155.3.2 255.255.255.0	209.155.2.2 255.255.255.0	192.168.110.1 255.255.255.0	192.168.11.2 255.255.255.0 192.168.11.1	192.168.5.2 255.255.255.0 192.168.5.1	192.168.110.2 255.255.255.0 192.168.110.1
12	209.154.3.2 255.255.255.0	209.154.2.2 255.255.255.0	192.168.120.1 255.255.255.0	192.168.12.2 255.255.255.0 192.168.12.1	192.168.4.2 255.255.255.0 192.168.4.1	192.168.120.2 255.255.255.0 192.168.120.1
13	209.153.3.2 255.255.255.0	209.153.2.2 255.255.255.0	192.168.130.1 255.255.255.0	192.168.13.2 255.255.255.0 192.168.13.1	192.168.3.2 255.255.255.0 192.168.3.1	192.168.130.2 255.255.255.0 192.168.130.1
14	209.152.3.2 255.255.255.0	209.152.2.2 255.255.255.0	192.168.140.1 255.255.255.0	192.168.14.2 255.255.255.0 192.168.14.1	192.168.2.2 255.255.255.0 192.168.2.1	192.168.140.2 255.255.255.0 192.168.140.1
15	209.151.3.2 255.255.255.0	209.151.2.2 255.255.255.0	192.168.150.1 255.255.255.0	192.168.15.2 255.255.255.0 192.168.15.1	192.168.1.2 255.255.255.0 192.168.1.1	192.168.150.2 255.255.255.0 192.168.150.1

Питання для самоконтролю.

1. Дати характеристику протоколу маршрутизації IGRP.
2. Дати характеристику протоколу маршрутизації OSPF.
3. Як задаються параметри протоколу маршрутизації IGRP?
4. Як задаються параметри протоколу маршрутизації OSPF?

12. Налагодження протоколу маршрутизації PPP

Протокол PPP (Point-to-Point Protocol) розроблений групою IETF (Internet Engineering Task Force), як частина стека TCP/IP для передачі кадрів інформації по послідовних глобальних каналах зв'язку замість застарілого протоколу SLIP (Serial Line IP).

Протокол PPP став фактичним стандартом для глобальних ліній зв'язку при з'єднанні видалених клієнтів з серверами і для утворення з'єднань між маршрутизаторами в корпоративній мережі. При розробці протоколу PPP за основу був узятий формат кадрів HDLC і доповнений власними полями. Поля протоколу PPP вкладені в поле даних кадру HDLC [3, 4].

Пізніше були розроблені стандарти, що використовують вкладення кадру PPP в кадри frame relay і інших протоколів глобальних мереж.

Основна відмінність PPP від інших протоколів канального рівня полягає в тому, що він добивається узгодженої роботи різних пристроїв за допомогою переговорної процедури, під час якої передаються різні параметри, такі як якість лінії, протокол аутентифікації (перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора) і протоколи мережевого рівня, що інкапсулюються (метод побудови модульних мережевих протоколів). Переговорна процедура відбувається під час встановлення з'єднання.

Протокол PPP заснований на чотирьох принципах:

- переговорне ухвалення параметрів з'єднання;
- багатопротокольна підтримка;
- розширюваність протоколу;
- незалежність від глобальних служб.

Переговорне ухвалення параметрів з'єднання. У корпоративній мережі кінцеві системи часто відрізняються розмірами буферів для тимчасового зберігання пакетів, обмеженнями на розмір пакету, списком підтримуваних протоколів мережевого рівня.

Фізична лінія, що зв’язує кінцеві пристрої, може варіюватися від низькошвидкісної аналогової лінії до високошвидкісної цифрової лінії з різними рівнями якості обслуговування [7].

Щоб справитися зі всіма можливими ситуаціями, в протоколі PPP є набір стандартних установок, що діють за замовчанням і що враховують всі стандартні конфігурації. При встановленні з’єднання два пристрої, що взаємодіють між собою, для знаходження взаєморозуміння намагаються спочатку використати ці установки. Кожен кінцевий вузол описує свої можливості і вимоги.

Потім на підставі цієї інформації приймаються параметри поєднання, обидві сторони, порівнюють формати інкапсуляції даних, розміри пакетів, якість лінії і процедуру аутентифікації.

Протокол, відповідно до якого приймаються параметри з’єднання, називається протоколом управління зв’язком (Link Control Protocol, LCP). Протокол, який дозволяє кінцевим вузлам домовитися про те, які мережеві протоколи передаватимуться у встановленому з’єднанні, називається протоколом управління мережевим рівнем (Network Control Protocol, NCP).

Усередині одного PPP-з’єднання можуть передаватися потоки даних різних мережевих протоколів [11].

Практичне завдання 12.

В завданні потрібно створити локальну мережу, в яку будуть входити: три маршрутизатори з інтегрованими службами 1841, три комутатори 2960-24TT, та три комп’ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 12.1, але перш ніж з’єднувати пристрої кабелями, в маршрутизатор потрібно встановити плату ***WIC-2T*** (плата, що має два роз’єми Serial).

2. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

3. На вкладці "Вид фізичного пристрою" (***Physical***) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

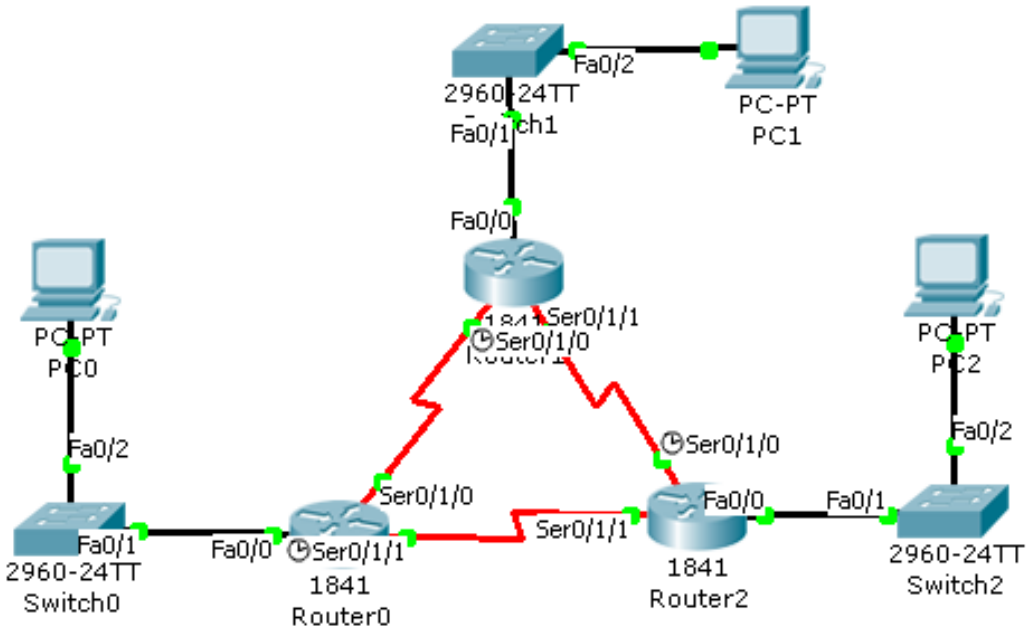


Рисунок 12.1 – Схема локальної мережі складена з трьох маршрутизаторів, трьох комутаторів та трьох комп’ютерів.

4. В лівій частині вікна натиснути на кнопку ***WIC-2T***, після чого внизу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний лівий роз’єм маршрутизатора.

5. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

6. Провести такі самі налаштунки на маршрутизаторі ***Router1*** та ***Router2***.

7. З’єднати всі пристрої між собою кабелями, при цьому обов’язково дотримуйтесь схеми при з’єднанні інтерфейсів. Маршрутизатори з’єднати між собою кабелем ***Serial DTE*** або ***Serial DCE*** (обов’язково зверніть увагу, як розташовані годинники ◷ на кабелі, інакше буде помилка. Годинник показує на якому інтерфейсі повинна вказуватись тактова частота), а всі інші пристрої – кабелем з прямим з’єднанням контактів.

8. Надати кожному комп’ютеру IP-адресу, маску підмережі та шлюз, що вказані у таблиці варіантів.

9. В маршрутизаторі ***Router0*** увійти у вікно конфігурування пристрою та перейти на вкладку "Конфігурація" (***Config***) і у рядку ***Hostname*** (кнопка ***Setting***)

ввести нове мережеве ім’я ***R0***. Далі потрібно увімкнути та налагодити відповідні інтерфейси натиснувши на інтерфейс ***FastEthernet0/0***, задати IP адресу, маску підмережі, що вказані в таблиці варіантів та поставити відмітку ***ON*** навпроти рядка ***Port Status***. Аналогічно налаштувати інтерфейс ***Serial 0/1/0*** та ***Serial 0/1/1*** але в цих інтерфейсах потрібно також встановити тактову частоту в рядку ***Clock Rate***, що вказана у варіанті (частота ставиться на тих інтерфейсах, на яких у схемі стоїть годинник).

10. Провести такі самі налаштунки на маршрутизаторі ***Router1*** та ***Router2***. (Примітка: мережеве ім’я для маршрутизатора Router1 – R1, а для маршрутизатора Router2 – R2, всі останні дані – згідно варіанту).

11. Після того, як всі дані були введені потрібно налаштувати протокол ***PPP***. Для конфігурації протоколу ***PPP*** необхідно викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** де прописати:

Примітка: буде прописано два з’єднання, спочатку маршрутизатора Router0 з маршрутизатором Router1.

…

R0(config)#username R1 password 123

Примітка: вказується ім’я вузла від якого очікується з’єднання та пароль, що повинен бути ідентичним на з’єднаних пристроях.

R0(config)#interface serial 0/1/0

Примітка: вказується інтерфейс маршрутизатора Router0 з яким з’єднується Router1.

R0(config-if)#encapsulation ppp

Примітка: інкапсуляція.

R0(config-if)#ppp authentication chap

Примітка: аутентифікація.

R0(config-if)#exit

Примітка: з’єднання маршрутизатора Router0 з маршрутизатором Router2.

R0(config)#username R2 password 123

R0(config)#interface serial 0/1/1

Примітка: вказується інтерфейс маршрутизатора Router0 з яким з'єднується Router2.

R0(config-if)#encapsulation ppp

R0(config-if)#ppp authentication chap

12. Самостійно прописати конфігурацію для маршрутизатора ***Router1*** та ***Router2***. При конфігуруванні цих маршрутизаторів можуть раптово виводитись повідомлення – це означає, що такий маршрут знайдений і відбулося з'єднання.

13. Щоб подивитися на результат конфігурування необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

R0#show running-config

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

R0#show ip route

Аналогічно перевірити інші маршрутизатори, а дані інтерфейсів та таблиці маршрутизації занотувати.

14. Щоб створити зв'язок між комп'ютерами потрібно використати один з протоколів, наприклад ***RIP***.

15. Викликати вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку "Конфігурація" (***Config***). В лівій панелі вікна натиснути на кнопку RIP, і навпроти рядка ***Network*** ввести IP-адресу інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі ***X.X.X.0*** та натиснути кнопку ***Add***. Після цього знову навпроти рядка ***Network*** ввести IP-адресу інтерфейсу Serial 0/1/0 маршрутизатора Router0 в форматі ***X.X.X.0*** та натиснути кнопку ***Add***. І останню IP-адресу маршрутизатора Router0 інтерфейсу Serial 0/1/1 ввести навпроти рядка ***Network*** в форматі ***X.X.X.0*** та натиснути кнопку ***Add***.

16. Аналогічно сконфігурувати протокол для маршрутизатора ***Router1*** та ***Router2***.

17. Щоб подивитися на результат сконфігурованого протоколу RIP необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

R0#show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

R0#show ip route

Аналогічно перевірити інші маршрутизатори, а дані протоколу та таблиці маршрутизації занотувати.

18. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC2*]

PC>ping [*IP-адреса комп'ютера PC1*]

19. Протестувати мережу в режимі моделювання ***Simulation Mode*** та подивитися, як відбувається обмін пакетами за допомогою ***ping-запиту***.

20. Зберегти файл та продемонструвати викладачеві.

Таблиця 12.1 Варіанти до практичного завдання 12.

№ варіанту	Router0				Router1			
	IP-адреса та маска інтерфейсу Serial 0/1/0	IP-адреса та маска інтерфейсу Serial 0/1/1	IP-адреса та маска інтерфейсу FastEhernet0/0	Тактова частота Clock Rate на інтерфейсі Serial 0/1/1	IP-адреса та маска інтерфейсу Serial 0/1/0	IP-адреса та маска інтерфейсу Serial 0/1/1	IP-адреса та маска інтерфейсу FastEhernet0/0	Тактова частота Clock Rate на інтерфейсі Serial 0/1/0
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	209.165.1.1 255.255.255.0	209.165.3.2 255.255.255.0	192.168.1.1 255.255.255.0	4000000	209.165.1.2 255.255.255.0	209.165.2.1 255.255.255.0	192.168.15.1 255.255.255.0	148000
2	209.164.1.1 255.255.255.0	209.164.3.2 255.255.255.0	192.168.2.1 255.255.255.0	2000000	209.164.1.2 255.255.255.0	209.164.2.1 255.255.255.0	192.168.14.1 255.255.255.0	128000
3	209.163.1.1 255.255.255.0	209.163.3.2 255.255.255.0	192.168.3.1 255.255.255.0	1300000	209.163.1.2 255.255.255.0	209.163.2.1 255.255.255.0	192.168.13.1 255.255.255.0	125000
4	209.162.1.1 255.255.255.0	209.162.3.2 255.255.255.0	192.168.4.1 255.255.255.0	1000000	209.162.1.2 255.255.255.0	209.162.2.1 255.255.255.0	192.168.12.1 255.255.255.0	72000

1	2	3	4	5	6	7	8	9
5	209.161.1.1 255.255.255.0	209.161.3.2 255.255.255.0	192.168.5.1 255.255.255.0	800000	209.161.1.2 255.255.255.0	209.161.2.1 255.255.255.0	192.168.11.1 255.255.255.0	64000
6	209.160.1.1 255.255.255.0	209.160.3.2 255.255.255.0	192.168.6.1 255.255.255.0	500000	209.160.1.2 255.255.255.0	209.160.2.1 255.255.255.0	192.168.10.1 255.255.255.0	56000
7	209.159.1.1 255.255.255.0	209.159.3.2 255.255.255.0	192.168.7.1 255.255.255.0	250000	209.159.1.2 255.255.255.0	209.159.2.1 255.255.255.0	192.168.9.1 255.255.255.0	38400
8	209.158.1.1 255.255.255.0	209.158.3.2 255.255.255.0	192.168.8.1 255.255.255.0	148000	209.158.1.2 255.255.255.0	209.158.2.1 255.255.255.0	192.168.8.1 255.255.255.0	19200
9	209.157.1.1 255.255.255.0	209.157.3.2 255.255.255.0	192.168.9.1 255.255.255.0	128000	209.157.1.2 255.255.255.0	209.157.2.1 255.255.255.0	192.168.7.1 255.255.255.0	9600
10	209.156.1.1 255.255.255.0	209.156.3.2 255.255.255.0	192.168.10.1 255.255.255.0	125000	209.156.1.2 255.255.255.0	209.156.2.1 255.255.255.0	192.168.6.1 255.255.255.0	4800
11	209.155.1.1 255.255.255.0	209.155.3.2 255.255.255.0	192.168.11.1 255.255.255.0	72000	209.155.1.2 255.255.255.0	209.155.2.1 255.255.255.0	192.168.5.1 255.255.255.0	2400
12	209.154.1.1 255.255.255.0	209.154.3.2 255.255.255.0	192.168.12.1 255.255.255.0	64000	209.154.1.2 255.255.255.0	209.154.2.1 255.255.255.0	192.168.4.1 255.255.255.0	1200
13	209.153.1.1 255.255.255.0	209.153.3.2 255.255.255.0	192.168.13.1 255.255.255.0	56000	209.153.1.2 255.255.255.0	209.153.2.1 255.255.255.0	192.168.3.1 255.255.255.0	2400
14	209.152.1.1 255.255.255.0	209.152.3.2 255.255.255.0	192.168.14.1 255.255.255.0	38400	209.152.1.2 255.255.255.0	209.152.2.1 255.255.255.0	192.168.2.1 255.255.255.0	4800
15	209.151.1.1 255.255.255.0	209.151.3.2 255.255.255.0	192.168.15.1 255.255.255.0	19200	209.151.1.2 255.255.255.0	209.151.2.1 255.255.255.0	192.168.1.1 255.255.255.0	9600

Продовження таблиці 12.1 Варіанти до практичного завдання 12.

№ варіанту	Router2				IP-адреса маска та шлюз PC0	IP-адреса маска та шлюз PC1	IP-адреса маска та шлюз PC2
	IP-адреса та маска інтерфейсу Serial 0/1/0	IP-адреса та маска інтерфейсу Serial 0/1/1	IP-адреса та маска інтерфейсу FastEhernet 0/0	Тактова частота Clock Rate на інтерфейсі Serial 0/1/0			
1	2	3	4	5	6	7	9
1	209.165.2.2 255.255.255.0	209.165.3.2 255.255.255.0	192.168.10.1 255.255.255.0	19200	192.168.1.2 255.255.255.0 192.168.1.1	192.168.15.2 255.255.255.0 192.168.15.1	192.168.10.2 255.255.255.0 192.168.10.1
2	209.164.2.2 255.255.255.0	209.164.3.1 255.255.255.0	192.168.20.1 255.255.255.0	38400	192.168.2.2 255.255.255.0 192.168.2.1	192.168.14.2 255.255.255.0 192.168.14.1	192.168.20.2 255.255.255.0 192.168.20.1
3	209.163.2.2 255.255.255.0	209.163.3.1 255.255.255.0	192.168.30.1 255.255.255.0	56000	192.168.3.2 255.255.255.0 192.168.3.1	192.168.13.2 255.255.255.0 192.168.13.1	192.168.30.2 255.255.255.0 192.168.30.1
4	209.162.2.2 255.255.255.0	209.162.3.1 255.255.255.0	192.168.40.1 255.255.255.0	64000	192.168.4.2 255.255.255.0 192.168.4.1	192.168.12.2 255.255.255.0 192.168.12.1	192.168.40.2 255.255.255.0 192.168.40.1
5	209.161.2.2 255.255.255.0	209.161.3.1 255.255.255.0	192.168.50.1 255.255.255.0	72000	192.168.5.2 255.255.255.0 192.168.5.1	192.168.11.2 255.255.255.0 192.168.11.1	192.168.50.2 255.255.255.0 192.168.50.1
6	209.160.2.2 255.255.255.0	209.160.3.1 255.255.255.0	192.168.60.1 255.255.255.0	125000	192.168.6.2 255.255.255.0 192.168.6.1	192.168.10.2 255.255.255.0 192.168.10.1	192.168.60.2 255.255.255.0 192.168.60.1
7	209.159.2.2 255.255.255.0	209.159.3.1 255.255.255.0	192.168.70.1 255.255.255.0	128000	192.168.7.2 255.255.255.0 192.168.7.1	192.168.9.2 255.255.255.0 192.168.9.1	192.168.70.2 255.255.255.0 192.168.70.1
8	209.158.2.2 255.255.255.0	209.158.3.1 255.255.255.0	192.168.80.1 255.255.255.0	148000	192.168.8.2 255.255.255.0 192.168.8.1	192.168.8.2 255.255.255.0 192.168.8.1	192.168.80.2 255.255.255.0 192.168.80.1

1	2	3	4	5	6	7	9
9	209.157.2.2 255.255.255.0	209.157.3.1 255.255.255.0	192.168.90.1 255.255.255.0	250000	192.168.9.2 255.255.255.0 192.168.9.1	192.168.7.2 255.255.255.0 192.168.7.1	192.168.90.2 255.255.255.0 192.168.90.1
10	209.156.2.2 255.255.255.0	209.156.3.1 255.255.255.0	192.168.100.1 255.255.255.0	500000	192.168.10.2 255.255.255.0 192.168.10.1	192.168.6.2 255.255.255.0 192.168.6.1	192.168.100.2 255.255.255.0 192.168.100.1
11	209.155.2.2 255.255.255.0	209.155.3.1 255.255.255.0	192.168.110.1 255.255.255.0	800000	192.168.11.2 255.255.255.0 192.168.11.1	192.168.5.2 255.255.255.0 192.168.5.1	192.168.110.2 255.255.255.0 192.168.110.1
12	209.154.2.2 255.255.255.0	209.154.3.1 255.255.255.0	192.168.120.1 255.255.255.0	1000000	192.168.12.2 255.255.255.0 192.168.12.1	192.168.4.2 255.255.255.0 192.168.4.1	192.168.120.2 255.255.255.0 192.168.120.1
13	209.153.2.2 255.255.255.0	209.153.3.1 255.255.255.0	192.168.130.1 255.255.255.0	1300000	192.168.13.2 255.255.255.0 192.168.13.1	192.168.3.2 255.255.255.0 192.168.3.1	192.168.130.2 255.255.255.0 192.168.130.1
14	209.152.2.2 255.255.255.0	209.152.3.1 255.255.255.0	192.168.140.1 255.255.255.0	2000000	192.168.14.2 255.255.255.0 192.168.14.1	192.168.2.2 255.255.255.0 192.168.2.1	192.168.140.2 255.255.255.0 192.168.140.1
15	209.151.2.2 255.255.255.0	209.151.3.1 255.255.255.0	192.168.150.1 255.255.255.0	4000000	192.168.15.2 255.255.255.0 192.168.15.1	192.168.1.2 255.255.255.0 192.168.1.1	192.168.150.2 255.255.255.0 192.168.150.1

Питання для самоконтролю.

1. Для чого був розроблений протокол PPP?
2. На яких принципах заснований протокол PPP?
3. Який протокол називається управлінням мережевим рівнем?

13. Технологія бездротового зв’язку Wi-Fi

Технологія Wi-Fi – це безпровідний аналог стандарту Ethernet, на основі якого сьогодні побудована велика частина офісних комп’ютерних мереж. Він був зареєстрований в 1999 році і став справжнім відкриттям для менеджерів, торгових агентів, співробітників складів, основним робочим інструментом яких є ноутбук або інший мобільний комп’ютер [6, 7].

Wi-Fi – скорочення від англійського Wireless Fidelity, що означає стандарт бездротового (радіо) зв’язку, який об’єднує декілька протоколів та має офіційне найменування IEEE 802.11 (від Institute of Electrical and Electronic Engineers – міжнародної організації, що займається розробкою стандартів у галузі

електронних технологій). Найбільш відомим та поширеним на сьогоднішній день є протокол IEEE 802.11b (зазвичай під скороченням Wi-Fi мають на увазі саме його), що визначає функціонування бездротових мереж, в яких для передачі даних використовується діапазон частот від 2,4 до 2.4835 гігагерца і забезпечується максимальна швидкість 11 Мбіт/сек. Максимальна дальність передачі сигналу у такій мережі складає 100 метрів, однак на відкритій місцевості вона може досягати й більших значень (до 300-400 м).

Крім 802.11b існують ще бездротовий стандарт 802.11a, який використовує частоту 5 Ггц та забезпечує максимальну швидкість 54 Мбіт/с, а також 802.11g, що працює на частоті 2,4 Ггц і теж забезпечує 54 Мбіт/с. Однак, через меншу дальність, значно більшу обчислювальну складність алгоритмів і високе енергоспоживання ці технології поки не набули великого поширення. Крім того, в даний час ведеться розробка стандарту 802.11n, який у найближчому майбутньому зможе забезпечити швидкість до 320 Мбіт/с [3].

Подібно традиційним провідним технологіям, Wi-Fi забезпечує доступ до серверів, що зберігають бази даних або програмні додатки, дозволяє вийти в Інтернет, роздруковувати файли і т. д. Але при цьому комп'ютер, з якого зчитується інформація, не потрібно підключати до комп'ютерної розетки. Досить розмістити його в радіусі 300 м від так званої точки доступу (access point) – Wi-Fi-пристрою (рис. 13.1), що виконує приблизно ті ж функції, що звичайна офісна АТС. У цьому випадку інформація буде передаватися за допомогою радіохвиль в частотному діапазоні 2,4-2,483 ГГц [5].

Таким чином, Wi-Fi-технологія дозволяє вирішити три важливих завдання:

- спростити спілкування з мобільним комп'ютером;
- забезпечити комфортні умови для роботи діловим партнерам, які прийшли в офіс зі своїм ноутбуком;
- створити локальну мережу в приміщеннях, де прокладка кабелю неможлива або надмірно дорога.

Бездротова технологія може стати, як основою IT-системи компанії, так і доповненням до вже існуючої кабельної мережі.

Рисунок 13.1 – Бездротова точка доступу Wi-Fi.

Ядром бездротової мережі Wi-Fi є так звана точка доступу (Access Point), яка підключається до якоїсь наземної мережевої інфраструктури (наприклад, офісної Ethernet-мережі) та забезпечує передачу радіосигналу. Зазвичай, точка доступу складається із приймача, передавача, інтерфейсу для підключення до дротової мережі та програмного забезпечення для обробки даних. Після підключення навколо точки доступу формується територія радіусом 50-100 метрів (її називають хот-спотом або зоною Wi-Fi), на якій можна користуватися бездротовою мережею [4].

Для того щоб підключитися до точки доступу та відчути всі переваги бездротової мережі, власнику ноутбуку або іншого мобільного пристрою, оснащеного Wi-Fi адаптером, необхідно просто потрапити в радіус її дії. Усі дії із визначення пристрою та налаштування мережі більшість ОС проводять автоматично. Якщо користувач потрапляє одночасно в кілька Wi-Fi зон, то відбувається підключення до точки доступу, що забезпечує найпотужніший сигнал. Час від часу проводиться перевірка наявності інших точок доступу, і в

разі, якщо сигнал від нової точки сильніший, пристрій перепідключається до неї, налаштовуючись абсолютно прозоро і непомітно для власника.

Одним з головних достоїнств будь-якої Wi-Fi мережі є можливість доступу до Інтернету для всіх її користувачів, яка забезпечується або прямим підключенням точки доступу до інтернет-каналу, або підключенням до неї будь-якого сервера, під'єднаного до Інтернет. В обох випадках мобільному користувачеві не потрібно нічого самостійно настроювати – досить запустити браузер і набрати адресу будь-якого інтернет-сайту.

Також декілька пристроїв з підтримкою Wi-Fi можуть з'єднуватися один з одним безпосередньо (зв'язок пристрій-пристрій), тобто без використання спеціальної точки доступу, утворюючи щось на кшталт локальної мережі, в якій можна обмінюватися файлами, але в цьому випадку обмежується число видимих станцій [9].

У випадку з пристроями без вбудованої підтримки технології Wi-Fi (наприклад, із звичайними домашніми або офісними комп'ютерами) потрібно буде придбати спеціальну карту, що підтримує цей стандарт (рис. 13.2).

Рисунок 13.2 – Бездротова точка доступу Wi-Fi.

Багато експертів вважають, що революція Wi-Fi почалася з ініціативи звичайних приватних користувачів. Людям сподобалося ділитися підключенням до мережі за допомогою нової бездротової технології. Для позначення безкоштовних Wi-Fi точок була розроблена система умовних знаків, які

наносилися крейдою на стіни будинків, біля яких можна було вийти в Інтернет. Спочатку ці дії викликали негативну реакцію мобільних і інтернет-операторів, але незабаром Wi-Fi провайдери стали мирно уживатися з приватними мережами.

Практичне завдання 13.

В завданні потрібно створити локальну мережу, в яку будуть входити: два маршрутизатори з інтегрованими службами 1841, комутатор 2960-24TT, дві точки доступу Access Point-PT, два сервера Server-PT та шість комп'ютерів PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 13.3, але перш ніж з'єднувати пристрої кабелями, в маршрутизатор потрібно встановити плату ***WIC-1T*** (плата, що має один роз'єм Serial).

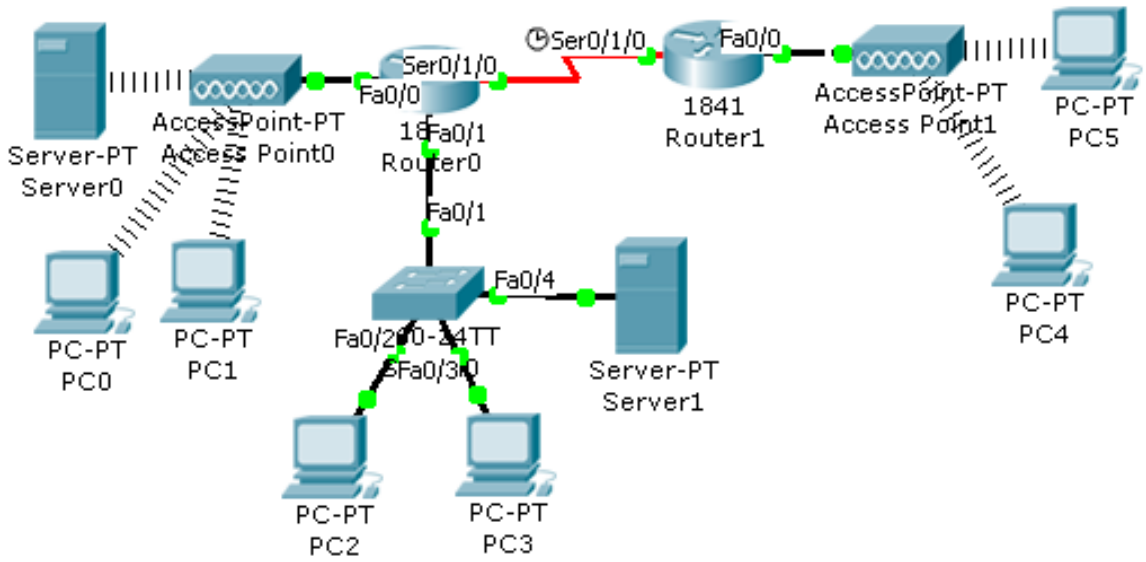


Рисунок 13.3 – Схема локальної мережі для завдання 13.

2. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

3. На вкладці "Вид фізичного пристрою" (***Physical***) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

4. В лівій частині вікна натиснути на кнопку ***WIC-1T***, після чого внизу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний лівий роз'єм маршрутизатора.

5. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

6. Провести такі самі налаштунки на маршрутизаторі ***Router1***.

7. Клацнути ЛК миші на комп'ютер ***PC0***, щоб викликати вікно конфігурації.

8. На вкладці "Вид фізичного пристрою" (***Physical***) клацнути на червону кнопку – живлення зникне и зелений індикатор погасне.

9. Опуститись в кінець вікна де знаходяться роз'єми комп'ютера. Перетягнути з комп'ютера роз'єм ***PT-HOST-NM-CFE*** на місце знаходження плат. Тепер у вільний слот помістити плату ***PT-HOST-NM-1W*** (плата Wi-Fi) та натиснути на кнопку живлення (червона кнопка) – з'явиться живлення і засвітиться зелений індикатор. Після закриття вікна конфігурацій на схемі утвориться бездротовий зв'язок (на схемі показано лінією зі штрихів).

Примітка: Не звертати увагу, якщо комп'ютер буде з'єднаний не з тією точкою доступу, що потрібно, далі буде описано налагодження.

10. Повторити аналогічні дії для комп'ютерів ***PC1***, ***PC4***, ***PC5*** та для сервера ***Server0***.

11. Клацнути ЛК миші на точку доступу ***Access Point0***, щоб ввійти у вікно конфігурації. Перейти на вкладку ***Config***, та натиснути в лівій частині вікна на кнопку ***Port 1***. Далі поставити відмітку навпроти рядка ***WEB*** та ввести пароль в рядку ***Key***: ***1234567890***.

12. Відкрити вікно конфігурації комп'ютера ***PC0***, перейти на вкладку ***Config***, та натиснути в лівій частині вікна на кнопку ***Wireless***. Далі поставити відмітку навпроти рядка ***WEB*** та ввести пароль в рядку ***Key***: ***1234567890***. Аналогічно налаштувати комп'ютер ***PC1*** та сервер ***Server0***.

13. Провести налагодження точки доступу ***Access Point1*** та комп'ютерів ***PC4***, ***PC5*** самостійно, використовуючи при цьому пароль: ***0987654321***. Після цих налагоджень бездротовий зв'язок повинен бути таким, як показано на схемі.

14. З'єднати всі пристрої між собою кабелями, при цьому обов'язково дотримуйтесь схеми при з'єднанні інтерфейсів. Маршрутизатори з'єднати між

собою кабелем ***Serial DTE*** або ***Serial DCE*** (обов'язково зверніть увагу, як розташований годинник ◷ на кабелі, інакше буде помилка. Годинник показує на якому інтерфейсі повинна вказуватись тактова частота) з розділу ***Connections***, точки доступу з маршрутизаторами з'єднати кабелем з перехресним з'єднанням контактів (***Copper Cross–Over***), а всі інші пристрої – кабелем з прямим з'єднанням контактів (***Copper Straight–Through***).

15. Зайти у вікно конфігурації ***Server0*** та перейти на вкладку ***Config***. В лівій частині вікна натиснути на кнопку ***DHCP*** та в рядку ***Default Gateway*** ввести шлюз. Далі перейти на вкладку робочого столу (***Desktop***) та клацнути на піктограму ***IP Configuration***, після чого знову задати шлюз, IP-адресу та маску підмережі. Закрити вікно конфігурацій та повторити аналогічні дії для сервера ***Server1***.

16. Клацнути ЛК миші по маршрутизатору ***Router0***, щоб зайти у вікно конфігурацій та перейти на вкладку ***Config***. Активувати та надати інтерфейсам ***FastEhernet 0/0***, ***FastEhernet 0/1*** та ***Serial 0/1/0*** відповідні IP-адреси і маски підмережі, що вказані в таблиці варіантів.

17. Відкрити вікно конфігурації маршрутизатора ***Router1*** та перейти на вкладку ***Config***, щоб активізувати і задати інтерфейсам ***FastEhernet 0/0*** та ***Serial 0/1/0*** IP-адресу, маску підмережі і тактову частоту (для інтерфейсу ***Serial 0/1/0***). Далі перейти на вкладку ***CLI*** та сконфігурувати послугу ***DHCP***, як це робилось в попередніх завданнях:

…

Router(config)#ip dhcp pool pool1

Router(dhcp-config)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router1 в форматі* ***X.X.X.0*** *що вказано у варіанті*] [маска підмережі]

<u>Примітка</u>: створення діапазону мережевих адрес для пулу DHCP.

Router(dhcp-config)#dns-server [*інтерфейсу FastEthernet0/0 маршрутизатора Router1 в форматі* ***X.X.X.50*** *що вказано у варіанті*]

Router(dhcp-config)#default-route [*інтерфейсу FastEthernet0/0 маршрутизатора Router1 в форматі* ***X.X.X.1*** *що вказано у варіанті*]

Router(dhcp-config)#exit

18. Відкрити вікно конфігурації комп'ютера ***PC4*** та перейти на кладку на вкладку робочого столу (***Desktop***), клацнути на піктограму ***IP Configuration*** та поставити відмітку навпроти рядка ***DHCP***. В результаті автоматично повинно буде вписано IP-адресу, маску підмережі та шлюз.

19. Аналогічно налаштувати послугу ***DHCP*** на всіх інших комп'ютерах.

20. Для того щоб мережі обмінювались пакетами даних потрібно прописати протокол, наприклад протокол ***IGRP***.

21. Відкрити вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** щоб сконфігурувати протокол:

…

Router(config)#router eigrp 200

Примітка: число 200 – це номер автономної системи, тобто сукупність мереж, які в подальшому будуть розумітись одним об'єктом.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/1 маршрутизатора Router0 в форматі* ***X.X.X.0***]

Router(config-router)#network [*IP-адреса інтерфейсу Serial0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***]

22. Аналогічно налагодити протокол на маршрутизаторі ***Router1***:

…

Router(config)#router eigrp 200

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router1 в форматі* ***X.X.X.0***]

Router(config-router)#network [*IP-адреса інтерфейсу Serial0/1/0 маршрутизатора Router1 в форматі* ***X.X.X.0***]

23. Щоб подивитися на результат сконфігурованого протоколу ***IGRP*** необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router #show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

Router #show ip route

Аналогічно перевірити інший маршрутизатор, а дані протоколу та таблиці маршрутизації занотувати.

24. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC2*]

PC>ping [*IP-адреса комп'ютера PC4*]

Для більшої впевненості роботи мережі надіслати з інших комп'ютерів ***ping***-запити.

25. Зберегти файл та продемонструвати викладачеві.

Таблиця 13.1 Варіанти до практичного завдання 13.

№ варіанту	Router0			Router1		IP-адреса, маска та шлюз сервера Server0	IP-адреса, маска та шлюз сервера Server1
	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса та маска інтерфейсу FastEhernet0/1	IP-адреса та маска інтерфейсу Serial 0/1/0	IP-адреса та маска інтерфейсу FastEhernet0/0	IP-адреса, маска та тактова частота інтерфейсу Serial 0/1/0		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	192.168.1.1 255.255.255.0	192.168.10.1 255.255.255.0	209.165.1.1 255.255.255.0	192.168.15.1 255.255.255.0	209.165.1.2 255.255.255.0 4000000	192.168.1.3 255.255.255.0 192.168.1.1	192.168.10.100 255.255.255.0 192.168.15.1
2	192.168.2.1 255.255.255.0	192.168.20.1 255.255.255.0	209.164.1.1 255.255.255.0	192.168.14.1 255.255.255.0	209.164.1.2 255.255.255.0 2000000	192.168.2.3 255.255.255.0 192.168.2.1	192.168.20.100 255.255.255.0 192.168.14.1
3	192.168.3.1 255.255.255.0	192.168.30.1 255.255.255.0	209.163.1.1 255.255.255.0	192.168.13.1 255.255.255.0	209.163.1.2 255.255.255.0 1300000	192.168.3.3 255.255.255.0 192.168.3.1	192.168.30.100 255.255.255.0 192.168.13.1
4	192.168.4.1 255.255.255.0	192.168.40.1 255.255.255.0	209.162.1.1 255.255.255.0	192.168.12.1 255.255.255.0	209.162.1.2 255.255.255.0 1000000	192.168.4.3 255.255.255.0 192.168.4.1	192.168.40.100 255.255.255.0 192.168.12.1
5	192.168.5.1 255.255.255.0	192.168.50.2 255.255.255.0	209.161.1.1 255.255.255.0	192.168.11.1 255.255.255.0	209.161.1.2 255.255.255.0 800000	192.168.5.3 255.255.255.0 192.168.5.1	192.168.50.100 255.255.255.0 192.168.11.1

1	2	3	4	5	6	7	8
6	192.168.6.1 255.255.255.0	192.168.60.1 255.255.255.0	209.160.1.1 255.255.255.0	192.168.10.1 255.255.255.0	209.160.1.2 255.255.255.0 500000	192.168.6.3 255.255.255.0 192.168.6.1	192.168.60.100 255.255.255.0 192.168.10.1
7	192.168.7.1 255.255.255.0	192.168.70.1 255.255.255.0	209.159.1.1 255.255.255.0	192.168.9.1 255.255.255.0	209.159.1.2 255.255.255.0 250000	192.168.7.3 255.255.255.0 192.168.7.1	192.168.70.100 255.255.255.0 192.168.9.1
8	192.168.8.1 255.255.255.0	192.168.80.1 255.255.255.0	209.158.1.1 255.255.255.0	192.168.8.1 255.255.255.0	209.158.1.2 255.255.255.0 148000	192.168.8.3 255.255.255.0 192.168.8.1	192.168.80.100 255.255.255.0 192.168.8.1
9	192.168.9.1 255.255.255.0	192.168.90.1 255.255.255.0	209.157.1.1 255.255.255.0	192.168.7.1 255.255.255.0	209.157.1.2 255.255.255.0 128000	192.168.9.3 255.255.255.0 192.168.9.1	192.168.90.100 255.255.255.0 192.168.7.1
10	192.168.10.1 255.255.255.0	192.168.100.1 255.255.255.0	209.156.1.1 255.255.255.0	192.168.6.1 255.255.255.0	209.156.1.2 255.255.255.0 125000	192.168.10.3 255.255.255.0 192.168.10.1	192.168.100.10 0 255.255.255.0 192.168.6.1
11	192.168.11.1 255.255.255.0	192.168.110.1 255.255.255.0	209.155.1.1 255.255.255.0	192.168.5.1 255.255.255.0	209.155.1.2 255.255.255.0 72000	192.168.11.3 255.255.255.0 192.168.11.1	192.168.110.10 0 255.255.255.0 192.168.5.1
12	192.168.12.1 255.255.255.0	192.168.120.1 255.255.255.0	209.154.1.1 255.255.255.0	192.168.4.1 255.255.255.0	209.154.1.2 255.255.255.0 64000	192.168.12.3 255.255.255.0 192.168.12.1	192.168.120.10 0 255.255.255.0 192.168.4.1
13	192.168.13.1 255.255.255.0	192.168.130.2 255.255.255.0	209.153.1.1 255.255.255.0	192.168.3.1 255.255.255.0	209.153.1.2 255.255.255.0 56000	192.168.13.3 255.255.255.0 192.168.13.1	192.168.130.10 0 255.255.255.0 192.168.3.1
14	192.168.14.1 255.255.255.0	192.168.140.1 255.255.255.0	209.152.1.1 255.255.255.0	192.168.2.1 255.255.255.0	209.152.1.2 255.255.255.0 38400	192.168.14.3 255.255.255.0 192.168.14.1	192.168.140.10 0 255.255.255.0 192.168.2.1
15	192.168.15.1 255.255.255.0	192.168.150.1 255.255.255.0	209.151.1.1 255.255.255.0	192.168.1.1 255.255.255.0	209.151.1.2 255.255.255.0 19200	192.168.15.3 255.255.255.0 192.168.15.1	192.168.150.10 0 255.255.255.0 192.168.1.1

Питання для самоконтролю.

1. Для чого застосовується технологія Wi-Fi?

2. На якій відстані забезпечується зв’язок Wi-Fi?

3. Для чого потрібна точка доступу?

4. Який протокол маршрутизації використовувався при виконанні завдання?

5. Скільки підмереж було створено?

14. Інтернет та Web-запити

DNS-сервер забезпечує трансляцію імен сайтів в IP-адреси. Дуже абстрактно можна сказати, що кожен комп'ютер в Інтернеті має два основних ідентифікатора – це доменне ім'я (наприклад, www.imena.ua) і IP-адресу (наприклад, 127.0.0.1). А ось абстрактність полягає в тому, що у IP-адрес і у комп'ютера може бути кілька (більше того, у кожного інтерфейсу може бути своя адреса, до того ж ще й кілька адрес можуть належати одному інтерфейсі), та імен теж може бути декілька. Причому вони можуть зв'язуватися, як з одним, так і з декількома IP-адресами. А по-третє, у комп'ютера може взагалі й не бути доменного імені [10].

Основним завданням DNS-сервера є трансляція доменних імен в IP адреси і навпаки. На зорі зародження Інтернету, коли він ще був ARPANETом, це вирішувалося веденням довгих списків усіх комп'ютерних мереж. При цьому копія такого списку повинна була знаходитися на кожному комп'ютері. Природно, що із зростанням мережі така технологія вже стала не зручною для користувачів, тому що ці файли були великих розмірів, до того ж їх ще й потрібно було синхронізувати. До речі, деякі такі "відлуння минулого" цього методу можна ще зустріти і зараз. Ось так в файл HOSTS (UNIX, Windows) можна внести адреси серверів, з якими користувач регулярно працюєте.

Так на зміну незручній "однофайловій" системі і прийшов DNS – ієрархічна структура імен, придумана доктором Полом Мокапетріс.

Отже, є "корінь дерева" – "." (Крапка). Враховуючи те, що цей корінь єдиний для всіх доменів, то точка в кінці імені зазвичай не ставиться. Але вона використовується в описах DNS і це треба запам'ятати. Нижче цього "кореня" знаходяться домени першого рівня. Їх небагато – com, net, edu, org, mil, int, biz, info, gov та ін., і домени держав, наприклад, ua. Ще нижче знаходяться домени другого рівня, а ще нижче – третього і т.д [11].

DNS-сервера можуть бути рекурсивні і нерекурсивні. Різниця в них у тому, що рекурсивні завжди повертають клієнтові відповідь, оскільки самостійно

відстежують відсилання до інших DNS-серверів і опитують їх, а нерекурсивні – повертають клієнтові ці відсилання, і клієнт повинен самостійно опитувати вказаний сервер.

Рекурсивні сервера зазвичай використовують на низьких рівнях, наприклад, в локальних мережах, так як вони кешують всі проміжні відповіді, і так при подальших до нього запитах, відповіді будуть повертатися швидше. А нерекурсивні сервера часто стоять на верхніх щаблях ієрархії, оскільки вони отримують так багато запитів, що для кешування відповідей попросту не вистачить ніяких ресурсів.

Інтернет – міжмережжя, система об'єднаних комп'ютерних мереж глобального загальнолюдського суспільства, яка в наш час покриває практично всю поверхню земної кулі.

Мережа побудована на використанні протоколу IP і маршрутизації пакетів даних. В наш час Інтернет відіграє важливе значення у створенні інформаційного простору глобального суспільства, слугує фізичною основою доступу до веб-сайтів і багатьох систем (протоколів) передачі даних.

Сьогодні при вживанні слова "Інтернет" найчастіше мається на увазі саме веб і доступна через нього інформація, а не сама фізична адреса, що призводить до різноманітних юридичних колізій та правових наслідків.

Практичне завдання 14.

В завданні потрібно створити локальну мережу, в яку будуть входити: два маршрутизатори з інтегрованими службами 1841, три комутатори 2960-24TT, одна точки доступу Access Point-PT, чотири сервера Server-PT та чотири комп'ютера PC–PT.

1. В середовищі Packet Tracer побудувати мережу, що показана на рис. 14.1, але перш ніж з'єднувати пристрої кабелями, в маршрутизатор потрібно встановити плату ***WIC-1T*** (плата, що має один роз'єм Serial).

2. Шляхом натиснення ЛК миші на маршрутизатор ***Router0***, викликати вікно конфігурації пристрою.

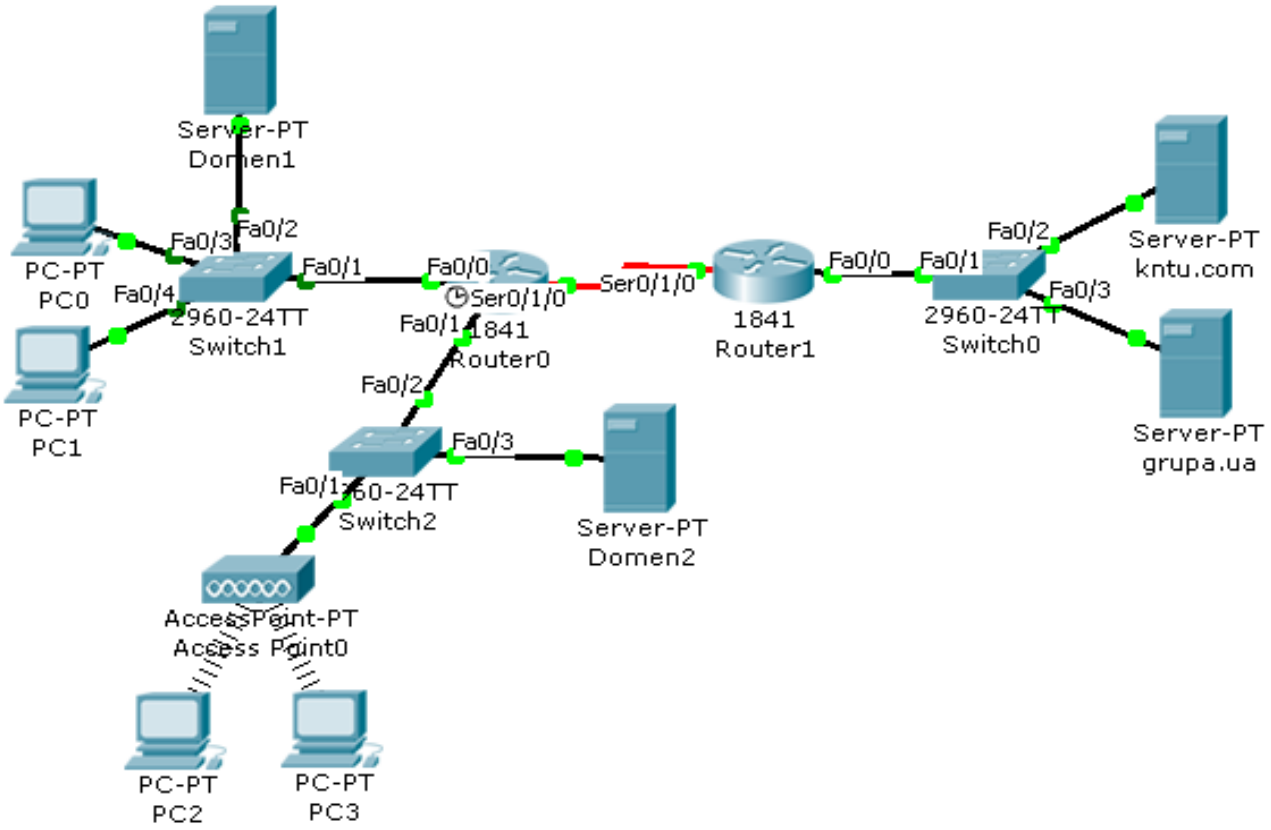


Рисунок 14.1 – Схема локальної мережі для завдання.

3. На вкладці "Вид фізичного пристрою" (***Physical***) перемкнути кнопку живлення в положення **0** (зелений індикатор біля кнопки живлення вимкнеться).

4. В лівій частині вікна натиснути на кнопку ***WIC-1T***, після чого внизу вікна буде зображено вигляд плати та її опис. ЛК миші перетягнути цю плату у вільний лівий роз'єм маршрутизатора.

5. Перемкнути кнопку живлення в положення **I** (індикатор біля кнопки живлення засвітиться зеленим кольором).

6. Провести такі самі налаштунки на маршрутизаторі ***Router1***.

7. Клацнути ЛК миші на комп'ютер ***PC2***, щоб викликати вікно конфігурації.

8. На вкладці "Вид фізичного пристрою" (***Physical***) клацнути на червону кнопку – живлення зникне і зелений індикатор погасне.

9. Опуститись в кінець вікна де знаходяться роз'єми комп'ютера. Перетягнути з комп'ютера роз'єм ***PT-HOST-NM-CFE*** на місце знаходження плат. Тепер у вільний слот помістити плату ***PT-HOST-NM-1W*** (плата Wi-Fi) та

натиснути на кнопку живлення (червона кнопка) – з'явиться живлення і засвітиться зелений індикатор. Після закриття вікна конфігурацій на схемі утвориться бездротовий зв'язок (на схемі показано лінією зі штрихів). Повторити аналогічні дії для комп'ютера ***PC3***.

10. З'єднати всі пристрої між собою кабелями, при цьому обов'язково дотримуйтесь схеми при з'єднанні інтерфейсів. Маршрутизатори з'єднати між собою кабелем ***Serial DTE*** або ***Serial DCE*** (обов'язково зверніть увагу, як розташований годинник на кабелі, інакше буде помилка. Годинник показує на якому інтерфейсі повинна вказуватись тактова частота) з розділу ***Connections***, а всі інші пристрої – кабелем з прямим з'єднанням контактів (***Copper Straight–Through***).

11. Перейменувати всі сервери так, як вказано на схемі.

12. Зайти у вікно конфігурації сервера ***kntu.com*** та перейти на вкладку робочого столу (***Desktop***) і клацнути на піктограму ***IP Configuration***, після чого задати IP-адресу маску підмережі та шлюз, що вказані у варіанті. Перейти на вкладку ***Config*** та клацнути на кнопку ***HTTP*** де вписати такий код:

```
<html>
<center><font size='20' color='red'><b><i><u>University KNTU</b></i></u></font></center>
<p><center><h3>One of the best universities in Ukraine - Kirovograd National Technical University (KNTU)</h3></center></p>
<center><h2><font color='blue'>Thank you!</font></h2></center>
</html>
```

Цей код відображає веб-сторінку, що повинна з'являтися на комп'ютерах мережі при зверненні до неї.

13. Закрити вікно конфігурацій та повторити аналогічні дії для сервера ***grupa.ua***. Код в ***HTTP*** вписати такий:

```
<html>
<center><h1><font color='green'>Student Group</font></h1></center>
<p>This group, which includes all students in Ukraine. Here you can find all the news and talk with other students.</p>
```

<h3>Phone Company: (044) 23-45-67</h3>

</html>

14. Відкрити вікно конфігурації сервера ***Domen1***, перейти на вкладку робочого столу (***Desktop***) і клацнути на піктограму ***IP Configuration***, після чого задати IP-адресу маску підмережі та шлюз, що вказані у варіанті. Далі перейти на вкладку ***Config*** та натиснути на кнопку ***DHCP***. В рядку ***Default Gateway*** ввести шлюз (інтерфейсу FastEthernet сервера Domen1 в форматі ***X.X.X.1***, що вказано у варіанті), а в рядку ***DNS Server*** ввести адресу (інтерфейсу FastEthernet сервера Domen1 в форматі ***X.X.X.50***, що вказано у варіанті). Натиснути на кнопку ***DNS*** та ввести в рядок ***Domain Name*** ім'я: ***kntu.com***, а в рядок ***IP Address*** – IP-адресу домену ***kntu.com***, що вказано у варіанті, після чого натиснути на кнопку ***Add***. Знову в рядок ***Domain Name*** ввести ім'я: ***grupa.ua***, а в рядок ***IP Address*** – IP-адресу домену ***grupa.ua***, що вказано у варіанті, після чого натиснути на кнопку ***Add***.

15. Аналогічно налаштувати сервер ***Domen2***.

16. Клацнути ЛК миші по маршрутизатору ***Router0***, щоб зайти у вікно конфігурацій та перейти на вкладку ***Config***. Активувати та надати інтерфейсам ***FastEhernet 0/0***, ***FastEhernet 0/1*** та ***Serial 0/1/0*** відповідні IP-адреси, маски підмережі та тактову частоту (для інтерфейсу ***Serial 0/1/0***), що вказані в таблиці варіантів.

17. Відкрити вікно конфігурації маршрутизатора ***Router1*** та перейти на вкладку ***Config***, щоб активізувати і задати інтерфейсам ***FastEhernet 0/0*** та ***Serial 0/1/0*** IP-адресу, маску підмережі.

18. Відкрити вікно конфігурації комп'ютера ***PC0*** та перейти на кладку на вкладку робочого столу (***Desktop***), клацнути на піктограму ***IP Configuration*** та поставити відмітку навпроти рядка ***DHCP***. В результаті автоматично повинно буде вписано IP-адресу, маску підмережі, шлюз та DNS-сервер.

19. Аналогічно налаштувати послугу ***DHCP*** на всіх інших комп'ютерах.

20. Для того щоб мережі обмінювались пакетами даних потрібно прописати протокол, наприклад протокол ***OSPF***.

21. Відкрити вікно конфігурації маршрутизатора ***Router0*** та перейти на вкладку ***CLI*** щоб сконфігурувати протокол:

…

Router(config)#router ospf 200

Примітка: число 200 – це номер автономної системи, тобто сукупність мереж, які в подальшому будуть розумітись одним об'єктом.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Примітка: 0.0.0.255 – перевернута маска (інверсна); area 15 – номер області.

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/1 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Router(config-router)#network [*IP-адреса інтерфейсу Serial0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

22. Аналогічно налагодити протокол на маршрутизаторі ***Router1***:

…

Router(config)#router ospf 200

Примітка: число 200 – це номер автономної системи, тобто сукупність мереж, які в подальшому будуть розумітись одним об'єктом.

Router(config-router)#network [*IP-адреса інтерфейсу Serial0/1/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.0.0.255 area 15

Router(config-router)#network [*IP-адреса інтерфейсу FastEthernet0/0 маршрутизатора Router0 в форматі* ***X.X.X.0***] 0.255.255.255 area 15

23. Щоб подивитися на результат сконфігурованого протоколу ***OSPF*** необхідно викликати вікно конфігурації маршрутизатора та перейти на вкладку ***CLI*** де прописати:

…

Router #show ip protocols

А щоб вивести таблицю маршрутизації, то потрібно прописати:

…

Router #show ip route

Аналогічно перевірити інший маршрутизатор, а дані протоколу та таблиці маршрутизації занотувати.

24. Щоб переконатись, що мережа працює правильно, потрібно зробити тестування. Клацнути ЛК миші по комп'ютеру ***PC0*** та перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму командного рядка (***Command Prompt***) та прописати:

PC>ping [*IP-адреса комп'ютера PC3*]

PC>ping [*IP-адреса сервера kntu.com*]

Для більшої впевненості роботи мережі надіслати з інших комп'ютерів ***ping***-запити.

25. Клацнути ЛК миші по будь-якому комп'ютеру, перейти на вкладку робочого столу (***Desktop***), далі натиснути на піктограму веб-браузера (***Web Browser***) – з'явиться вікно браузера, де в рядку ***URL*** ввести ***kntu.com*** після чого натиснути на кнопку ***Go***, в результаті повинна відкритись веб-сторінка. Вписати в рядок ***URL*** ім'я ***grupa.ua*** і проглянути, що виведе браузер. Протестувати браузер на інших комп'ютерах.

26. Зберегти файл та продемонструвати викладачеві.

Таблиця 14.1 Варіанти до практичного завдання 14.

№ варіанту	Router0			Router1	
	IP-адреса та маска інтерфейсу FastEhernet0/0	**IP-адреса та маска інтерфейсу FastEhernet0/1**	**IP-адреса, маска та тактова частота інтерфейсу Serial 0/1/0**	**IP-адреса та маска інтерфейсу FastEhernet0/0**	**IP-адреса та маска інтерфейсу Serial 0/1/0**
1	**2**	**3**	**4**	**5**	**6**
1	192.168.1.1 255.255.255.0	192.168.10.1 255.255.255.0	209.165.1.2 255.255.255.0 4000000	10.10.10.1 255.0.0.0	209.165.1.1 255.255.255.0
2	192.168.2.1 255.255.255.0	192.168.20.1 255.255.255.0	209.164.1.2 255.255.255.0 2000000	10.10.11.1 255.0.0.0	209.164.1.1 255.255.255.0
3	192.168.3.1 255.255.255.0	192.168.30.1 255.255.255.0	209.163.1.2 255.255.255.0 1300000	10.10.12.1 255.0.0.0	209.163.1.1 255.255.255.0
4	192.168.4.1 255.255.255.0	192.168.40.1 255.255.255.0	209.162.1.2 255.255.255.0 1000000	10.10.13.1 255.0.0.0	209.162.1.1 255.255.255.0

1	2	3	4	5	6
5	192.168.5.1 255.255.255.0	192.168.50.2 255.255.255.0	209.161.1.2 255.255.255.0 800000	10.10.14.1 255.0.0.0	209.161.1.1 255.255.255.0
6	192.168.6.1 255.255.255.0	192.168.60.1 255.255.255.0	209.160.1.2 255.255.255.0 500000	10.10.15.1 255.0.0.0	209.160.1.1 255.255.255.0
7	192.168.7.1 255.255.255.0	192.168.70.1 255.255.255.0	209.159.1.2 255.255.255.0 250000	10.10.16.1 255.0.0.0	209.159.1.1 255.255.255.0
8	192.168.8.1 255.255.255.0	192.168.80.1 255.255.255.0	209.158.1.2 255.255.255.0 148000	10.10.17.1 255.0.0.0	209.158.1.1 255.255.255.0
9	192.168.9.1 255.255.255.0	192.168.90.1 255.255.255.0	209.157.1.2 255.255.255.0 128000	10.10.18.1 255.0.0.0	209.157.1.1 255.255.255.0
10	192.168.10.1 255.255.255.0	192.168.100.1 255.255.255.0	209.156.1.2 255.255.255.0 125000	10.10.19.1 255.0.0.0	209.156.1.1 255.255.255.0
11	192.168.11.1 255.255.255.0	192.168.110.1 255.255.255.0	209.155.1.2 255.255.255.0 72000	10.10.20.1 255.0.0.0	209.155.1.1 255.255.255.0
12	192.168.12.1 255.255.255.0	192.168.120.1 255.255.255.0	209.154.1.2 255.255.255.0 64000	10.10.21.1 255.0.0.0	209.154.1.1 255.255.255.0
13	192.168.13.1 255.255.255.0	192.168.130.2 255.255.255.0	209.153.1.2 255.255.255.0 56000	10.10.22.1 255.0.0.0	209.153.1.1 255.255.255.0
14	192.168.14.1 255.255.255.0	192.168.140.1 255.255.255.0	209.152.1.2 255.255.255.0 38400	10.10.23.1 255.0.0.0	209.152.1.1 255.255.255.0
15	192.168.15.1 255.255.255.0	192.168.150.1 255.255.255.0	209.151.1.2 255.255.255.0 19200	10.10.24.1 255.0.0.0	209.151.1.1 255.255.255.0

Продовження таблиці 14.1 Варіанти до практичного завдання 14.

№ варіанту	IP-адреса, маска та шлюз сервера Domen1	IP-адреса, маска та шлюз сервера Domen2	IP-адреса, маска та шлюз сервера kntu.com	IP-адреса, маска та шлюз сервера grupa.ua
1	2	3	4	5
1	192.168.1.50 255.255.255.0 192.168.1.1	192.168.10.50 255.255.255.0 192.168.10.1	10.10.10.2 255.0.0.0 10.10.10.1	10.10.10.3 255.0.0.0 10.10.10.1
2	192.168.2.50 255.255.255.0 192.168.2.1	192.168.20.50 255.255.255.0 192.168.20.1	10.10.11.2 255.0.0.0 10.10.11.1	10.10.11.3 255.0.0.0 10.10.11.1
3	192.168.3.50 255.255.255.0 192.168.3.1	192.168.30.50 255.255.255.0 192.168.30.1	10.10.12.2 255.0.0.0 10.10.12.1	10.10.12.3 255.0.0.0 10.10.12.1

1	2	3	4	5
4	192.168.4.50 255.255.255.0 192.168.4.1	192.168.40.50 255.255.255.0 192.168.40.1	10.10.13.2 255.0.0.0 10.10.13.1	10.10.13.3 255.0.0.0 10.10.13.1
5	192.168.5.50 255.255.255.0 192.168.5.1	192.168.50.50 255.255.255.0 192.168.50.1	10.10.14.2 255.0.0.0 10.10.14.1	10.10.14.3 255.0.0.0 10.10.14.1
6	192.168.6.50 255.255.255.0 192.168.6.1	192.168.60.50 255.255.255.0 192.168.60.1	10.10.15.2 255.0.0.0 10.10.15.1	10.10.15.3 255.0.0.0 10.10.15.1
7	192.168.7.50 255.255.255.0 192.168.7.1	192.168.70.50 255.255.255.0 192.168.70.1	10.10.16.2 255.0.0.0 10.10.16.1	10.10.16.3 255.0.0.0 10.10.16.1
8	192.168.8.50 255.255.255.0 192.168.8.1	192.168.80.50 255.255.255.0 192.168.80.1	10.10.17.2 255.0.0.0 10.10.17.1	10.10.17.3 255.0.0.0 10.10.17.1
9	192.168.9.50 255.255.255.0 192.168.9.1	192.168.90.50 255.255.255.0 192.168.90.1	10.10.18.2 255.0.0.0 10.10.18.1	10.10.18.3 255.0.0.0 10.10.18.1
10	192.168.10.50 255.255.255.0 192.168.10.1	192.168.100.50 255.255.255.0 192.168.100.1	10.10.19.2 255.0.0.0 10.10.19.1	10.10.19.3 255.0.0.0 10.10.19.1
11	192.168.11.50 255.255.255.0 192.168.11.1	192.168.110.50 255.255.255.0 192.168.110.1	10.10.20.2 255.0.0.0 10.10.20.1	10.10.20.3 255.0.0.0 10.10.20.1
12	192.168.12.50 255.255.255.0 192.168.12.1	192.168.120.50 255.255.255.0 192.168.120.1	10.10.21.2 255.0.0.0 10.10.21.1	10.10.21.3 255.0.0.0 10.10.21.1
13	192.168.13.50 255.255.255.0 192.168.13.1	192.168.130.50 255.255.255.0 192.168.130.1	10.10.22.2 255.0.0.0 10.10.22.1	10.10.22.3 255.0.0.0 10.10.22.1
14	192.168.14.50 255.255.255.0 192.168.14.1	192.168.140.50 255.255.255.0 192.168.140.1	10.10.23.2 255.0.0.0 10.10.23.1	10.10.23.3 255.0.0.0 10.10.23.1
15	192.168.15.50 255.255.255.0 192.168.15.1	192.168.150.50 255.255.255.0 192.168.150.1	10.10.24.2 255.0.0.0 10.10.24.1	10.10.24.3 255.0.0.0 10.10.24.1

Питання для самоконтролю.

1. Для чого потрібний DNS-сервер?

2. Яка відмінність між рекурсивними і нерекурсивними серверами?

3. Яку роль відігравали сервери?

4. Скільки підмереж було створено в при виконанні завдання?

15. Комплексна розробка обчислювальної мережі з обліком її апаратної і програмної складових

Метою роботи за даним розділом є перевірка здатностей здобувачів самостійно, творчо застосовувати на практиці теоретичні знання, які отримані як при вивченні дисципліни “Телекомунікаційні та інформаційні мережі”, так і дисциплін «Теорія інформації», «Основи збору передачі та обробки інформації», «Основи комп'ютерної схемотехніки» та «Операційні системи». У процесі роботи здобувачі також повинні придбати практичні навички в області прийняття технічно обґрунтованих рішень при комплексній розробці обчислювальних мереж з обліком їх апаратної і програмної складових.

Виконання роботи включає розробку технічного завдання на основі технічних вимог. Етапи виконання роботи в цілому включають:

- вибір варіанту організації обчислювальної мережі або її частин, включаючи порівняльний аналіз варіантів з обґрунтуванням кінцевого результату;

- розробку структурної електричної схеми обчислювальної мережі та налаштування всіх її елементів.

Завданням роботи є розробка локальної мережі невеликого підприємства, яке має шість підрозділів. Кожен підрозділ підприємства розміщений в окремому кабінеті і має певний набір обладнання не з’єднаного локальною мережею. Розроблена локальна мережа повинна бути підключена до глобальної мережі Internet, для чого підприємство у провайдера отримало виділений пул адрес. Для логічної структуризації локальної мережі необхідно для кожного підрозділу підприємства створити власну підмережу. Зазвичай слід дотримуватись наступних етапів розробки:

1. Обрати свій варіант завдання, до складу якого входить:

а. схема розміщення обладнання (Додаток А);

б. протокол маршрутизації на вибір: 1 – RIP, 2 – OSPF, 3 – IGRP.

2. Ознайомитись з наявним обладнанням, проаналізувати його розміщення та визначити можливості його об’єднання в локальну мережу.

3. Обрати топологію для мережі (краще, щоб це була гібридна топологія), та пояснити свій вибір в пояснювальній записці. З огляду на обрану топологію потрібно підрахувати та обрати необхідну кількість обладнання для мережі, а саме маршрутизаторів (роутерів), комутаторів (свічів) та концентраторів (хабів). При виборі обладнання потрібно звернути увагу на тип та можливість удосконалення в подальшому локальної мережі.

4. Згідно з обраною топологією розробити логічну схему і таблицю розподілу адресного простору локальної мережі підключеної до мережі Internet з врахуванням збільшення кількості комп’ютерів згідно таблиці 15.1. Для мережі провайдером виділений безперервний пул IP-адрес 131.57.X.0/24 (X - порядковий номер студента). Даний пул адрес розподілити між підмережами за допомогою масок з урахуванням умови мінімально достатньої кількості адрес на кожну підмережу. Значення MAC-адрес портів маршрутизаторів, комп'ютерів, а також умовні доменні адреси комп'ютерів призначити самостійно.

5. Виконати моделювання роботи локальної мережі в середовищі Packet Tracer, для чого:

а) завантажити план будівлі, щоб розмістити необхідне обладнання мережі. План приміщення можна створити в Paint або іншому графічному редакторі;

б) розмістити мережне обладнання та з’єднати відповідними кабелями;

в) задати параметри комп’ютерам, серверам, принтерам, а саме: ім’я, IP-адресу, маску підмережі, шлюз та DNS-сервер. (Хоча б дві підмережі повинні автоматично конфігурувати пристрої, тобто використовуючи DHCP);

г) в безпровідній мережі потрібно створити захист від несанкціонованого доступу, тобто встановити пароль доступу;

д) для створення Інтернету використати мінімум п’ять серверів, для кожного з яких створити веб-сторінку. Інтернет повинен бути лише в тих кабінетах, які вказані у варіанті:

е) кожен маршрутизатор повинен мати своє ім’я та пароль на вхід в привілейований режим;

є) при конфігуруванні протоколів маршрутизації, першими сформувати декілька статичних маршрутів, а потім динамічні;

ж) описати функціонування мережних засобів по маршруту просування пакета і привести список подій режиму Simulation при зверненні одного з комп’ютерів локальної мережі до веб-сторінки Інтернету.

6. Всі дані, що встановлюються в мережі повинні бути вставлені в таблиці маршрутизації.

На початковій стадії проектування слід провести аналіз завдання, знайомиться з літературою та іншими матеріалами. При цьому відбувається так звана деталізація проекту, тобто розкладання цільового завдання проектування на часткові завдання, кожне з яких, у свою чергу, розбивається на більш дрібні. Цей процес добре інтерпретується у вигляді деревоподібної структури, де корінь відповідає проектованій ЛОМ, а кожна наступна гілка представляє ту або іншу деталізацію роботи. У підсумку кінцеві гілки утворять нижчий рівень деталізації. Для даного проекту таким рівнем є змодельована структурна схема ЛОМ.

Першим етапом роботи над розробкою мережі є ознайомлення з наявним обладнанням (додаток А). На цьому етапі необхідно проаналізувати наявне обладнання, його розміщення та визначити можливості його об’єднання в загальну мережу. Для побудови мережі рекомендується обрати гібридну топологію. З метою утворення в кожному кабінеті власної підмережі, необхідно виділити на кожний кабінет окремий порт маршрутизатора. Рекомендується використати три маршрутизатори і підключити на кожний по два кабінети. Також для підвищення надійності роботи мережі рекомендується об’єднати дані маршрутизатори в кільце та з’єднати кожен з четвертим маршрутизатором виділеним для з’єднання з зовнішньою мережею провайдера. Обладнання в кожному кабінеті об’єднується за допомогою комутаторів або концентраторів. Приклад побудованої локальної мережі, з використанням вище зазначених рекомендацій, зображений на рис. 15.1.

Таблиця 15.1 – Кількість комп'ютерів після розширення мережі (X – без змін).

Номер варіанту	Номер кабінету					
	1	2	3	4	5	6
1	X	X	X	25	45	X
2	X	X	25	25	X	X
3	X	20	X	X	X	X
4	X	40	50	X	X	X
5	X	X	X	X	20	20
6	X	X	25	25	25	X
7	50	20	X	X	X	X
8	X	X	25	25	X	25
9	X	X	X	25	25	40
10	X	X	X	X	X	X
11	X	50	X	40	X	X
12	X	X	25	25	50	X
13	20	X	X	X	40	40
14	X	X	20	X	45	X
15	X	25	25	X	X	X
16	X	25	X	X	25	X
17	X	X	40	X	20	X
18	X	20	20	20	X	X
19	X	25	40	X	X	X
20	X	X	X	45	45	X
21	X	X	X	25	25	X
22	25	X	X	25	25	X
23	X	X	45	X	X	25
24	X	X	20	20	20	X
25	X	X	X	X	X	X
26	X	20	X	X	X	X
27	X	40	40	X	X	X
28	X	20	20	20	X	X
29	X	X	X	X	40	40
30	X	X	20	X	X	X

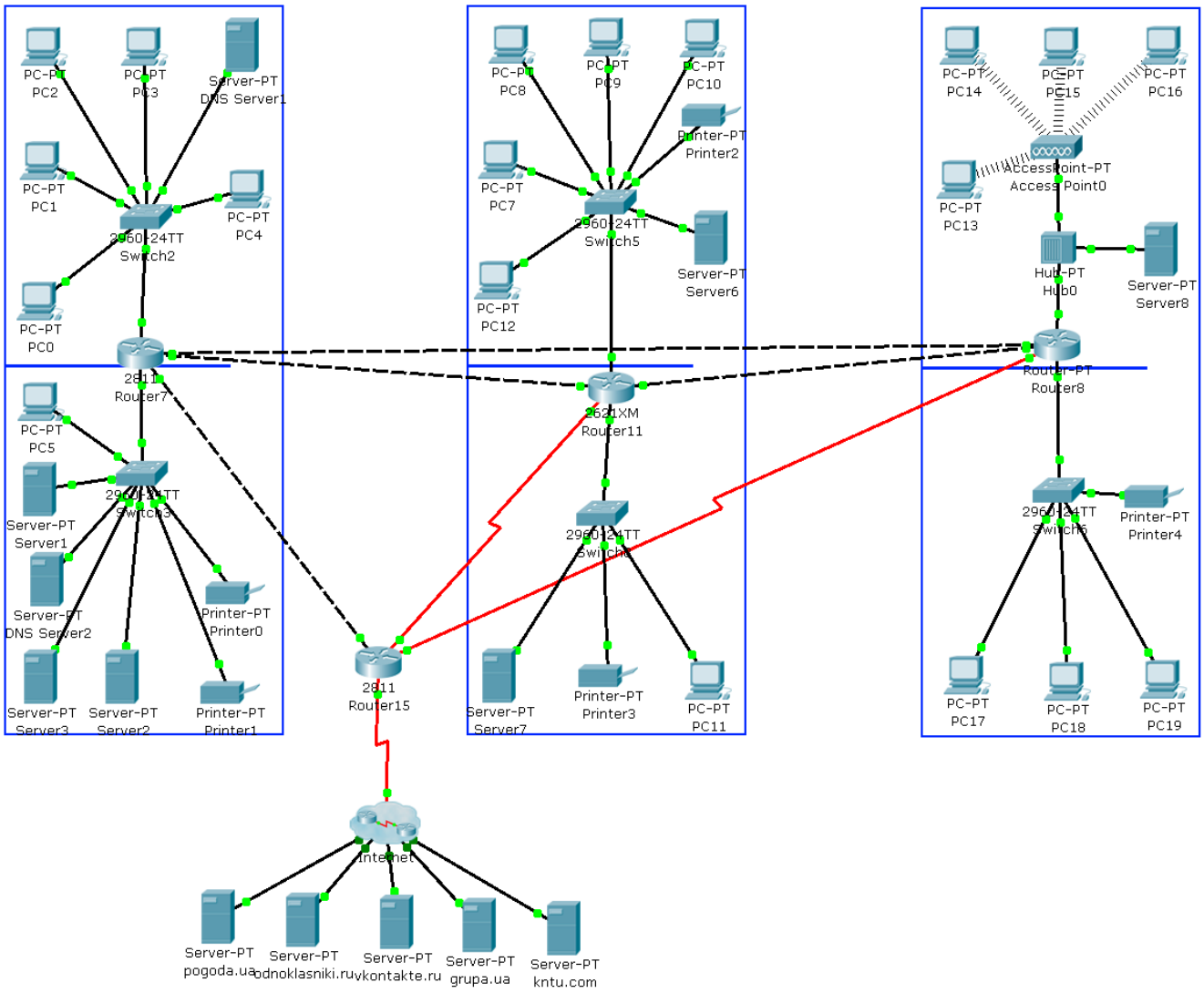


Рисунок 15.1 – Приклад побудови локальної мережі.

Другим етапом роботи є розробка логічної схеми і таблиці розподілу адресного простору локальної мережі. Згідно завдання для мережі провайдером виділений безперервний пул IP-адрес 131.57.X.0/24 (X - порядковий номер студента). Даний пул адрес необхідно розподілити між підмережами за допомогою масок з урахуванням умови мінімально достатньої кількості адрес на кожну підмережу.

Маска – це число, що застосовується в парі з IP-адресою, причому двійковий запис маски містить безперервну послідовність одиниць у тих

розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Границя між послідовностями одиниць і нулів у масці відповідає границі між номером мережі і номером вузла в IP-адресі.

Для даної мережі виділений пул в кількості 256 IP-адрес починаючи з 131.57.X.0/24 по 131.57.X.255/24. Даний пул адрес необхідно розподілити між під мережами, причому кожна підмережа може містити різну кількість обладнання, для якого потрібно виділити IP-адресу. Для розподілу IP-адрес потрібно застосовувати маски змінної довжини (табл. 15.2).

Таблиця 15.2 – Маски змінної довжини.

Маска	Кількість IP-адрес	Максимальна кількість вузлів у мережі
255.255.255.128	128	126
255.255.255.192	64	62
255.255.255.224	32	30
255.255.255.240	16	14
255.255.255.248	8	6
255.255.255.252	4	2

Для вибору маски підмережі у кожному кабінеті необхідно підрахувати кількість IP-адрес, які потрібні для наявного обладнання з урахуванням порту маршрутизатору, до якого буде підключена підмережа або взяти дану кількість з таблиці 1, якщо для даного кабінету планується розширення.

Розглянемо приклад розподілу адресного простору між підмережами локальної мережі. Нехай провайдером виділений пул адрес 131.57.50.0/24. В кабінетах міститься наступна кількість обладнання: кабінет №1 – 10; кабінет №2 – 50; кабінет №3 – 25; кабінет №4 – 12; кабінет №5 – 20; кабінет №6 – 4. Кабінети з’єднані в локальну мережу маршрутизаторами так, як зображено на рисунку 1. Для кожного кабінету потрібно виділити мінімально необхідну кількість IP-адрес. На з’єднання роутерів між собою достатньо виділити чотири IP-адреси з маскою 255.255.255.252. Приклад розподілу зображений на рис. 15.2.

	1 байт	2 байт	3 байт	4 байт		
	Поле номера мережі			Поле номера підмережі	Поле адреси вузла	
Адресний простір 2^8	131	57	50	00 . . 00	000000 . . 111111	Кімната 2 Мережа 131.57.50.0 Маска 255.255.255.192 Кількість вузлів 2^6-2
				010 . . 010	00000 . . 11111	Кімната 3 Мережа 131.57.50.64 Маска 255.255.255.224 Кількість вузлів 2^5-2
				011 . . 011	00000 . . 11111	Кімната 5 Мережа 131.57.50.96 Маска 255.255.255.224 Кількість вузлів 2^5-2
				1000 . . 1000	0000 . . 1111	Кімната 1 Мережа 131.57.50.128 Маска 255.255.255.240 Кількість вузлів 2^4-2
				1001 . . 1001	0000 . . 1111	Кімната 4 Мережа 131.57.50.144 Маска 255.255.255.240 Кількість вузлів 2^4-2
				10100 . . 10100	000 . . 111	Кімната 6 Мережа 131.57.50.160 Маска 255.255.255.248 Кількість вузлів 2^3-2
				101010 . . 101010	00 . . 11	З'єднання роутерів R1-R2 Мережа 131.57.50.168 Маска 255.255.255.252 Кількість вузлів 2^2-2
				101011 . . 101011	00 . . 11	З'єднання роутерів R1-R3 Мережа 131.57.50.172 Маска 255.255.255.252 Кількість вузлів 2^2-2
				101100 . . 101100	00 . . 11	З'єднання роутерів R2-R3 Мережа 131.57.50.176 Маска 255.255.255.252 Кількість вузлів 2^2-2
				101101 . . 101101	00 . . 11	З'єднання роутерів R1-R4 Мережа 131.57.50.180 Маска 255.255.255.252 Кількість вузлів 2^2-2
				101110 . . 101110	00 . . 11	З'єднання роутерів R2-R4 Мережа 131.57.50.184 Маска 255.255.255.252 Кількість вузлів 2^2-2
				101111 . . 101111	00 . . 11	З'єднання роутерів R3-R4 Мережа 131.57.50.188 Маска 255.255.255.252 Кількість вузлів 2^2-2
				110000 . . 110000	00 . . 11	З'єднання роутера R4 з роутером провайдера Мережа 131.57.50.192 Маска 255.255.255.252 Кількість вузлів 2^2-2
				110001 . . 111111	00 . . 11	Вільний діапазон адрес для утворення нових підмереж Кількість адрес 60

Рисунок 15.2 – Приклад розподілу адресного простору.

Також для кожного кабінету необхідно вказати: діапазон виділених адрес, маску, IP-адреси шлюзу та DNS-серверу, IP-адреси призначені статично (для принтерів та серверів обов'язково) та діапазон IP-адрес виділених для протоколу DHCP (у випадку використання). DNS-сервер може бути один для всіх кабінетів або міститись в кожному кабінеті за вибором розробника.

На цьому етап підготовчих робіт завершено і розробник може переходити до етапу моделювання локальної мережі в середовищі Packet Tracer.

Більш докладно розглянемо пункт опису функціонування мережних засобів по маршруту просування пакета і привести список подій режиму Simulation при зверненні одного з комп'ютерів локальної мережі до веб-сторінки Інтернету. Даний пункт є підтвердженням працездатності створеної локальної мережі. Для виконання цього пункту необхідно відкрити файл розробленої мережі, дочекатись автоматичного налаштування всіх вузлів і не виконуючи ніяких зайвих дій (умова незаповненості ARP-таблиць вузлів мережі) перейти в режим Simulation. За допомогою фільтра налаштувати відображення тільки наступних протоколів: ARP, DNS, HTTP, TCP. Далі зайти у вікно браузера одного з комп'ютерів, який має доступ до мережі Інтернет, та ввести символьне ім'я попередньо налаштованої веб-сторінки. В пояснювальну записку занести у вигляді рисунку список подій режиму Simulation. Приклад наведений на рис. 15.3.

Також необхідно привести опис даних подій. Опис подій рекомендується виконати за наступним алгоритмом: хочемо – маємо – не маємо – робимо. Наприклад, хочемо отримати веб-сторінку у вікні браузера, для цього вводимо символьне ім'я веб-сторінки, але оскільки не маємо IP-адреси веб-серверу, то вступає в дію протокол DNS, який призначений для відображення символьного імені в IP-адресу. Протокол DNS формує запит для відправки на DNS-сервер. IP-адреса DNS-серверу відома комп'ютеру з налаштувань, але MAC-адреса DNS-серверу не відома, тому запит не може бути відправлений. Для визначення MAC-адреси DNS-серверу вступає в дію протокол ARP, який призначений для відображення IP-адреси в MAC-адресу. В такому ж стилі необхідно описати проходження всіх пакетів, що містяться в списку подій режиму Simulation.

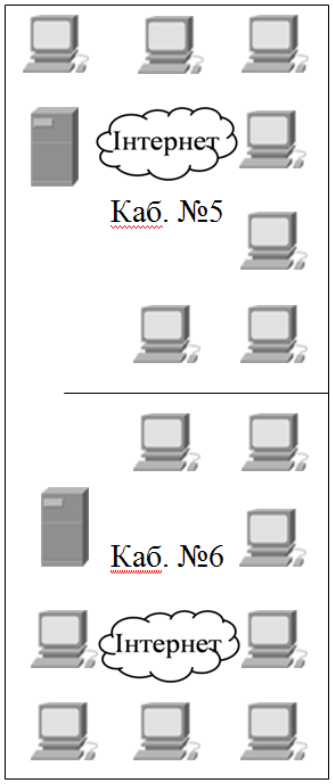
Time (sec)	Last Device	At Device	Type	Info
0.000	--	PC10	DNS	
0.000	--	PC10	ARP	
0.001	PC10	Switch2	ARP	
0.002	Switch2	PC9	ARP	
0.002	Switch2	PC11	ARP	
0.002	Switch2	PC12	ARP	
0.002	Switch2	Server4	ARP	
0.002	Switch2	Printer3	ARP	
0.002	Switch2	Router2	ARP	
0.003	Server4	Switch2	ARP	
0.004	Switch2	PC10	ARP	
0.004	--	PC10	DNS	
0.005	PC10	Switch2	DNS	
0.006	Switch2	Server4	DNS	
0.007	Server4	Switch2	DNS	
0.008	--	PC10	TCP	
0.008	Switch2	PC10	DNS	
0.008	--	PC10	ARP	
0.009	PC10	Switch2	ARP	
0.010	Switch2	PC9	ARP	
0.010	Switch2	PC11	ARP	
0.010	Switch2	PC12	ARP	
0.010	Switch2	Server4	ARP	
0.010	Switch2	Printer3	ARP	
0.010	Switch2	Router2	ARP	
0.011	Router2	Switch2	ARP	
0.012	Switch2	PC10	ARP	
0.012	--	PC10	TCP	
0.013	PC10	Switch2	TCP	
0.014	Switch2	Router2	TCP	
0.015	Router2	Router3	TCP	
0.016	Router3	Router4	TCP	
0.017	Router4	Hub3	TCP	
0.018	Hub3	google.com.ua	TCP	
0.018	Hub3	sinoptik.ua	TCP	
0.018	Hub3	rozetka.com.ua	TCP	
0.018	Hub3	mail.ru	TCP	
0.018	Hub3	kinoafisha.ua	TCP	
0.019	google.com.ua	Hub3	TCP	
0.020	Hub3	Router4	TCP	
0.020	Hub3	sinoptik.ua	TCP	
0.020	Hub3	rozetka.com.ua	TCP	
0.020	Hub3	mail.ru	TCP	
0.020	Hub3	kinoafisha.ua	TCP	
0.021	Router4	Router3	TCP	
0.021	Router4	Router3	TCP	
0.022	Router3	Router2	TCP	
0.023	Router2	Switch2	TCP	
0.024	Switch2	PC10	TCP	
0.024	--	PC10	HTTP	
0.025	PC10	Switch2	TCP	
0.025	--	PC10	HTTP	
0.026	PC10	Switch2	HTTP	
0.026	Switch2	Router2	TCP	
0.027	Switch2	Router2	HTTP	
0.027	Router2	Router3	TCP	
0.028	Router2	Router3	HTTP	
0.028	Router3	Router4	TCP	
0.029	Router3	Router4	HTTP	
0.029	Router4	Hub3	TCP	
0.030	Router4	Hub3	HTTP	
0.030	Hub3	google.com.ua	TCP	
0.030	Hub3	sinoptik.ua	TCP	
0.030	Hub3	rozetka.com.ua	TCP	
0.030	Hub3	mail.ru	TCP	
0.030	Hub3	kinoafisha.ua	TCP	
0.031	Hub3	google.com.ua	HTTP	
0.031	Hub3	sinoptik.ua	HTTP	
0.031	Hub3	rozetka.com.ua	HTTP	
0.031	Hub3	mail.ru	HTTP	
0.031	Hub3	kinoafisha.ua	HTTP	
0.031	--	google.com.ua	TCP	
0.032	google.com.ua	Hub3	TCP	
0.032	--	google.com.ua	HTTP	
0.033	google.com.ua	Hub3	HTTP	
0.033	Hub3	Router4	TCP	
0.033	Hub3	sinoptik.ua	TCP	
0.033	Hub3	rozetka.com.ua	TCP	
0.033	Hub3	mail.ru	TCP	
0.033	Hub3	kinoafisha.ua	TCP	
0.034	Hub3	Router4	HTTP	
0.034	Hub3	sinoptik.ua	HTTP	
0.034	Hub3	rozetka.com.ua	HTTP	
0.034	Hub3	mail.ru	HTTP	
0.034	Hub3	kinoafisha.ua	HTTP	
0.034	Router4	Router3	TCP	
0.035	Router4	Router3	HTTP	
0.035	Router3	Router2	TCP	
0.036	Router3	Router2	HTTP	
0.036	Router2	Switch2	TCP	
0.037	Router2	Switch2	HTTP	

Рисунок 15.3 – Опис функціонування мережі в режимі Simulation.

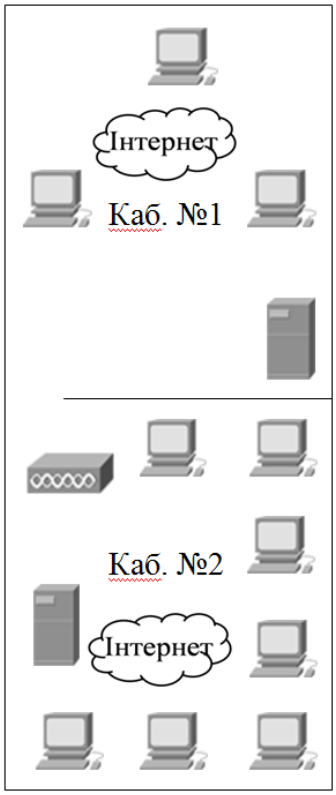
Додаток А

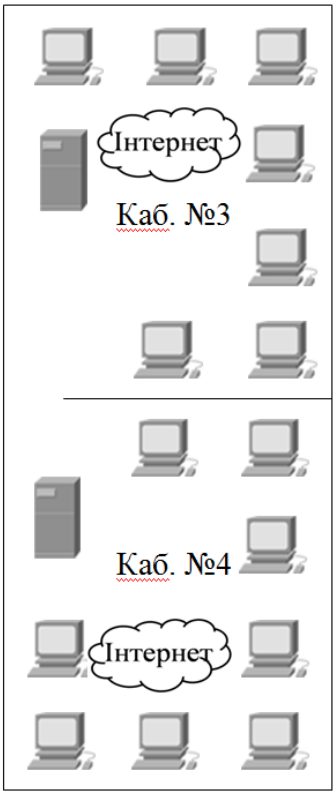
Схема розміщення обладнання

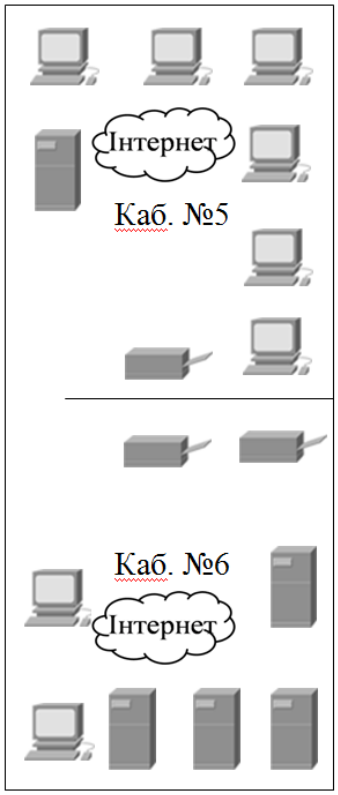
Варіант 1



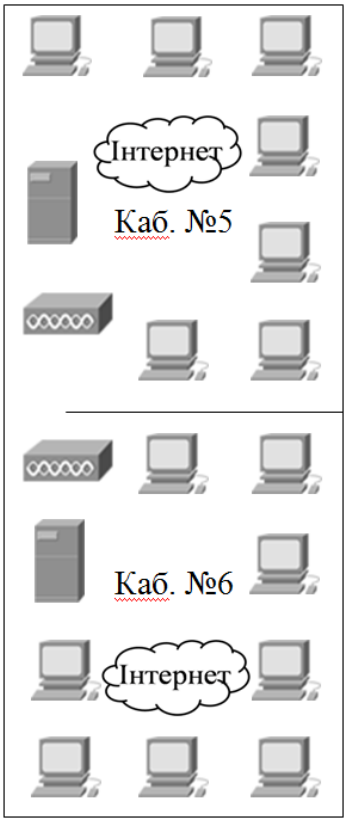
Варіант 2



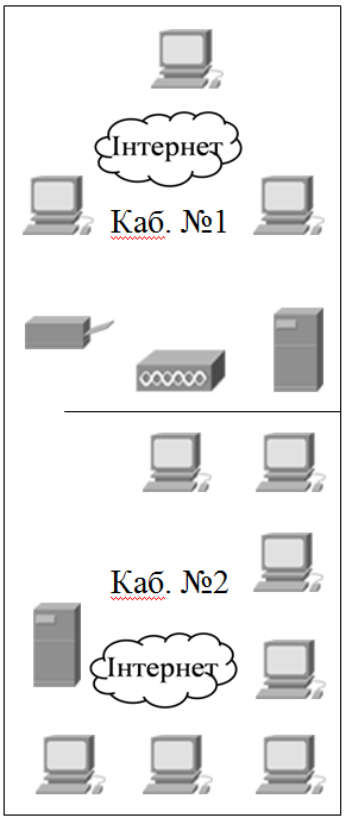


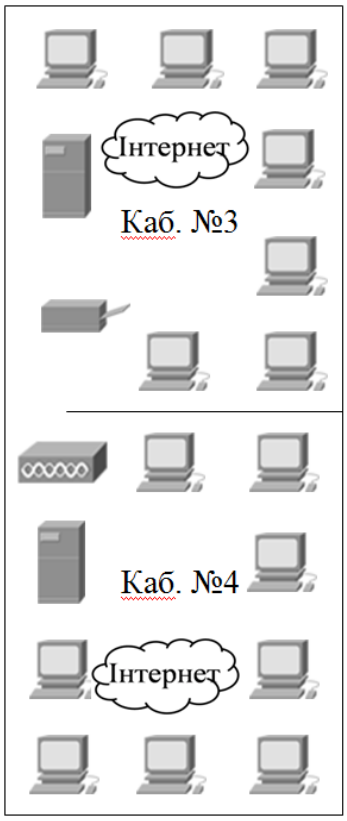


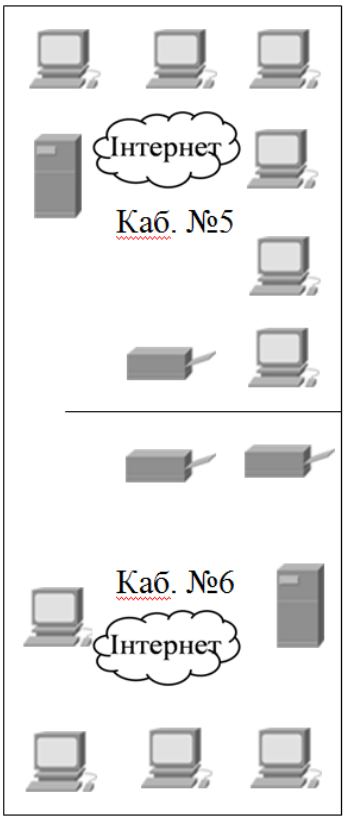
Варіант 3



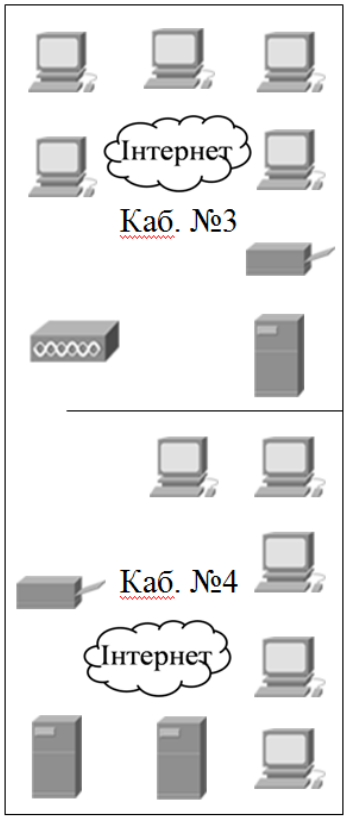
Варіант 4

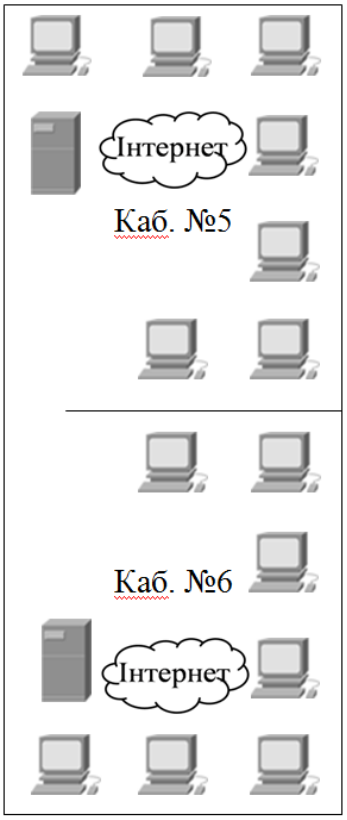




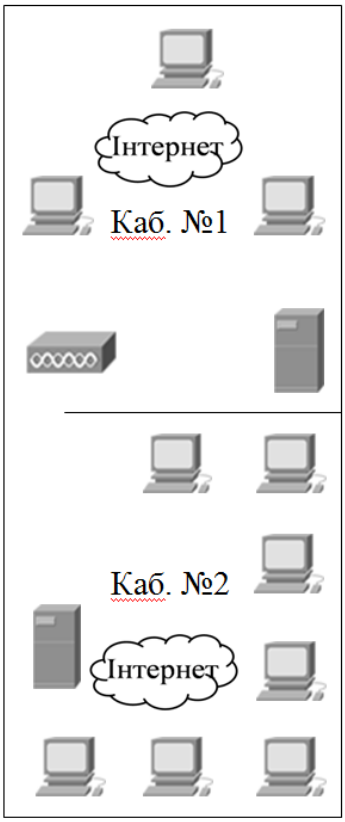


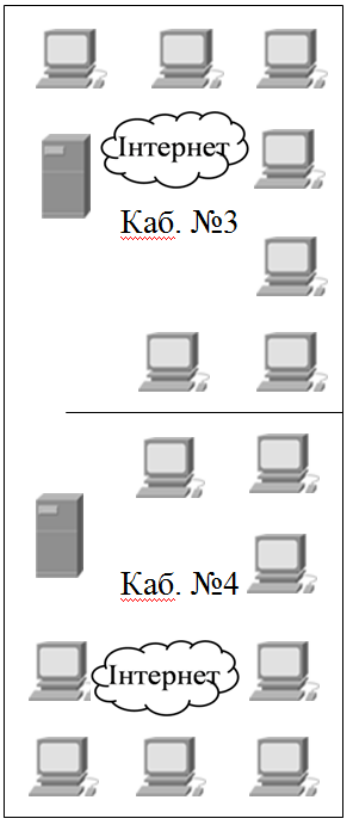
Варіант 5

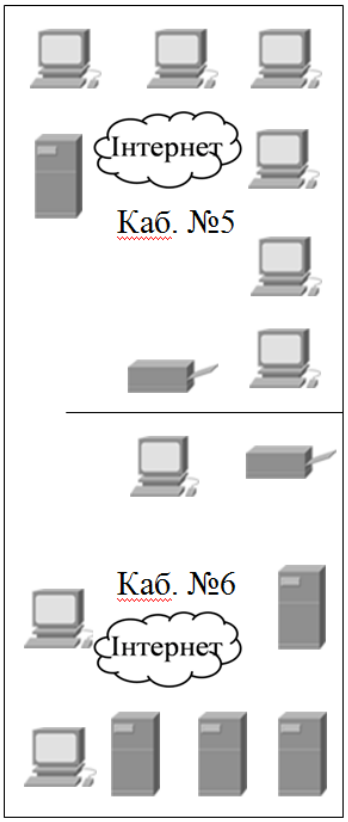




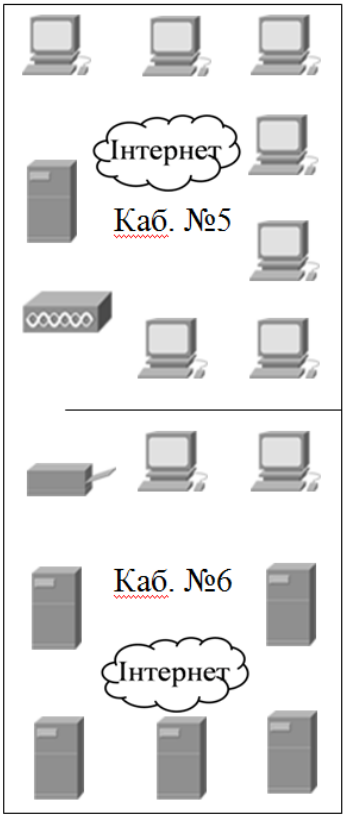
Варіант 6



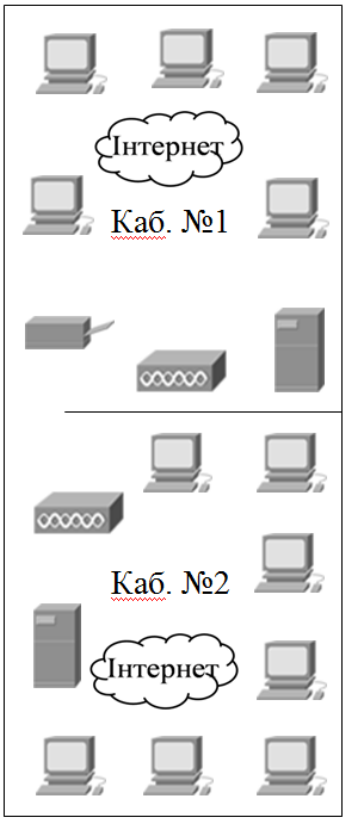


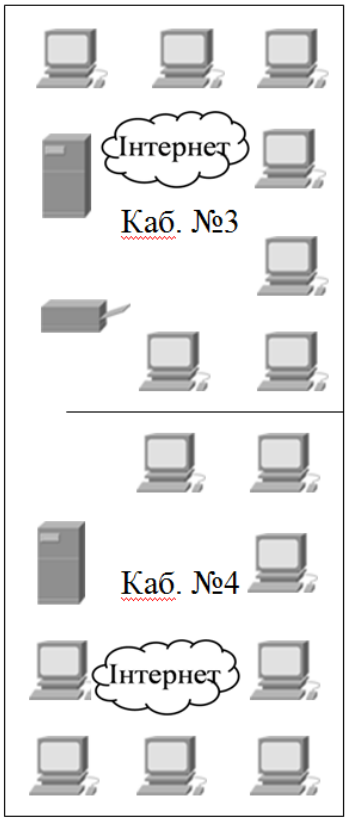


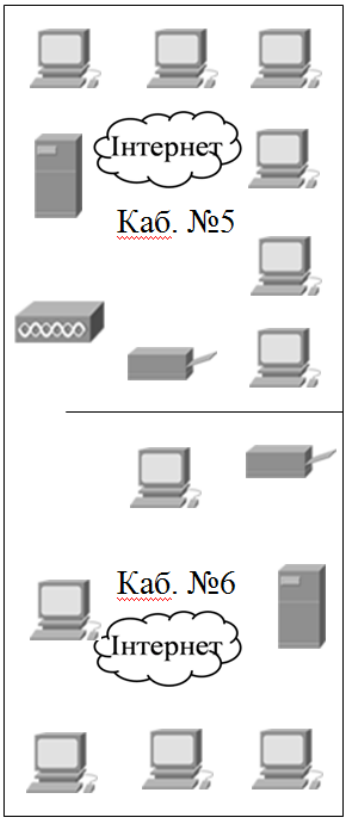
Варіант 7



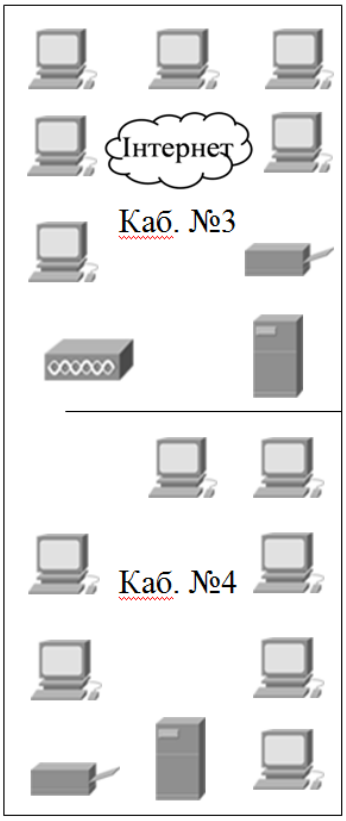
Варіант 8

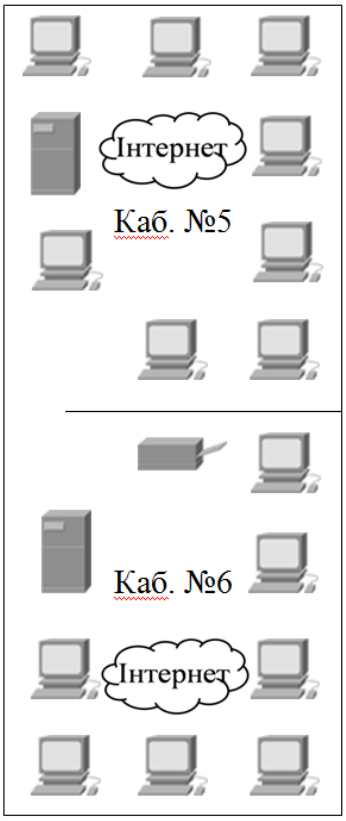




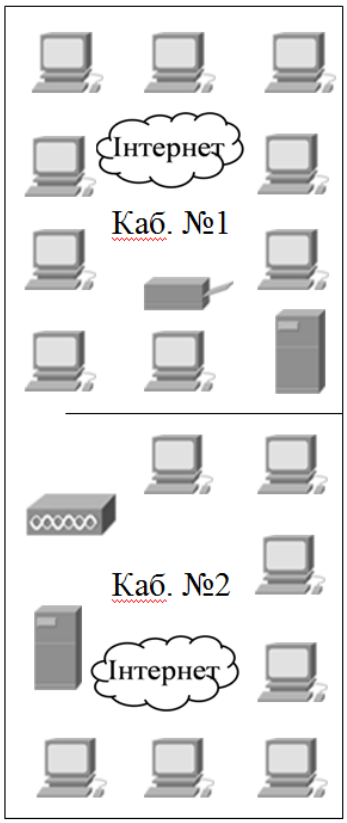


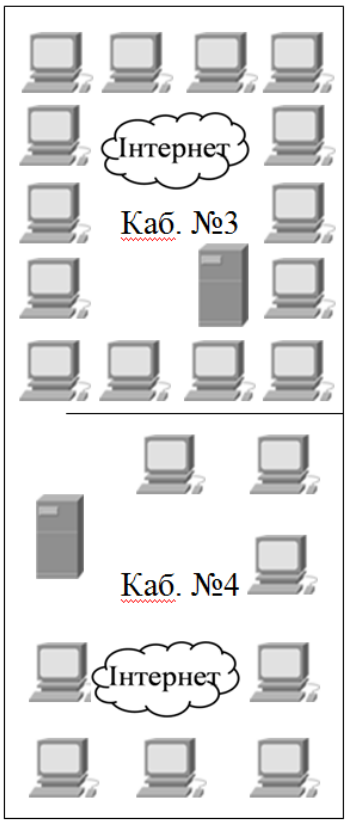
Варіант 9

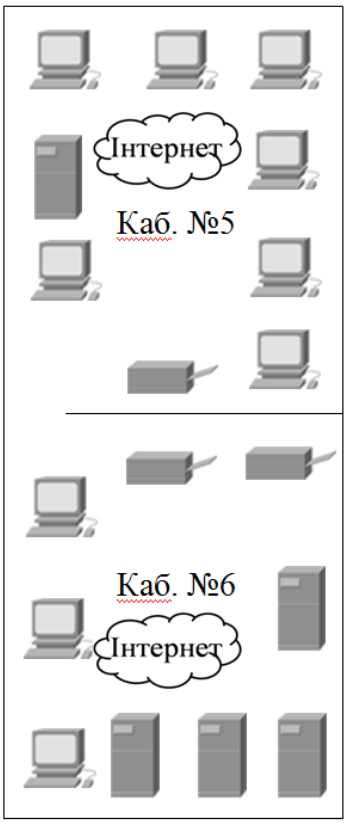




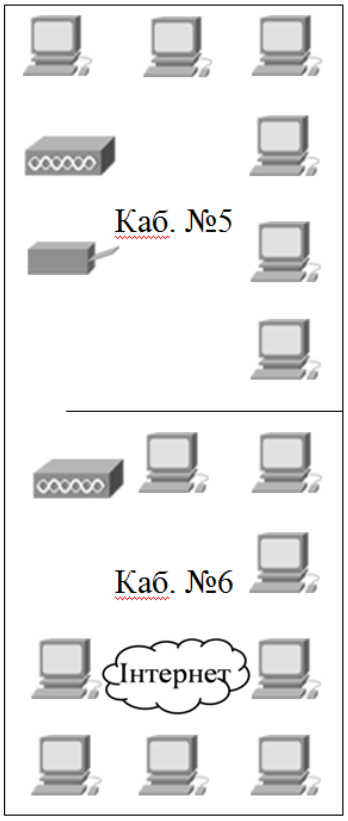
Варіант 10



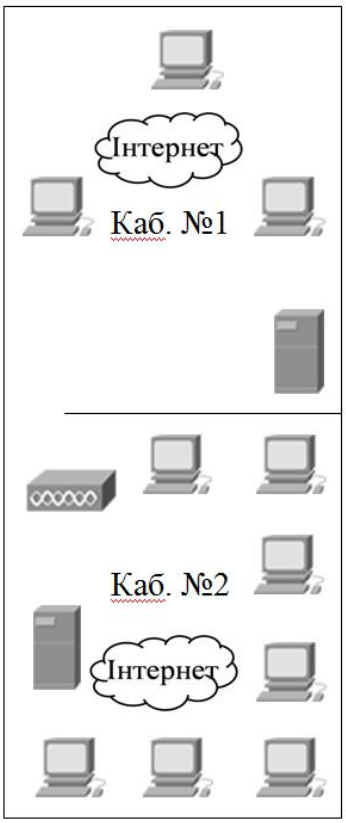


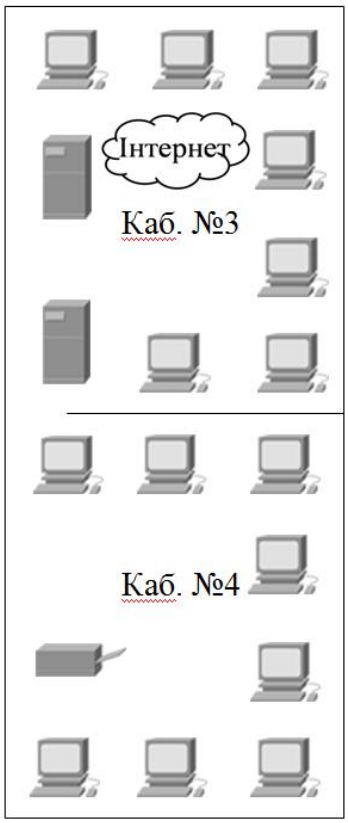


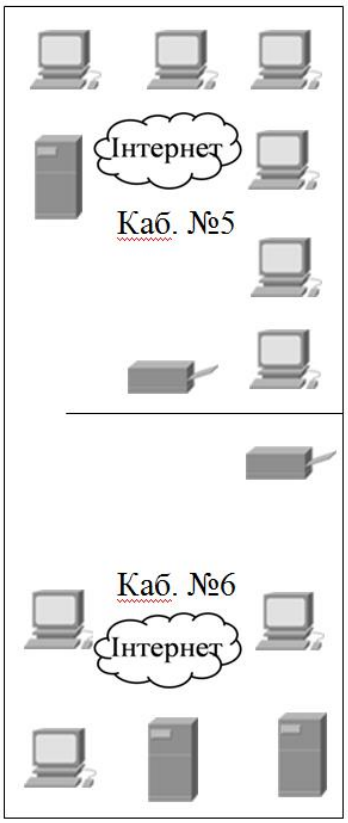
Варіант 11



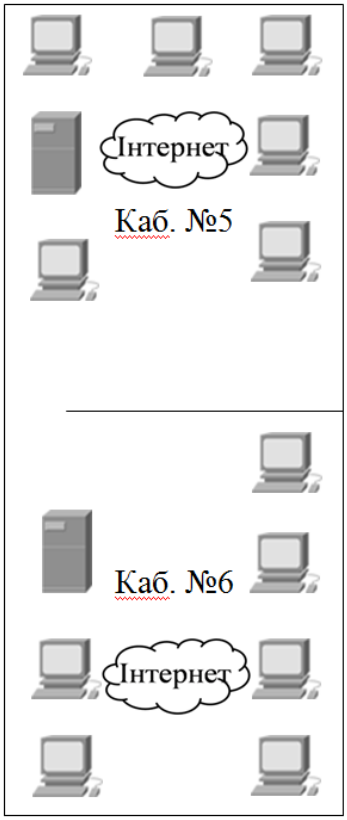
Варіант 12



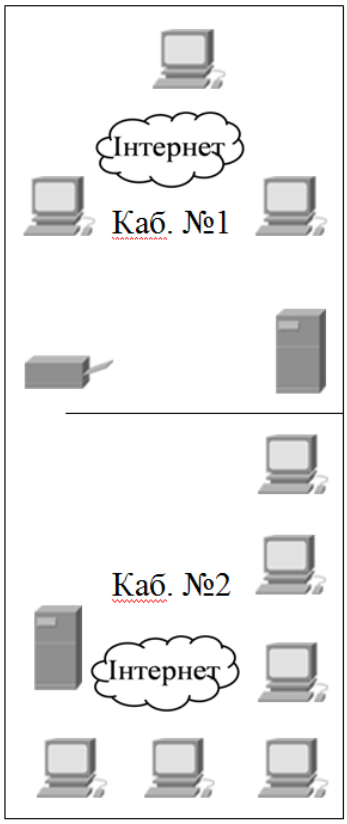


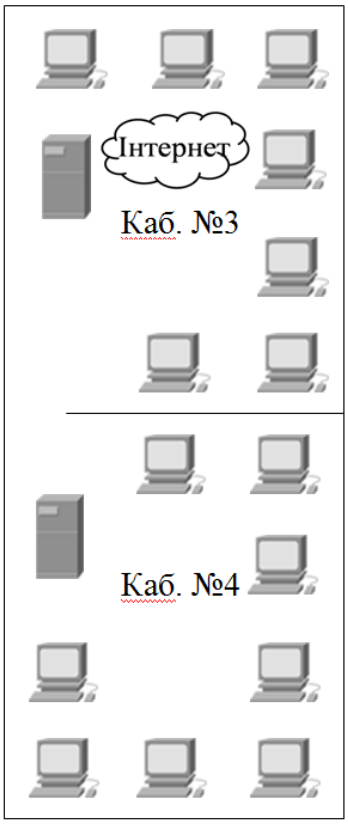


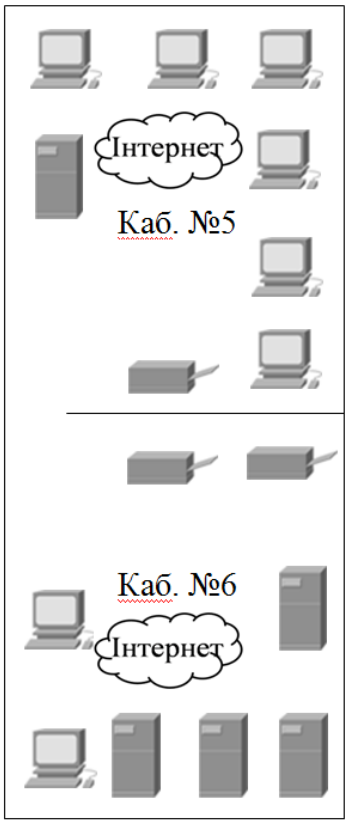
Варіант 13



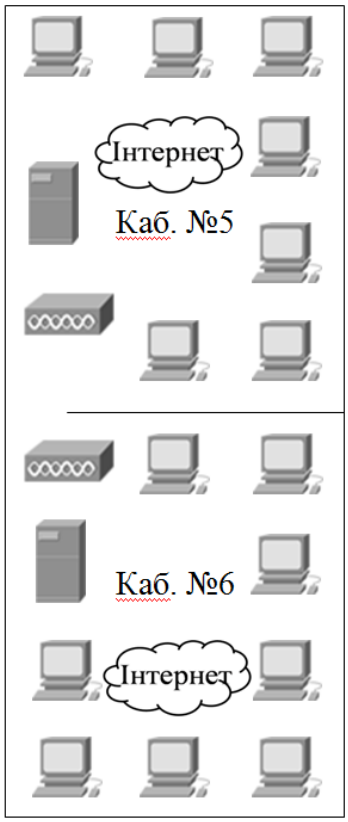
Варіант 14



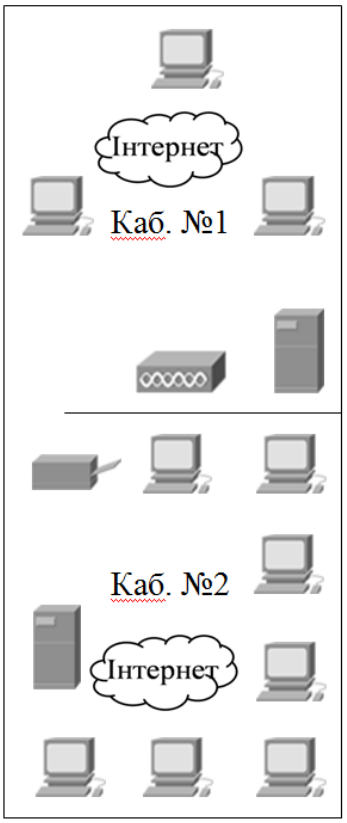


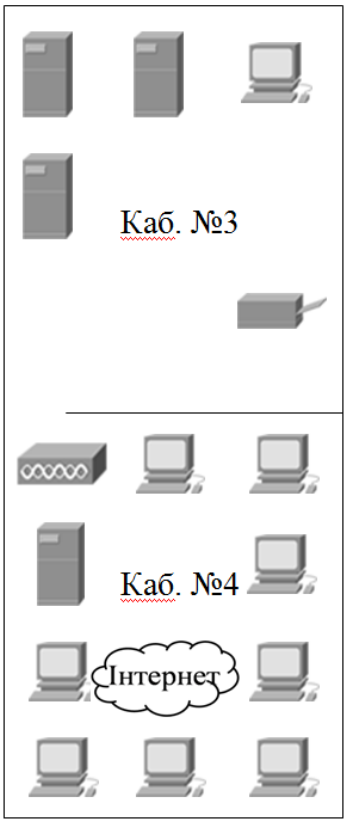


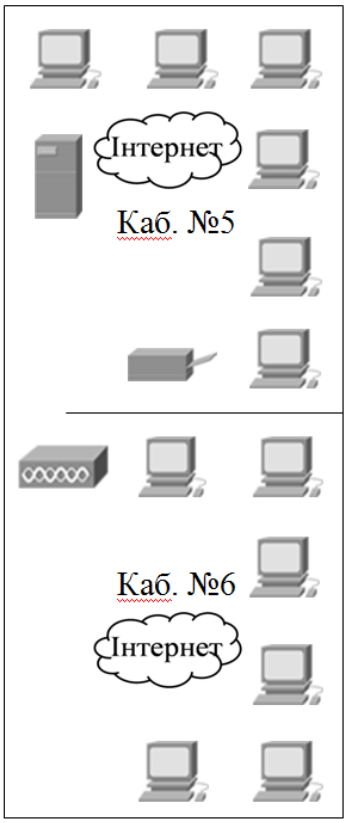
Варіант 15



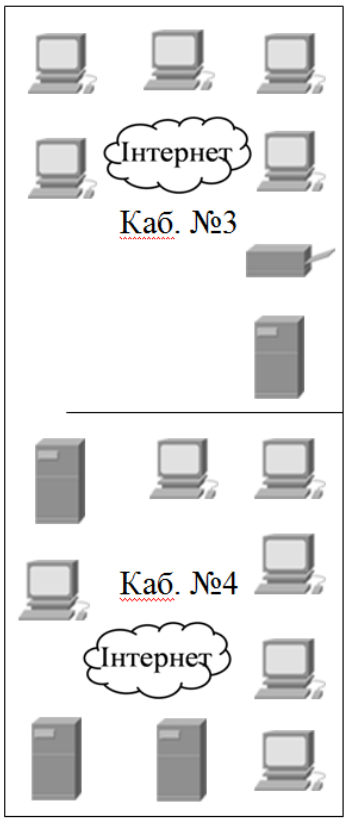
Варіант 16

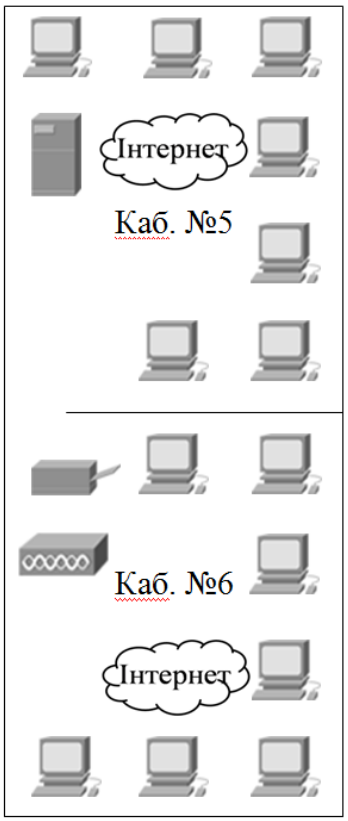




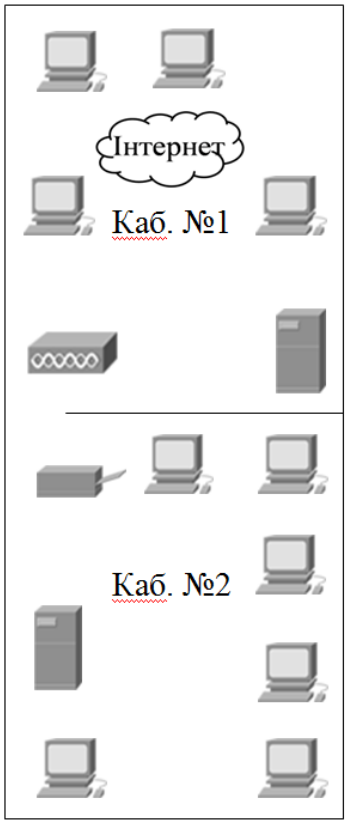


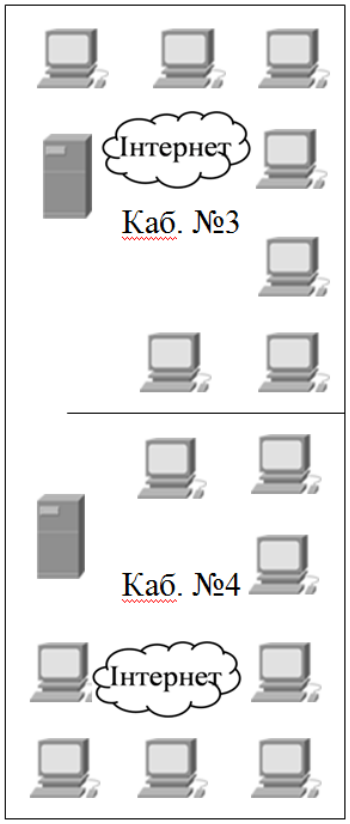
Варіант 17

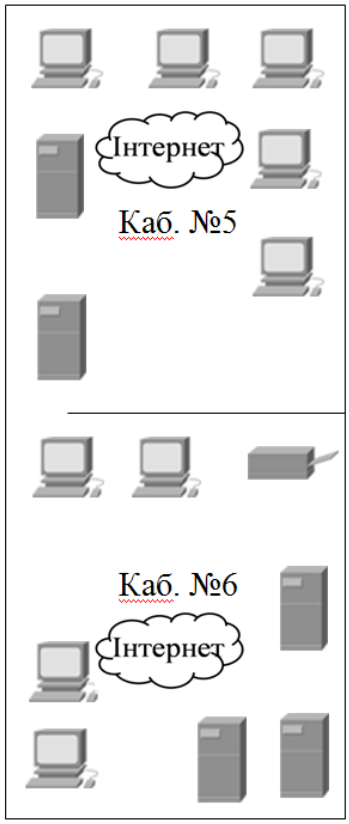




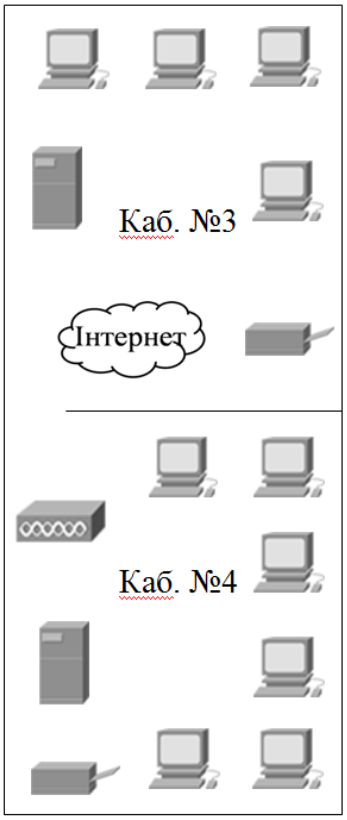
Варіант 18

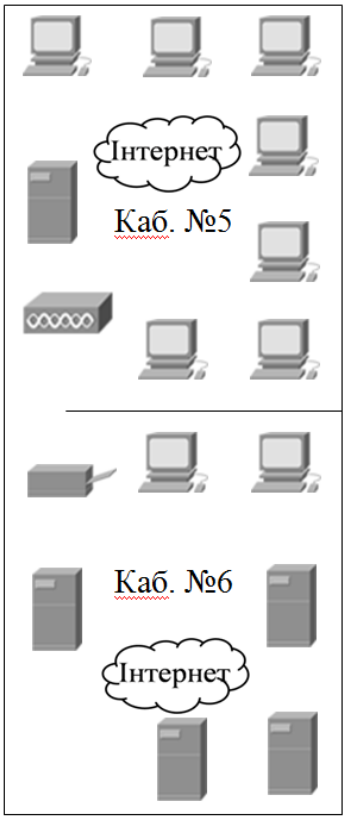




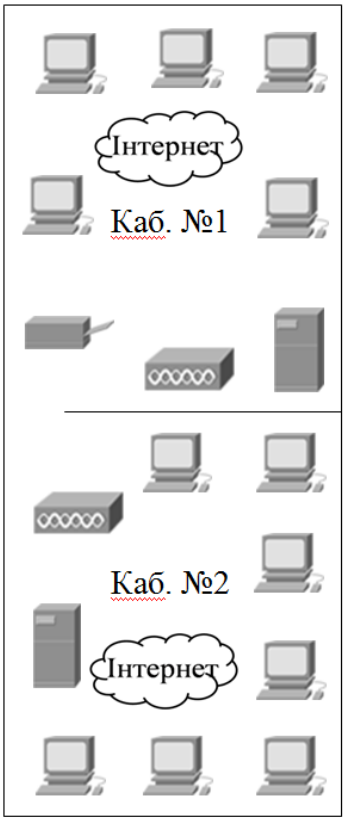


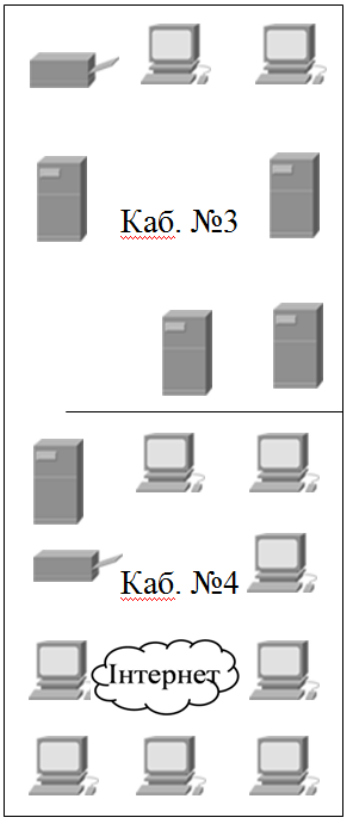
Варіант 19

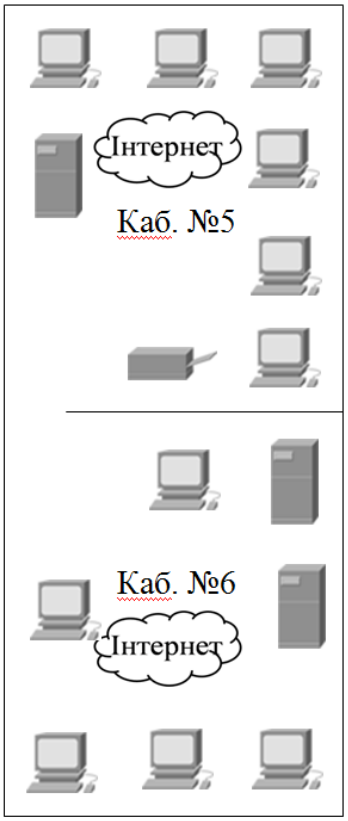




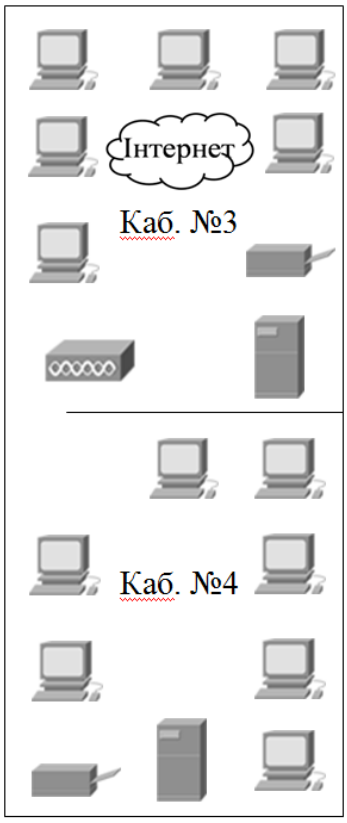
Варіант 20

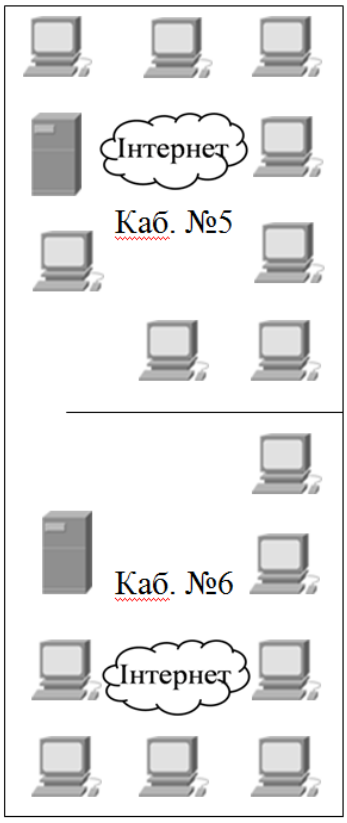




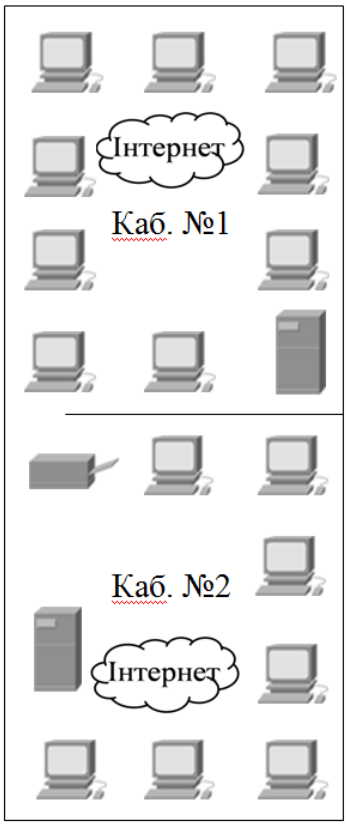


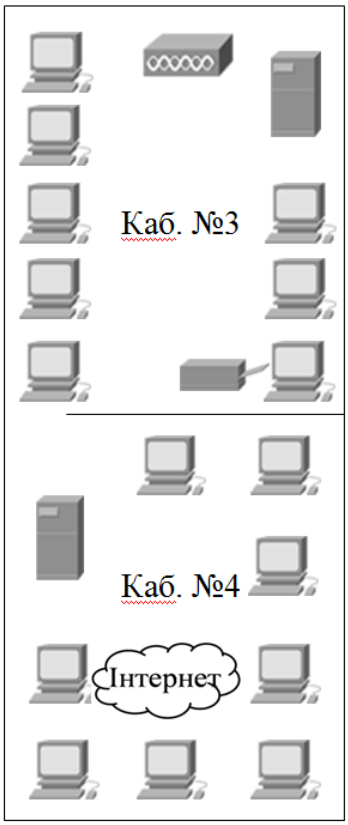
Варіант 21

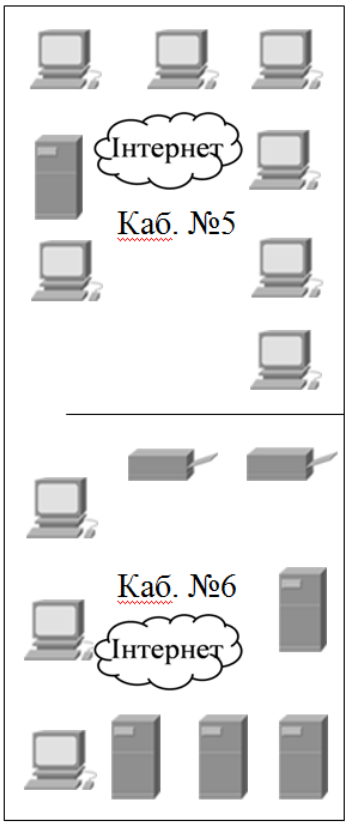




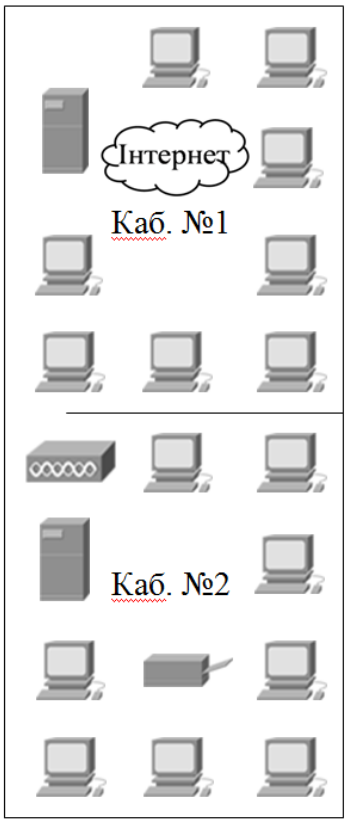
Варіант 22

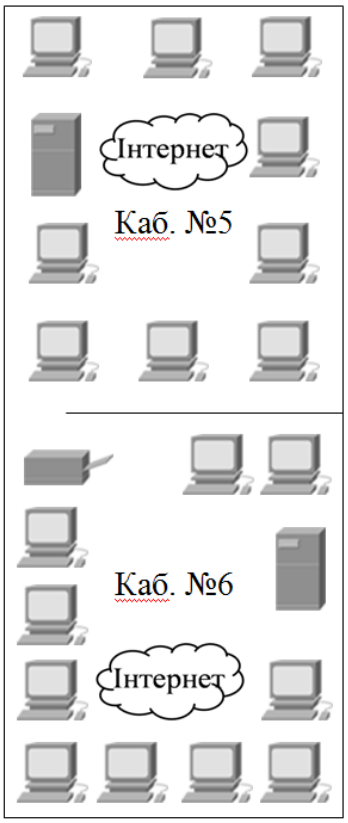




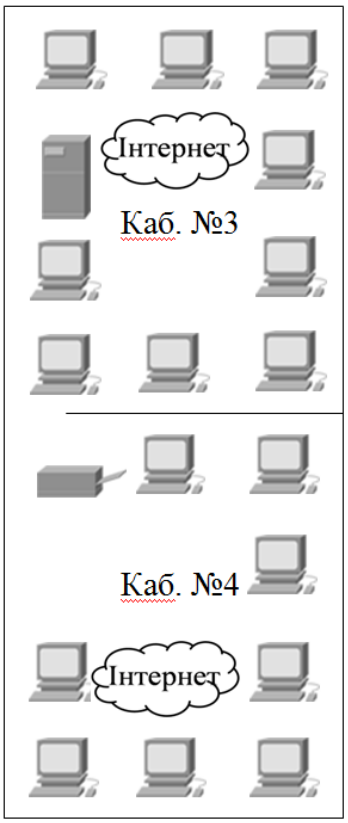


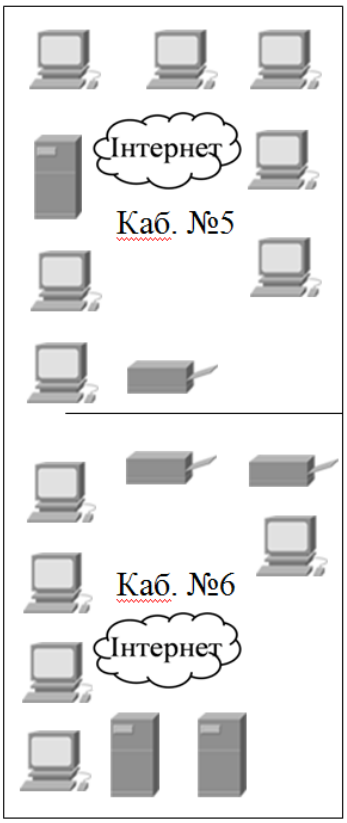
Варіант 23



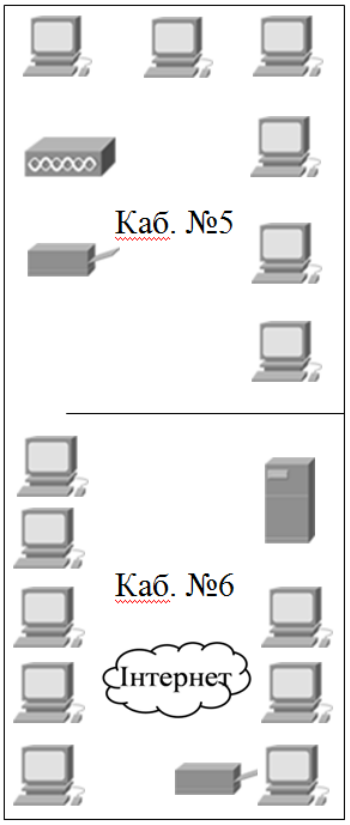


Варіант 24

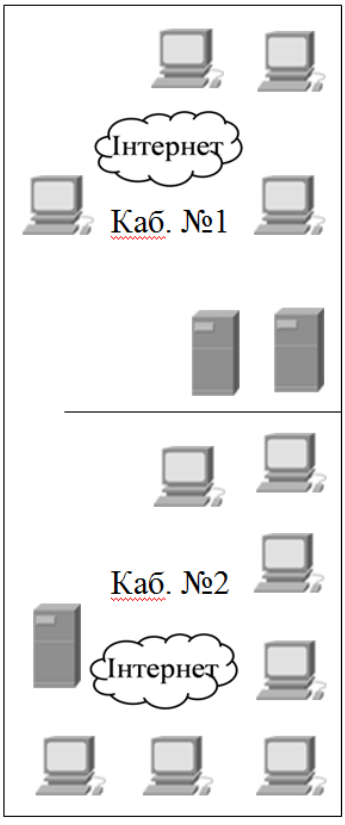


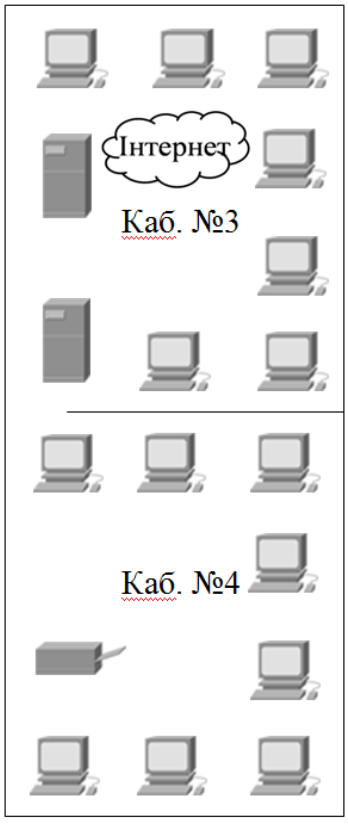


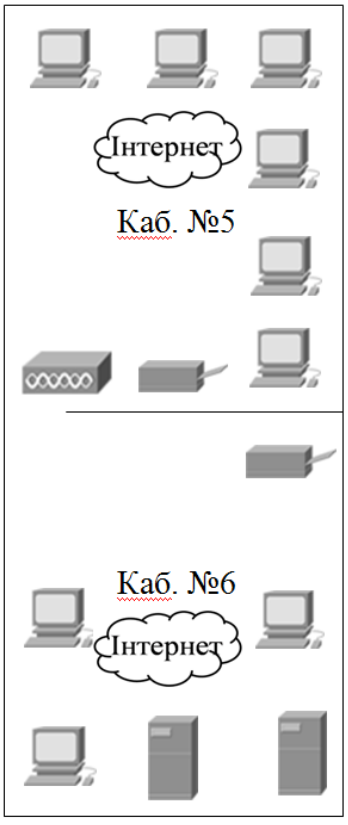
Варіант 25



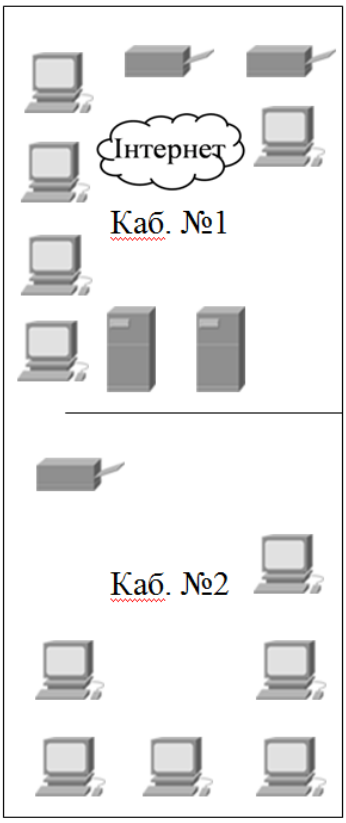
Варіант 26

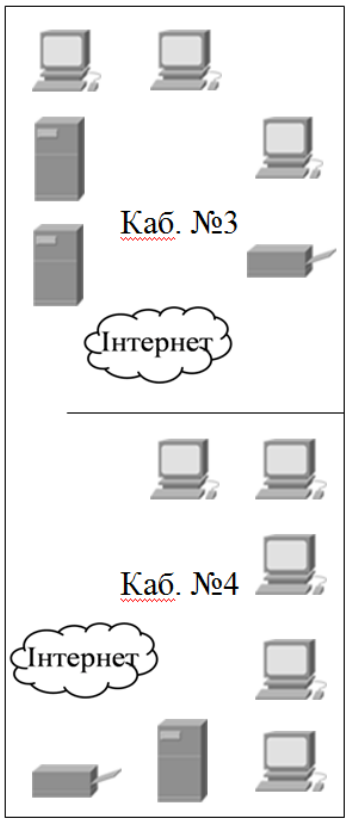


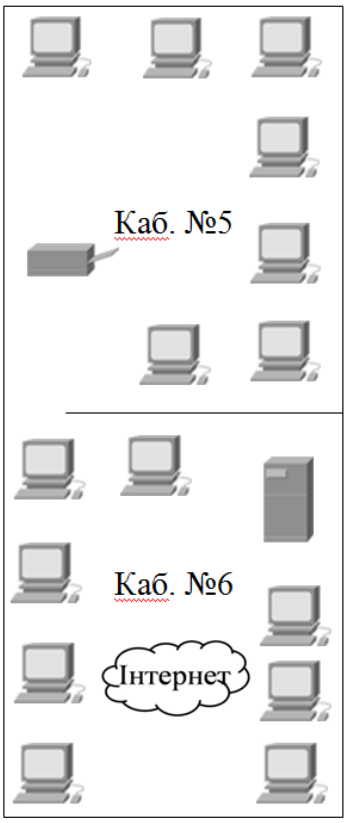




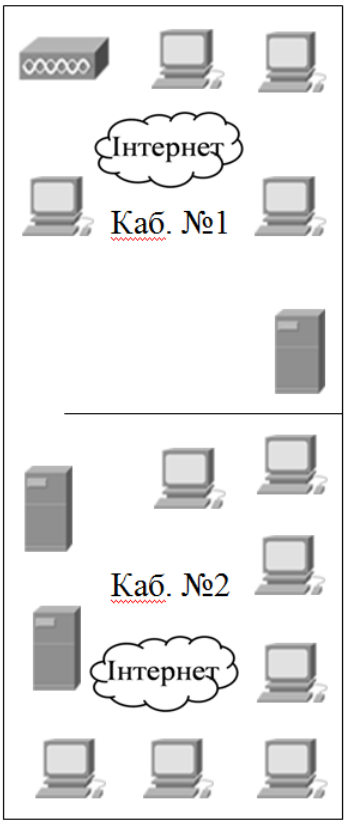
Варіант 27

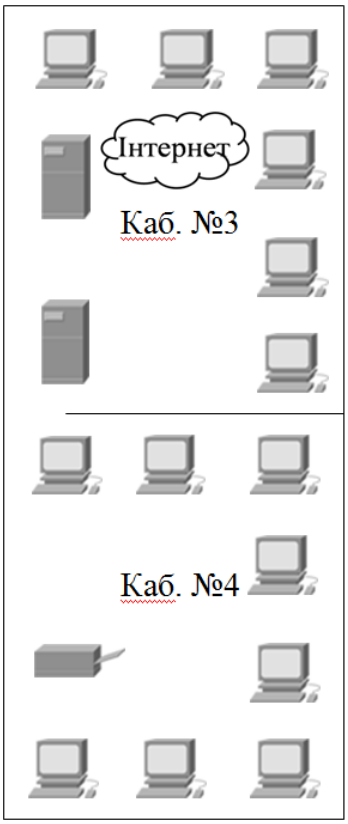


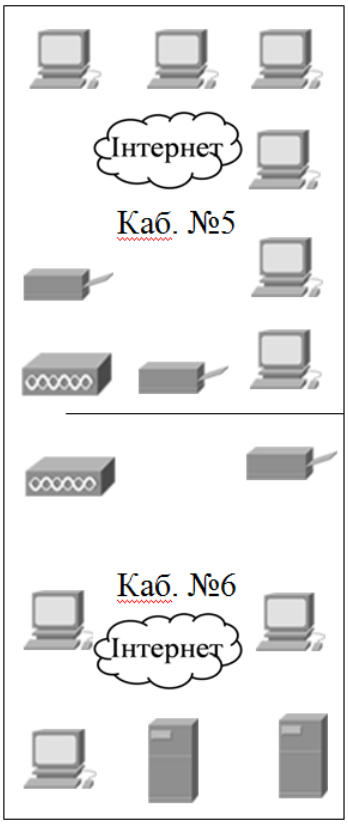




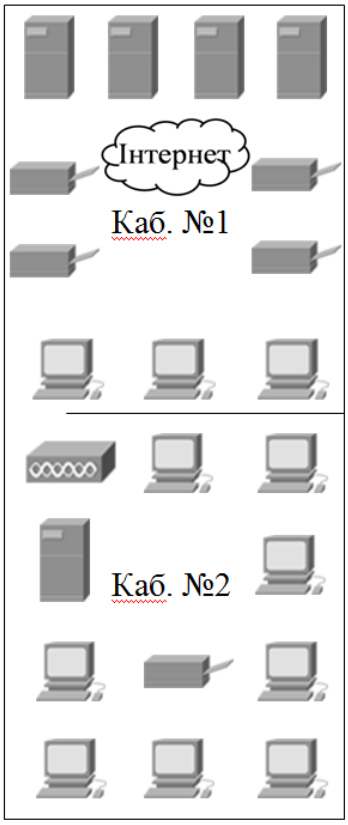
Варіант 28

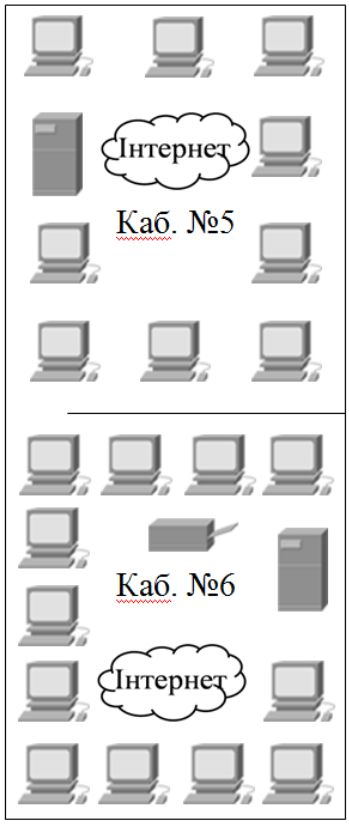




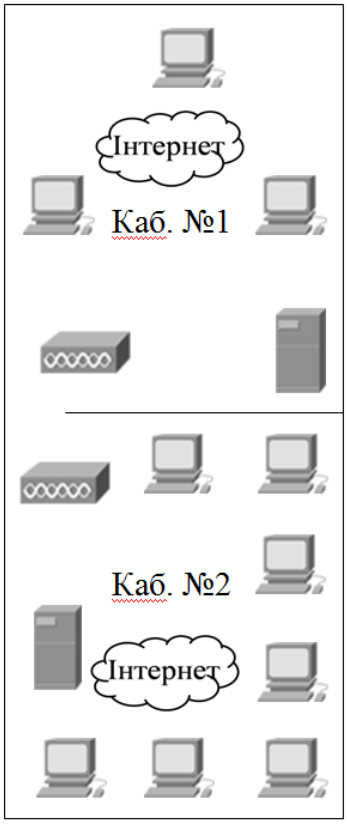


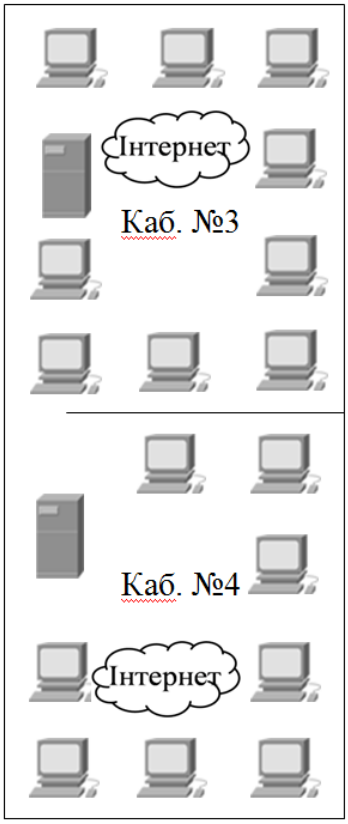
Варіант 29

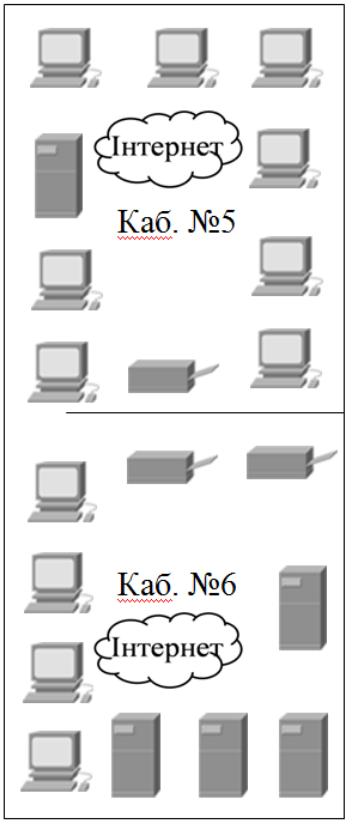




Варіант 30







Список використаних джерел

1. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ № 1/11-11650 від 16.07.12р.) – Львів, «Магнолія 2006», 2014. – 312 с.
2. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник [для вищих навчальних закладів] Київ : САММІТ-Книга, 2010. 708 с.
3. Телекомунікаційні та інформаційні мережі: метод. вказ. для виконання лаб. роб.: для студ. денної та заочної форми навчання спец. 151 - Автоматизація та комп'ютерно-інтегровані технології / [уклад.: О.К. Дідик, О.М. Сербул]; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т, каф. автоматизації виробничих процесів. - Кропивницький: ЦНТУ, 2020. - 114 с.
http://dspace.kntu.kr.ua/jspui/handle/123456789/10634
4. Голь В.Д., Ірха М.С. Телекомунікаційні та інформаційні мережі: навчальний посібник. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 250 с.
5. Tanenbaum A.S., Wetherall D.J. Computer Networks 5th Edition. – Prentice Hall, 2011. – 960 p.
6. Телекомунікаційні та інформаційні мережі: метод. вказ. до виконання курс. роб.: для студ. денної та заочної форми навчання спец. 151 - Автоматизація та комп'ютерно-інтегровані технології / [уклад.: О.К. Дідик, О.М. Сербул]; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т, каф. автоматизації виробничих процесів. - Кропивницький: ЦНТУ, 2020. - 40 с.
http://dspace.kntu.kr.ua/jspui/handle/123456789/10635
7. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: навчальний посібник. Київ : "Техніка", 2003. 923 с.
8. Романов А.И. Телекомунікаційні мережі та управління : навчальний посібник. Київ : ВПЦ "Київський університет", 2003. 247 с.
9. Kurose James F., Ross Keith W. Computer Networking: A Top-Down Approach 8th Edition. – Pearson, 2021. – 792 p. – ISBN-13 9780136681557.
10. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.
11. Goralski Walter. The Illustrated Network: How TCP/IP Works in a Modern Network 2nd Edition. – Morgan Kaufmann, 2017. – 937 p. – ISBN: 978-0-12-811027-0.
12. Жуков І.А., Дрововозов В.І., Махновський Б.Г.Експлуатація комп'ютерних систем та мереж. – К.: НАУ, 2007. – 361с.
13. Рамський Ю.С., Олексюк В.П., Балик А.В. Адміністрування комп'ютерних мереж і систем: навчальний посібник. – Тернопіль: Навч. кн. – Богдан, 2010. 196 с.
14. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ № 1/11-8052 від 28.05.12р.) – Львів, «Магнолія 2006», 2013. – 256 с.

Навчально-методична література

Центральноукраїнський національний технічний університет

О.К. Дідик, О.М. Сербул, І.А. Березюк

Навчальний посібник
ТЕЛЕКОМУНІКАЦІЇНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ

Для студентів спеціальності

174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка»