МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
"Комп'ютерні мережі"
для студентів III курсу денної форми навчання
Напрям підготовки – комп'ютерні науки

ЗАТВЕРДЖЕНО
методичною комісією факультету
комп'ютерних наук
протокол № ___ від _____ 2013 р.

Одеса 2013

Методичні вказівки до виконання лабораторних робіт студентів з дисципліни “Комп’ютерні мережі” для студентів ІІІ курсу денної форми навчання. Напрям підготовки – комп’ютерні науки / Укладач: Кузніченко С.Д., к.г.н., доц. – Одеса, ОДЕКУ, 2013. – 56 с.

Передмова

Методичні вказівки призначені для студентів III курсу денної форми навчання. Мета виконання лабораторних робіт – закріплення теоретичного лекційного матеріалу та придбання практичних навичок у використанні мережного емулятора Cisco Packet Tracer 5.3.2 на базі устаткування компанії Cisco System, стандартних мережних утиліт ОС Windows, та розрахунків пропускної здатності і конфігурації локальних мереж. Для досягнення поставленої мети розглянуті основні принципи, методи та можливості технологій комп'ютерних мереж, до яких в першу чергу відносяться: топології мереж, методи фізичної та логічної структуризації за допомогою мережного комунікаційного обладнання, особливості адресації вузлів у мережі, багаторівнева система передачі даних, протоколи комп'ютерних мереж та ін. Методичні вказівки містять приклади конфігурування віртуальних машин мережевого устаткування (маршрутизаторів) компанії Cisco та приклади розрахунку конфігурації локальної мережі Ethernet, які можуть служити базою при виконані аналогічних завдань лабораторних робіт.

Дисципліна «Комп’ютерні мережі» є однією з основних дисциплін формуючих спеціалістів з напряму підготовки комп’ютерні науки, яка розглядає моделі та методи побудови сучасних локальних і глобальних мереж. Дисципліна викладається у напрямі бакалаврської підготовки «Комп’ютерні науки» і відноситься до циклу професійної та практичної підготовки (цикл В).

Внаслідок вивчання дисципліни студент повинен:

знати: призначення основних мережних утиліт операційних систем сімейства Windows; етапи діагностики мережі; структуру та основні протоколи стека TCP/IP; основи адресації в IP – мережах; архітектури комп’ютерних мереж; принципи структурування та конфігурування мереж; методи передачі дискретних даних на фізичному і канальному рівнях; характеристики ліній зв'язку; принципи стандартизації в комп'ютерних мережах; технології Ethernet, Token Ring, FDDI локальних мереж.

вміти: аналізувати конфігурацію мережі на платформі ОС Windows; одержувати IP – адреси, ім’я домена, імена комп’ютерів, що входять у домен; переглядати і підключати загальні ресурси; визначати причини неполадок у мережі; працювати з емулятором IP-мереж Cisco Packet Tracer 5.3.2; конфігурувати та проводити налаштування комутаційного обладнання та маршрутизаторів Cisco за допомогою команд операційної системи Cisco IOS; розраховувати конфігурацію локальної мережі Ethernet відповідно її фізичного середовища.

Лабораторна робота № 3

Конфігурування маршрутизаторів Cisco

1. Мета роботи

Метою лабораторної роботи є ознайомлення студентів з прийомами роботи з мережною операційною системою Cisco IOS та отримання навичок конфігурування комутаційного обладнання та маршрутизаторів Cisco.

2. Завдання до лабораторної роботи

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Фізична і логічна структуризація мережі за допомогою різних типів комунікаційного обладнання” і „Принципи роботи маршрутизаторів”. Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

2.1 Конфігурування комутаторів і маршрутизаторів з командного рядка операційної системи IOS

Розглянемо більш детально на прикладі конфігурування комутаторів і маршрутизаторів використання команд командного рядка операційної системи IOS.

При першому вході в мережевий пристрій користувач бачить командний рядок режиму користувача виду:

Switch>

Команди, доступні в режимі користувача є підмножиною команд, що доступні в привілейованому режимі. Ці команди дозволяють виводити на екран інформацію без зміни установок мереженого пристрою.

Щоб отримати доступ до повного набору команд, необхідно спочатку активізувати привілейований режим.

Press ENTER to start.

Switch>

Switch>**enable**

Switch#

Switch#**disable**

Switch>

Тут і далі виведення мережевого пристрою буде даватися звичайним шрифтом, а виведення користувача **жирним** шрифтом.

Про перехід у цей режим буде свідчити поява в командному рядку запрошення у виді знака #. З привілейованого рівня можна отримати інформацію про настройки системи і отримати доступ до режиму глобального конфігурування і інших спеціальних режимів конфігурування, включаючи режими конфігурування інтерфейсу, підінтерфейсу, лінії, мережевого пристрою, карти маршрутів і т.п. Для виходу з системи IOS необхідно набрати на клавіатурі команду exit (вихід).

Switch>**exit**

Незалежно від того, як звертаються до мережевого пристрою: через консоль термінальної програми, що приєднана через ноль-модем до COM-порту мережевого пристрою, або в рамках сеансу протоколу Telnet, пристрій можна перевести в один з режимів. Нас цікавлять такі режими.

Режим користувача – це режим перегляду, в якому користувач може тільки переглядати певну інформацію про мережевий пристрій, але не може нічого змінювати. В цьому режимі запрошення має вигляд типу Switch>.

Привілейований режим – підтримує команди настройки і тестування, детальну перевірку мережевого пристрою, маніпуляцію з конфігураційними файлами і доступ в режим конфігурування. В цьому режимі запрошення має вигляд типу Switch#.

Команди в будь-якому режимі IOS розпізнає за першими унікальними символами. При натисненні табуляції IOS сам доповнить команду до повного імені.

При введенні в командному рядку будь-якого режиму імені команди і знака питання (?) на екран виводяться коментарі до команди. При введені одного знака результатом буде список всіх команд режиму. На екран може виводиться багато екранів рядків, тому іноді знизу екрана буде з’являтися підказка – More -. Для продовження слід натиснути enter або пробіл.

Команди режиму глобального конфігурування визначають поведінку системи в цілому. Крім того, команди режиму глобального конфігурування включають команди переходу в інші режими конфігурування, які використовуються для створення конфігурацій, що потребують багаторядкових команд. Для входу в режим глобального конфігурування використовується команда привілейованого режиму configure. При введенні цієї команди слід вказати джерело команд конфігурування: terminal (термінал), memory (енергонезалежна пам'ять або файл), network (сервер tftp (Trivial ftp – спрощений ftp) в мережі). За замовчуванням команди вводяться з терміналу консолі. Наприклад

Switch# configure terminal

Switch(config)#(commands)

Switch(config)#exit

Switch#

Команди для активізації частинного виду конфігурації повинні передувати командам глобального конфігурування. Так для конфігурації інтерфейсу, на можливість якої вказує запрошення Switch(config-if)#, спочатку вводиться глобальна команда для визначення типу інтерфейсу і номер його порту:

Switch# **conf t**

Switch(config)# **interface type port**

Switch(config-if)# ***(commands)***

Switch(config-if)# **exit**

Switch(config)# **exit**

Для обмеження доступу до системи використовуються паролі. Команда **line console** встановлює пароль на вхід на термінал консолі:

Switch(config)# **line console 0**

Switch(config-line)# **login**

Switch(config-line)# **password Cisco**

Команда **line vty 0 4** встановлює парольний захист на вхід за протоколом Telnet:

Switch(config)# **line vty 0 4**

Switch(config-line)# **login**

Switch(config-line)# **password cisco**

Команда **enable password** обмежує доступ до привілейованого режиму:

Switch#**conf t**

Switch(config)# **enable password** пароль

Далее

Ctrl-Z

Switch#**ex**

…

Press RETURN to get started

Switch>**en**

Password: **пароль**

Switch#

Тут пароль **пароль** – послідовність латинських символів.

Для встановлення на мережевому інтерфейсі IP адреси використовується команда:

Router(config-if)#**ip address** [ip-address][subnet-mask],

Router(config-if)#**no shut**

Команда no shut (скорочення від no shutdown) використовується для того, щоб інтерфейс був активним (без цієї команди можливе довільне тимчасове відключення інтерфейсу). Зворотна команда – shut, вимкне інтерфейс.

Важливо мати можливість контролю вірності функціонування і стану мережевого пристрою в будь-який момент часу. Для цього служать команди:

Таблиця 2.1 – Show команди

Команда	Опис
show version	Виводить на екран дані про конфігурації апаратної частини системи, версії програмного забезпечення, імена і джерела файлів конфігурування і завантажені образи
show running-config	Показує зміст активної конфігурації
show interfaces	Показує дані про всі інтерфейси на пристроях
show protocols	Виводить дані про протоколи третього мережевого рівня.

2.2 Хід роботи

Реалізуємо поділ мережі на підмережі використовуючи програму Packet Tracer. Нехай адміністратор виконав розбиття мережі 192.168.8.0/24 на 6 підмереж. Використовуючи адреси 4-х перших підмереж, представимо їх логічну структуру за допомогою програми. Адреси підмереж наведені в табл. 2.2.

Таблиця 2.2 – Адреси підмереж

Адреса мережі	Широкомовний адрес	Адреси хостів	
192.168.8.32	192.168.8.63	**від** 192.168.8.33	**до** 192.168.8.62
192.168.8.64	192.168.8.95	**від** 192.168.8.65	**до** 192.168.8.94
192.168.8.96	192.168.8.127	**від** 192.168.8.97	**до** 192.168.8.126
192.168.8.128	192.168.8.159	**від** 192.168.8.129	**до** 192.168.8.158

1. Побудуємо мережу з 4-ма підмережами (див. рис. 2.1). Використовуйте модель маршрутизатора за замовчуванням – Generic.
2. Сконфігуруємо стек протоколів кожного вузла мережі відповідно з даними табл.2.3.
3. Здійснімо тестування мережі, використовуючи команду ping.

Таблиця 2.3 – Параметри стеку TCP/IP для вузлів мережі

Пристрій	IP-адреса	Маска	Шлюз
PC1	192.168.8.33	255.255.255.224	192.168.8.62
PC2	192.168.8.65	255.255.255.224	192.168.8.94
PC3	192.168.8.97	255.255.255.224	192.168.8.126
PC4	192.168.8.129	255.255.255.224	192.168.8.158
Server1	213.33.168.60	255.255.255.0	213.33.168.254
Router0(порт 0/0)	192.168.8.62	255.255.255.224	
Router0(порт 1/0)	192.168.8.94	255.255.255.224	
Router0(порт 6/0)	192.168.8.126	255.255.255.224	
Router0(порт 7/0)	192.168.8.158	255.255.255.224	
Router0(порт 8/0)	213.33.168.254	255.255.255.0	

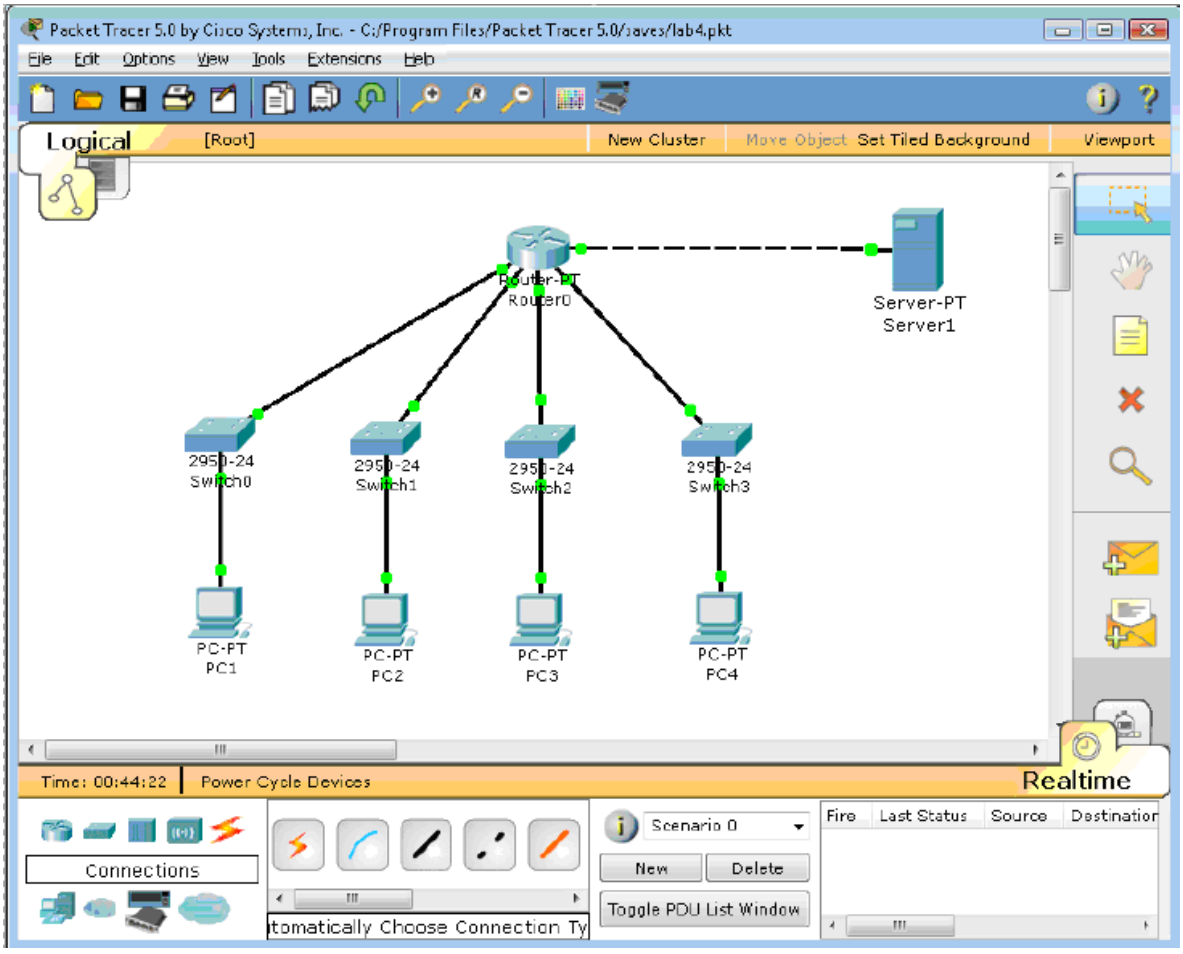


Рисунок 2.1 – Конфігурація мережі з 4-ма підмережами

Нижче приведений порядок конфігурування маршрутизатора за допомогою CLI Cisco IOS.

1. Для вибору мережевого пристрою Router0 натисніть в робочій області програми на його зображення. Відкриється вікно настройок мережевого пристрою. Вибираємо вкладку CLI для керування маршрутизатором.
2. В середині екрану ви побачити:
   Continue with configuration dialog? [yes/no]:
   Введіть “no” і натисніть клавішу <Enter>.
   З’явиться запрошення виду:
   Router>

Це означає, що ви підключені до мережевого пристрою і знаходитесь в командному рядку режиму користувача. Тут “Router” – це і’мя мережевого пристрою, а “>” позначає режим користувача.

3. Далі введіть команду enable, щоб потрапити в привілейований режим.
   Router> **enable**
   Router#
4. Перегляньте список доступних команд в привілейованому режимі:
   Router#?
5. Перейдемо в режим конфігурації:
   Router# config terminal
   Router(config)#
6. Ім’я хосту мережевого пристрою використовується для локальної ідентифікації. Коли ви входите до мережевого пристрою, ви бачите ім’я хосту перед символом режиму (“>” або “#”). Це ім’я може бути використано для визначення місця знаходження. Встановіть “ Router0” как ім’я вашого мереженого пристрою.
   Router(config)# **hostname Router0**
   Router0(config)#
7. Пароль доступу дозволяє контролювати доступ в привілейованому режимі. Це дуже важливий пароль, тому що в привілейованому режимі можна вносити зміни в конфігурації пристрою. Встановіть пароль доступу “cisco”
   Router0(config)#enable password cisco
8. Випробуємо цій пароль. Вийдіть з мережевого пристрою і спробуйте зайти в привілейований режим:
   Router0>en
   Password:*****
   Router0#
   Тут знаки: ***** - це ваш введений пароль. Ці знаки на екрані не видно.

2.2.1 Основні Show команди

Перейдіть до контексту користувача командою disable. Введіть команду для перегляду всіх доступних show команд.

Router0>**show ?**

1. Команда show version використовується для отримання типу платформи мережевого пристрою, версії операційної системи, імені файла образу операційної системи, часу роботи системи, об'єму пам'яті, кількості інтерфейсів і регістру конфігурації.

2. Можна побачити часи

Router0>**show clock**

3. В флеш-пам'яті мережевого пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від операційної пам'яті, в реальних устаткуваннях флеш-пам'ять зберігає файл-образ навіть при перебої живлення.

Router0>**show flash**

4. Інтерфейс командного рядка мереженого пристрою за замовчуванням зберігає 10 останніх введених команд

Router0>**show history**

5. Дві команди дозволяють повернуться до команд, що були введених раніше. Натисніть на стрілку вгору або <ctrl>P.

6. Дві команди дозволяють перейти до наступної команди, яка зберігається в буфері. Натисніть на стрілку вниз або <ctrl>N.

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

Router0>**show hosts**

8. Наступна команда виводить детальну інформацію про кожний інтерфейс:

Router0>**show interfaces**

9. Команда

Router0>**show sessions**

Виведе інформацію про кожну telnet сесію.

10.Команда

Router0>**show terminal**

показує параметри конфігурації терміналу.

11.Список всіх користувачів, приєднаних до пристрою по термінальних лініях можна побачити, використовуючи команду:

Router0>**show users**

12.Команда

Router0>**show controllers**

показує стан контролерів інтерфейсів.

13. Перейдемо до привілейованого режиму

Router0>en

14. Введіть команд для перегляду всіх доступних show команд.

Router0# show ?

Привілейований режим включає до себе всі show команди контексту користувача і ряд нових.

15. Подивимося активну конфігурацію в пам'яті мереженого пристрою.

Router0# show running-config

Активна конфігурація автоматично не зберігається і буде втрачена в разі перебою живлення. Для продовження перегляду наступної сторінки конфігурації натисніть на клавішу пробіл.

16. Наступна команда дозволяє переглянути поточний стан протоколів третього рівня

Router0# **show protocols**

2.2.2 Конфігурація інтерфейсів

Розглянемо команди, які дозволяють вмикати (піднімати) інтерфейси мережевого пристрою та переводити їх в стан UP.

1. На мережевому пристрої Router0 увійдемо в контекст конфігурації

Router0#**conf t**

Router0(config)#

2. Щоб настроїти Ethernet інтерфейс, треба зайти в контекст конфігурації інтерфейсу:

Router0(config)#**interface FastEthernet 0/0**

Router0(config-if)#

3. Переглянемо усі доступні в цьому контексті команди

Router0(config-if)#**?**

Для виходу в контекст глобальної конфігурації наберіть exit. Знову увійдіть в контекст конфігурації інтерфейсу:

Router0(config)#**int fa0/0**

Ми використали скорочене ім'я інтерфейсу.

4. Встановимо IP адресу Ethernet інтерфейсу

Router0(config-if)#**ip address 192.168.8.62 255.255.255.224**

5. Увімкнемо цей інтерфейс

Router0(config-if)#**no shutdown**

6. Додамо до інтерфейсу опис:

Router0(config-if)#**description Ethernet interface on Router 0**

Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду show interface.

Router0(config-if)#**end**

Router0# **show interface**

7. Після того, як виконано конфігурування усіх інтерфейсів можна переглянути активну конфігурацію пристрою і переконатися, що з'явилися призначені IP - адреси

Router0# **show running-config**

8. Перегляньте детальну IP інформацію про кожний інтерфейс та переконайтеся, що інтерфейси, що були сконфігуровані, перейшли до стану UP

Router0# **show ip interface**

Коротку інформацію можна отримати командою show ip interface brief

Router0# **show ip in bri**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	194.138.33.62	YES	manual	up	up
FastEthernet1/0	194.138.33.94	YES	manual	up	up
Serial2/0	unassigned	YES	unset	administratively down	down
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down
FastEthernet6/0	194.138.33.126	YES	manual	up	up
FastEthernet7/0	194.138.33.158	YES	manual	up	up
FastEthernet8/0	213.33.168.254	YES	manual	up	up
FastEthernet9/0	unassigned	YES	unset	administratively down	down

2.3 Контрольні питання

1. Які є контексти вводу команд в командному рядку?
2. Як перемикатися між контекстами вводу команд в командному рядку?
3. Яку роль виконує клавіша табуляції при вводі команд?
4. Як увійти до режиму глобальної конфігурації, активізувати частинний вигляд конфігурації та вийти з цих режимів?
5. Як орієнтуватися в командах, що були введені раніше, і повторювати їх?
6. Як задати ім'я хоста?
7. Яку інформацію можна переглянути командами show в контексті користувача?

8. Яку інформацію можна переоглянути командами show в привілейованому режимі, але неможна переглянути в режимі користувача?
9. Як підняти інтерфейс і визначити його стан?
10. Як призначити IP адресу на інтерфейсі і переконатися, що вона призначена?
11. Яка команда задає пароль на конфігурацію мережевого пристрою?

2.4 Перелік літератури

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. – 944 с.: ил.
2. Коломоец Г.П. Организация компьютерных сетей: учебное пособие. Запорожье: КПУ, 2012. – 156 с.
3. Кравец, О.Я. Практикум по вычислительным сетям и телекоммуникациям : учебное пособие / О. Я. Кравец. – Изд. 2-е, перераб. и доп. – Воронеж: Научная книга, 2006. – 156 с.

2.5 Варіанти завдань для самостійної роботи

1. Отримати у викладача варіант і розрахувати кількість підмереж згідно з даними табл.2.4.
2. Побудувати схему мережі згідно результатів попереднього розрахунку.
3. Сконфігурувати стек протоколів кожного вузла мережі.
4. Задати ім’я маршрутизатора, пароль на привілейований режим конфігурування, зберегти зміни у файлі стартової конфігурації.
5. За результатами роботи оформити звіт для другої частини.

Таблиця 2.4 – Варіанти завдання до другої частини лабораторної роботи

Варіант	IP-адреса	Маска	Завдання
1	194.138.33.0	/24	Розбити мережу на 4 підмережі
2	192.168.45.0	/24	Розбити мережу на 3 підмережі
3	82.207.118.0	/24	Розбити мережу на 5 підмережі
4	113.45.25.0	/24	Розбити мережу на 6 підмережі
5	164.34.24.0	/24	Розбити мережу на 5 підмережі
6	155.150.100.0	/24	Розбити мережу на 4 підмережі
7	164.90.34.0	/24	Розбити мережу на 3 підмережі
8	197.230.100.0	/24	Розбити мережу на 5 підмережі
9	87.217.118.0	/24	Розбити мережу на 6 підмережі

Варіант	IP-адреса	Маска	Завдання
10	182.207.120.0	/24	Розбити мережу на 4 підмережі
11	105.23.47.0	/24	Розбити мережу на 6 підмережі
12	97.13.45.0	/24	Розбити мережу на 3 підмережі

3. Прилади, устаткування та інструменти

Для виконання лабораторної роботи використовуються ПЕОМ, об'єднані в локальну мережу, програмний емулятор IP-мереж Cisco Packet Tracer.

4. Правила техніки безпеки та охорони праці

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

5. Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
5. Продемонструвати викладачу результати виконання завдання для самостійної роботи. Показати звіт про виконання команди ping з будь-якого комп’ютера на інший.
6. Оформити звіт.
7. Захистити звіт.

6. Оформлення та захист звіту

Звіт готується в електронному вигляді і роздруковується. Підготовленний до захисту звіт до лабораторної роботи повинен містити:

1. Найменування лабораторної роботи.
2. Відомості про виконавця, номер варіанту.
3. Завдання до лабораторної роботи.
4. Таблицю розрахованих адрес під мереж
5. Скріншот логічної структури мережі

6. Таблицю з параметрами стеку TCP/IP для вузлів мережі
7. Листинг команд конфігурування маршрутизатора в Cisco IOS (з файлу *.txt)
8. Скріншот виконання команди show ip interface brief
9. Скріншот виконання команди ping між будь-якими двома вузлами мережі
10. Скріншот завантаження HTTP сторінки на будь-який вузол з серверу.
11. Висновок

Лабораторна робота № 4

З’єднання з мережевими пристроями Cisco. Статична маршрутизація

1. Мета роботи

Метою лабораторної роботи є ознайомлення студентів з прийомами роботи з мережною операційною системою Cisco IOS та отримання навичок налаштування статичної маршрутизації на маршрутизаторах Cisco.

2. Завдання до лабораторної роботи

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Принципи роботи маршрутизаторів” і „Статична і динамічна маршрутизація”. Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

2.1 Cisco Discovery Protocol (CDP)

CDP дозволяє пристроям обмінюватися основною інформацією конфігурування. CDP буде працювати без настройки будь-якого протоколу. За замовчуванням CDP включений на всіх інтерфейсах. CDP працює на другому (канальному) рівні моделі OSI, тому він не є маршрутизованим протоколом і працює тільки з безпосередньо підключеними пристроями. Протокол CDP зв’язує фізичне середовище передачі даних більш низького рівня з протоколами більш високого мережевого рівня, тому пристрої, що підтримують різні протоколи третього рівня, можуть впізнавати один одного.

Під час запуску пристрою протокол CDP запускається автоматично. Після цього він може автоматично визначити сусідні пристрої, на яких також виконується протокол CDP. Серед знайдених пристроїв будуть не тільки ті, які працюють з протоколом IP.

CDP дозволяє адміністраторам мати доступ до даних про інший мережевий пристрій, до якого є безпосереднє з’єднання.

Для виводу інформації про сусідні пристрої, що виявлені за протоколом CDP, використовується сімейство команд **show cdp**. Воно виводить наступні дані по кожному порту і кожному пристрою, що з’єднаний з ним: ідентифікатори пристроїв, список адрес, ідентифікатор порту, перелік функціональних можливостей, апаратну платформу пристрою.

2.2 Команди ping і traceroute

Для діагностики можливості встановлення зв'язку в мережах використовуються протоколи типу запит-відповідь або протокол луна-пакетів. Результати роботи такого протоколу можуть допомогти в оцінці надійності путі до іншого пристрою, величин затримок в цілому і між проміжними пристроями. Для того щоб така команда працювала, необхідно, щоб не тільки локальний мережевий пристрій знав як потрапити до пункту призначення, але і щоб пристрій в пункті призначення знав, як дістатися до джерела.

Команда ping посилає ICMP(Internet Control Message Protocol) луна-пакети для верифікації з'єднання. У наведеному нижче прикладі час проходження одного луна-пакету перевищило заданий, про що свідчить точка (**.**) в інформації, що виведена, а чотири пакета пройшли успішно, про що свідчить знак оклику (**!**).

Switch> **ping 172.16.101.1**

Type escape sequence to abort.

Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:

.!!!!

Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms

Таблиця 2.1 – Результати команди ping

Символ	Значення
!	Успішний прийом луна-відповіді
.	Перевищений час очікування
U	Пункт призначення недосяжний
C	Перевантаження мережі
I	Виконання команди перервано адміністратором
?	Невідомий тип пакету
&	Пакет перевищив значення параметру часу життя TTL пакету

Команди traceroute показує адреси проміжних інтерфейсів (хопов) на путі пакетів в пункт призначення.

Switch> traceroute 172.16.101.1

Розширена версія команди ping підтримується тільки в привілейованому режимі (контекст адміністратора). Для того, щоб увійти в розширений режим, необхідно в рядку підсказки до Extended commands ввести букву «y» (Yes).

Команда в режимі діалогу опитує значення параметрів. Важливо відмітити, що ця команда дозволяє, знаходячись на одному пристрої, перевіряти зв'язок між мережевими інтерфейсами на інших пристроях.

```
Router# ping
Protocol [ip]:
Target IP address: 2.2.2.0
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data [no]:
Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]:
Sweep range of sizes [n]:
```

2.3 Команда telnet

Протокол віртуального термінала telnet, що входить до складу протоколів TCP/IP, дозволяє встановити з'єднання між мережевим пристроєм telnet клієнта і мережевим пристроєм telnet сервера, що забезпечує можливість роботи в режимі віртуального термінала. Telnet використовується для віддаленого керування мережевим пристроєм або для перевірки зв'язку на рівні додатків. Успішне встановлене telnet – з'єднання дозволяє керувати віддаленим пристроєм так, наче ви знаходитися за його консоллю. Мережеві пристрої Cisco здібні підтримувати одночасно до п'яті вхідних сеансів протоколу telnet.

2.4 Маршрутизація

Протоколи маршрутизації – це правила за якими здійснюється обмін інформації про шляхи передачі пакетів між маршрутизаторами. Протоколи характеризуються часом збіжності, втратами і маштабіруємістью. В даний час використовується декілька протоколів маршрутизації. Кожний протокол має свої достоїнства і недоліки.

Одна з головних задач маршрутизатора полягає в визначені найкращого шляху до заданого адресата. Маршрутизатор визначає шляхи (маршрути) до адресатів або із статичної конфігурації, введеної адміністратором, або динамічно на основі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизатори обмінюються маршрутною інформацією за допомогою протоколів маршрутизації. Маршрутизатор зберігає таблиці маршрутів в оперативній пам'яті. Таблиця маршрутів – це список найкращіх відомих доступних маршрутів. Маршрутизатор використовує цю таблицю для прийняття рішення, куди направляти пакет. Для перегляду таблиці маршрутів слід використовувати команду **show ip route**. Навіть, якщо на якомусь маршрутизаторі X не задавались ніякі команди маршрутизації, тоді він все одно будує таблицю маршрутів для безпосередньо приєднаних до нього мереж, наприклад:

…
C 192.168.4.0/24 is directly connected, Ethernet0
  10.0.0.0/16 is subnetted, 3 subnets
C 10.3.0.0 is directly connected, Serial0
C 10.4.0.0 is directly connected, Serial1
C 10.4.0.0 is directly connected, Ethernet1

Маршрут на безпосередньо приєднані мережі відображається на інтерфейс маршрутизатора, до якого вони приєднані. Тут /24 позначає маску 255.255.255.0, а /16 – 255.255.0.0.

Таблиця маршрутів відображає мережеві префікси (адреси мереж) на вихідні інтерфейси. Коли X одержує пакет, призначений для 192.168.4.46, він шукає префікс 192.168.4.0/24 в таблиці маршрутів. Згідно таблиці пакет буде направлений на інтерфейс Ethernet0. Якщо X отримує пакет для 10.3.21.5 он направить його на Serial0.

Ця таблиця показує чотири маршруту для безпосередньо приєднаних мереж. Вони мають мітку C. Маршрутизатор X відкидає всі пакети, що спрямовані до мереж, які не вказані в таблиці маршрутів. Для спрямування пакетів до інших адресатів необхідно в таблицю включити додаткові маршрути. Нові маршрути можуть бути додані двома методами:

Статична маршрутизація – адміністратор вручну визначає маршрути до мереж призначення.

Динамічна маршрутизація – маршрутизатори дотримуються правил, що визначаються протоколами маршрутизації, для обміну інформацією про маршрути і вибору найкращого шляху.

Статичні маршрути не змінюються самим маршрутизатором. Динамічні маршрути змінюються самим маршрутизатором автоматично при отриманні інформації про зміну маршрутів від сусідніх маршрутизаторів. Статична маршрутизація споживає мало обчислювальних ресурсів і корисна в мережах, які не мають декілька шляхів до адресату призначення. Якщо від маршрутизатора до маршрутизатора є тільки один шлях, то часто використовують статичну маршрутизацію.

Для конфігурації статичної маршрутизації Cisco використовують дві версії команди ip route

Перша версія

ip route АдресаМережіПризначення МаскаМережіПризначення Інтерфес

Команда вказує маршрутизатору, що всі пакети, які призначені для АдресаМережіПризначення-МаскаМережіПризначення слід направляти на свій інтерфейс Інтерфес. Якщо інтерфейс Інтерфес – типа Ethernet, то фізичні (MAC) адреси вихідних пакетів будуть широкомовними.

Друга версія

ip route АдресаМережіПризначення МаскаМережіПризначення Адреса

Команда вказує маршрутизатору, що всі пакети, які призначені для АдресаМережіПризначення-МаскаМережіПризначення, слід направляти на той свій інтерфейс, з якого досяжна IP адреса Адреса. Як правіло, **Адреса** це адреса наступного хопа по шляху до **Ошибка! Ошибка связи.**. Вихідний інтерфейс і фізичні адреси вихідних пакетів визначаються маршрутизатором за своїми ARP таблицями на підставі IP адрес Адреса. Наприклад

ip route 10.6.0.0 255.255.0.0 Serial1 (1)

ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

Перший приклад відображає мережевий префікс 10.6.0.0/16 на локальний інтерфейс маршрутизатора Serial1. Наступний приклад відображає мережевий префікс 10.7.0.0/16 на IP адресу 10.4.0.2 наступного хопа по шляху до 10.7.0.0/16. Обидві ці команді додадуть статичні маршрути в таблицю маршрутизації (мітка S):

S 10.6.0.0 via Serial1

S 10.7.0.0 [1/0] via 10.4.0.2

Коли інтерфейс падає, всі статичні маршрути, що відображаються на цей інтерфейс, видаляються з таблиці маршрутов. Якщо маршрутизатор не може більше знайти адресу наступного хопу по шляху до адреси, вказаної в статичному маршруті, то маршрут виключається з таблиці.

Зауважимо, що для мереж типа Ethernet рекомендується завжди використовувати формулу (2) команди ip route. Ethernet інтерфейс на маршрутизаторі, як правило, з'єднаний з декількома Ethernet інтерфейсами інших пристроїв в мережі. Вказівка в команді ip route IP адреси дозволить маршрутизатору вірно сформувати фізичну адресу вихідного пакету по своїм ARP таблицям.

2.5 Маршрутизація за замовчуванням

Зовсім не обов'язково, щоб кожний маршрутизатор обслуговував маршрути до всіх можливих мереж призначення. Замість цього маршрутизатор зберігає маршрут за замовчуванням або шлюз останнього пристановища (last resort). Маршрут за замовчанням використовується, коли маршрутизатор не може поставити у відповідність мережі призначення рядок в таблиці маршрутів. Маршрутизатор повинен використовувати маршрут за замовчанням для відсилання пакетів іншому маршрутизатору. Наступний маршрутизатор буде мати маршрут до цієї мережі призначення або мати свій маршрут за замовчуванням до третього маршрутизатора і т.д. В кінцевому рахунку, пакет буде маршрутизований на маршрутизатор, який має маршрут до мережі призначення.

Маршрут за замовчуванням може бути статично введений адміністратором або динамічно отриманий з протоколу маршрутизації.

Так як всі IP адреси належать мережі 0.0.0.0 з маскою 0.0.0.0, то в найпростішому випадку требі використовувати команду

ip route 0.0.0.0 0.0.0.0 [адреса наступного хопа | вихідний інтерфейс]

Ручне завдання маршруту за замовчуванням на кожному маршрутизаторі підходить для простих мереж. В складних мережах необхідно організовувати динамічний обмін маршрутами за замовчуванням.

2.6 Інтерфейс петля

На мережевих пристроях можна створювати інтерфейси не зв'язані з реальними каналами для передачі даних і призначати на них IP адреси з

масками. Такі інтерфейси називають петлями (loopback). Це чисто програмний інтерфейс, який тільки емулює роботу фізичного інтерфейсу. Він може використовуватися для віддаленого адміністрування і його функціонування не буде залежати від стану фізичних інтерфейсів, він буде завжди піднятий і доступний для будь-яких сесій. Петлі корисні при поетапному проектуванні мереж. Якщо до якогось реального мережевого інтерфейсу маршрутизатора в подальшому буде приєднана підмережа, то з початку на маршрутизаторі створюється loopback, налаштовується в плані взаємодії з іншими ділянками мережі і лише потім змінюється на реальний інтерфейс. Інтерфейс петля з'являється після команди interface loopbackN або скорочено int lN, де N ціле невід'ємне число – номер петлі.

Наприклад

Router(config)# **int loopback 10**

Router(config-if)#**ip address 1.1.1.1 255.0.0.0**

2.7 Команда trace

Команда trace є ідеальним засобом для з'ясування того, куди відправляються дані в мережі. Ця команда використовує ту ж технологію протоколу ICMP, що і команда ping, тільки замість перевірки наскрізного зв'язку між відправником і одержувачем, вона перевіряє кожний крок на шляху. Команда trace використовує здатність маршрутизаторів генерувати повідомлення про помилки при перевищенні пакетом свого встановленого часу життя (Time To Live, TTL). Ця команда посилає декілька пакетів і виводить на екран дані про час проходження туди і назад для кожного з них. Перевага команді **Ошибка! Ошибка связи.** полягає в тому, що вона показує черговий досягнутий маршрутизатор на шляху до пункту призначення. Це дуже потужний засіб для локалізації відмов на шляху від відправника до одержувача.

Таблиця 2.2 – Варіанти відповідей утиліти trace

Символ	Значення
!H	Зондуючий пакет був прийнятий маршрутизатором, але не переадресований, що звичайно буває через список доступу
P	Протокол недосяжний
N	Мережа недосяжна
U	Порт недосяжний
*	Перевищення межі очікування

2.8 Хід роботи

1. Створіть в Packet Tracer топологію, зображену на рис.2.1 з використанням моделі маршрутизатора за замовчуванням – Generic. Назвіть пристрої так, як на схемі: Router 1, Router 2 і Router 4.

Чорна лінія означає Ethernet з'єднання. Червона – послідовне з'єднання. Для створення послідовного з'єднання обираємо послідовне з'єднання точка-точка (serial cable). Обираємо другий пристрій. Визначаємо, який маршрутизатор буде виконувати функції DCE пристрою. Цій пристрій задає синхронізацію. В емуляторі для нього необхідно буде визначити частоту синхронізації.

Збережіть топологію.

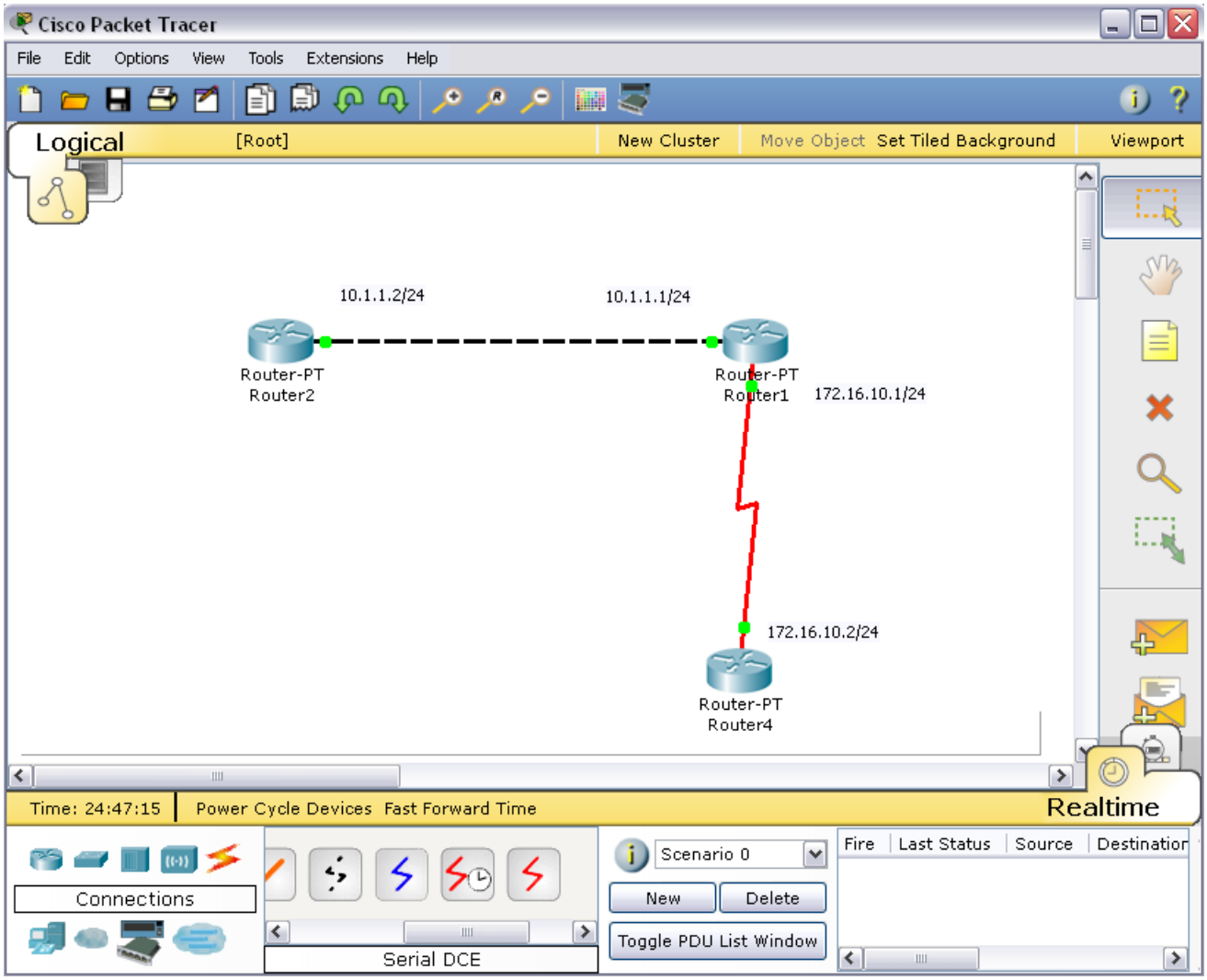


Рисунок 2.1 – Топологія мережі для моделювання

2. Командою hostname змініть імена маршрутизаторів. Задайте конфігурацію їх інтерфейсів відповідно з рисунком. Увімкніть інтерфейси. Конфігурацію послідовних інтерфейсів виконайте в наступній послідовності:

2.1 Зайдемо на Router1. Перевіримо, яким пристроєм виступає маршрутизатор для послідовної лінії зв'язку: кінцевим пристроєм DTE (data terminal equipment) або пристроєм зв'язку DCE (data circuit).

Router1#**show controllers S2/0**

Якщо бачити - **….DCE cable….-** , то цей маршрутизатор є пристроєм зв'язку і він повинен задавати частоту синхронізації тактових імпульсів, що використовуються при передачі даних. Частота обирається з певного ряду частот.

Router1#conf t

Router1(config)#int s2/0

Router1(config-if)#clock rate ?

Обираємо частоту 64000

Router1(config-if)#clock rate 64000

і подимаємо інтерфейс

Router1(config-if)#no shut

2.2 Перейдемо до маршрутизатора Router 4. Піднімімо на ньому інтерфейс serial2/0. Коли інтерфейси на двох кінцях послідовного з'єднання включені, на екрані з'явиться повідомлення про зміну стану інтерфейсу на активний.

2.3 Перевіримо на кожному пристрої, що інтерфейси, які були сконфігуровані, знаходяться в стані UP.

Router1#**sh int s2/0**

Router1#**sh int fa0/0**

Router2#**sh int fa0/0**

Router4#**sh int s2/0**

3. На кожному пристрої подивіться вашу активну конфігурацію і переконайтеся, що там з'явилися призначені IP адреси.

Router1#**show running-config**

Router2#**show running-config**

Router4#**show running-config**

4. Подивіться детальну IP інформацію про кожний інтерфейс і переконайтеся, що інтерфейси, які були сконфігуровані, перейшли у стан UP

Router1#**show ip interface**

Router2#**show ip interface**

Router4#**show ip interface**

5. Скорочену інформацію можна отримати командою show ip interface brief

Router1#**show ip in bri**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.1.1	YES	manual	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	172.16.10.1	YES	manual	up	up
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

Router2#**show ip in bri**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.1.2	YES	manual	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	unassigned	YES	unset	administratively down	down
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

Router4#**show ip in bri**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet1/0	unassigned	YES	unset	administratively down	down
Serial2/0	172.16.10.2	YES	manual	up	up
Serial3/0	unassigned	YES	unset	administratively down	down
FastEthernet4/0	unassigned	YES	unset	administratively down	down
FastEthernet5/0	unassigned	YES	unset	administratively down	down

2.8.1 Протокол CDP

1. На маршрутизаторі Router1 введемо команду для виводу стану всіх інтерфейсів на яких працює CDP.

Router1#show cdp interface

Треба переконатися, що обидва інтерфейсу підняти і посилають CDP пакети.

FastEthernet0/0 is up, line protocol is up

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

Serial2/0 is up, line protocol is up

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

2. Переконавшись, що мережевий пристрій посилає і одержує CDP-оновлення, можемо використовувати CDP для отримання інформації про безпосередньо підключені пристрої. Введіть команду

Router1#**show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Router2	Fas 0/0	121	R	PT1000	Fas 0/0
Router4	Ser 2/0	129	R	PT1000	Ser 2/0

Як можна побачити, маршрутизатор Router1 з'єднаний з інтерфейсом Fas 0/0 **(Port ID)** маршрутизатора **(Capability)** Router2 **(Device ID)** серії 1000 **(Platform)** через інтерфейс Fas 0/0 **(Local Intrfce)** і з інтерфейсом Ser 2/0 маршрутизатора Router4 серії 1000 через інтерфейс Ser 2/0.

3. На Router1 введіть команду для більш детальної інформації про сусідів

Router1#**show cdp neighbors detail**

Ця команда показує по одному пристрою за раз. Вона використовується для відображення адресної інформації мережевого рівня. В даний момент цей рівень у нас не налаштований, тому поле Entry address(es) пусте. Команда також виводить інформацію про версію IOS.

4. На Router1 введіть команду, щоб дізнатися інформацію про пристрій Router 4

Router1#**show cdp entry Router4**

Ця команда дає ту ж саму інформацію що і show cdp neighbors detail, але для одного конкретного пристрою. Пам'ятайте, що імена хостів чутливі до регістру.

5. На пристрої Router1 введіть команду, щоб побачити, як часто Router1 посилає сусідам оновлення CDP і як довго у сусідів вони повинні зберігатися.

Router1#**show cdp**

Global CDP information:

Sending CDP packets every 60 seconds

Sending a holdtime value of 180 seconds

Sending CDPv2 advertisements is enabled

Для економії смуги пропускання низько швидкісних пристроїв CDP можна відключити

Router1(config)# **no cdp run**

і знову вимкнути для усього пристрою

Router1(config)# **cdp run**

6. Іноді необхідно відключити CDP для певного інтерфейсу, наприклад при його вузький смуги пропускання або в цілях безпеки. На пристрої Router1 відключити CDP на інтерфейсі FastEthernet 0/0.

Router1(config)#**interface fa0/0**

Router1(config-if)#**no cdp enable**

Router1(config)#**Ctrl-Z**

Router1(config)#**show cdp interface**

В отриманому виводі ви не побачити відомостей про FastEthernet 0/0.

2.8.2 Команди ping і traceroute

1. Підключимося до пристрою Router1. Пропінгуємо безпосередньо приєднаний інтерфейс FastEthernet 0/0 на пристрої Router2

Router1#**ping 10.1.1.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 18/28/32 ms

Спробуємо пропінгувати інтерфейс Serial 2/0 на пристрої Router4

Router1#**ping 172.16.10.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms

Успішно.

2. Перейдемо на Router2. Спробуйте пропінгувати адрес 10.1.1.1 безпосередньо приєднаного FastEthernet 0/0 інтерфейсу на пристрої Router1. Успішно.

Перейдемо на Router4. Спробуйте пропінгувати адрес 172.16.10.1 безпосередньо приєднаного інтерфейсу Serial 2/0 на пристрої Router1. Успішно.

Спробуємо пропінгувати інтерфейс FastEthernet 0/0 на пристрої Router1:

Router4#**ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Невдача.

Спробуємо пропінгувати адресу 10.1.1.2 FastEthernet 0/0 інтерфейсу на пристрої Router2. Невдача.

3. Повернемося на Router2. Спробуємо пропінгувати адресу 172.16.10.1 інтерфейсу Serial 2/0 на пристрої Router1. Невдача. Спробуємо пропінгувати адресу 172.16.10.2 інтерфейсу Serial 2/0 на пристрої Router4. Невдача.

Невдачі спіткали нас тому, що ми не налаштували на маршрутизаторах маршрутизацію!

4. Зайдіть на пристрій Router1. Визначте шляхи проходження пакетів на Router2

Router1# **traceroute 10.1.1.2**

і Router4

Router1# **traceroute 172.16.10.2**

Ви повинні побачити по одному хопу.

5. Виконайте команду розширеного пінга від адреси 10.1.1.2 до адреси 172.16.10.2

Router1#**ping**

…

Target IP address: 172.16.10.2

…

Extended commands [n]: **y**

Source address: 10.1.1.2

…

2.8.3 Telnet

Будьте уважні: емулятор має обмежену підтримку telnet.

1. Увійдіть на пристрій Router1. Нам необхідно, щоб мережений пристрій приймав telnet-сесії і був захищений паролем. Кожна так звана лінія в мережевому пристрої потенційно представляє активну telnet-сесію, яку пристрій може підтримувати. Наші мережеві пристрої підтримують до 5 ліній, призначені на віртуальні термінали vty. Ми використовуємо всі 5 ліній

Router1(config)#**line vty 0 4**

Router1(config-line)#

2. Далі повідомимо мережевому пристрою, що нам знадобиться пароль входу в систему.

Router1(config-line)#**login**

Router1(config-line)#**password parol**

3. Увійдемо на пристрій Router2 і встановимо telnet – з'єднання з пристроєм Router1. Для цього ми використовуємо IP адресу його інтерфейсу FastEthernet 0/0

Router2#**telnet 10.1.1.1**

4. Ми побачимо запрошення ввести пароль. Введіть пароль parol і натисніть <enter>. Зауважте, що ім'я мережевого пристрою змінилося на Router1, тому що ми встановили telnet – з'єднання з Router1. Команда

Router1>**show user**

* 67 vty 0 idle 00:00:00 10.1.1.2

покаже, що з'єднання здійснено від адреси 10.1.1.2 пристрою Router2.

На секунду натисніть одночасно клавіші **<Ctrl>+<Shift>+6**, потім відпустить і зразу натисніть клавішу **x**. Ім'я мережевого пристрою змінилося знову на Router2. Тобто зараз ми на пристрої Router2.

Router1#**<Ctrl>+<Shift>+<6>** потім **x**

Router2#

5. Введіть команду show sessions. Це дозволить побачити всі активні telnet – сесії. Щоб відновити telnet – сесію визначте номер сесії, яку ви хочете відновити (у нашому випадку є тільки одна з номером 1) і введіть команду resume 1.

Router2#**show sessions**

Conn Host Address Byte Idle Conn Name

* 1 10.1.1.1 10.1.1.1 0 1 10.1.1.1

Router2#**resume 1**

Router1#

6. Ім'я хоста знову змінилося на Router1. Натисніть комбінацію <Ctrl>+<Shift>+<6> і клавішу x, щоб повернутися назад на Router2.

Router1#**<Ctrl>+<Shift>+<6>** потім **x**

Router2#

7. Закрийте сесію

Router2#disconnect 1

Closing connection to 10.1.1.1 [confirm]

2.8.4 Протокол ARP

1. Приєднайтеся до маршрутизатора Router1 і подивіться його ARP таблицю

Router1#**show arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.1.1.1 - 0002.4AD6.5391 ARPA FastEthernet0/0

Вона містить тільки один рядок про MAC адресу свого Ethernet інтерфейсу з IP адресою 10.1.1.1.

2. Приєднайтеся до маршрутизатора Router2 і подивіться його ARP таблицю. Вона містить тільки один рядок про MAC адресу свого Ethernet інтерфейсу з IP адресою 10.1.1.2

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.1.1.2 - 0001.C779.8AB5 ARPA FastEthernet0/0

3. Пропінгуйте Ethernet інтерфейс маршрутизатора Router1

Router2# ping 10.1.1.1

4. Знову подивіться ARP таблицю. Вона містить вже два рядка. З'явився запис про MAC адресу Ethernet інтерфейсу Router1 з IP адресою 10.1.1.1.

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.1.1.1 2 0002.4AD6.5391 ARPA FastEthernet0/0

Internet 10.1.1.2 - 0001.C779.8AB5 ARPA FastEthernet0/0

5. Приєднайтеся до маршрутизатора Router2 і подивіться його ARP таблицю. Вона містить вже два рядки

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.1.1.1 - 0002.4AD6.5391 ARPA FastEthernet0/0

Internet 10.1.1.2 4 0001.C779.8AB5 ARPA FastEthernet0/0

З'явився запис про MAC адресу Ethernet інтерфейсу маршрутизатора Router2 з IP адресою 10.1.1.2. Чому, адже ми не слали від Router1 ніяких IP пакетів? Тому що Router1 для відповіді на пінг від Router2 повинен був знати про MAC адресу Ethernet інтерфейсу маршрутизатора Router2 з IP адресою 10.1.1.2, і він сформував ARP пакет для його отримання.

2.8.5 Статичні маршрути

Раніше ми не могли з маршрутизаторів Router2 і Router4 пропінговати деякі інтерфейси через відсутність маршрутизації. Виправимо це.

1. Приєднайтесь до маршрутизатора Router2. Ми не могли пінговати адреси 172.16.10.1 і 172.16.10.2. Подивіться таблицю маршрутизації.

Router2#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

Ми бачимо безпосередньо приєднані мережі. Нема маршруту до мережі 172.16.10.0/24. Додамо маршрут до мережі 172.16.10.0/24 через адресу 10.1.1.1 найближчого хопа на шляху до цієї мережі:

Router2(config)#**ip route 172.16.10.0 255.255.255.0 10.1.1.1**

Тут і далі 172.16.10.0/24 – це скорочений запис – визначення підмережі 172.16.10.0 з маскою 255.255.255.0. У масці 255.255.255.0 міститься 24 одиниці, що і позначається /24.

2. Успішно пропінгуємо Serial інтерфейс Router1

Router2#**ping 172.16.10.1**

Знову подивимося таблицю маршрутів

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

172.16.0.0/24 is subnetted, 1 subnets

S 172.16.10.0 [1/0] via 10.1.1.1

3. Але ми не зможемо пропінгувати Serial інтерфейс Router4

Router2#**ping 172.16.10.2**

Чому? Тому що ICMP пакети пінгів не знають, як їм повернутися назад від Router4, оскільки на Router4 не прописані маршрути.

4. Приєднайтеся до маршрутизатора Router4. Подивіться таблицю маршрутів

Router4#**show ip route**

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.10.0 is directly connected, Serial2/0

Нема маршруту до мережі 10.1.1.0/24. Додамо маршрут до мережі 10.1.1.0/24 через адресу 172.16.10.1 найближчого хопа на шляху до цієї мережі:

Router4(config)#**ip route 10.1.1.0 255.255.255.0 172.16.10.1**

Знову подивимося таблицю маршрутів

10.0.0.0/24 is subnetted, 1 subnets

S 10.1.1.0 [1/0] via 172.16.10.1

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.10.0 is directly connected, Serial2/0

5. Зараз всі мережеві інтерфейси в мережі пінгуються з кожного мережевого пристрою. Перевірте це.

2.8.6 Маршрутизація за замовчуванням

Мережеві пристрої Router2 і Router4 мають тільки по одному виходу у зовнішній світ: через інтерфейси з адресами 10.1.1.1 і 172.16.10.1, відповідно. Тому можна не визначати на які підмережі ми маршрутизуємо пакети і використовувати маршрутизацію за замовчуванням.

1. Спочатку видалимо старі маршрути

Router2(config)#**no ip route 172.16.10.0 255.255.255.0 10.1.1.1**

Router4(config)# **no ip route 10.1.1.0 255.255.255.0 172.16.10.1**

2. Далі призначимо маршрути за замовчуванням

Router2(config)#**ip route 0.0.0.0 0.0.0.0 10.1.1.1**

Router4(config)# **ip route 0.0.0.0 0.0.0.0 172.16.10.1**

3. Подивіться таблицю маршрутів на всіх пристроях.

Router2#**sh ip route**

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

S* 0.0.0.0/0 [1/0] via 10.1.1.1

Router4#**sh ip route**

Gateway of last resort is 172.16.10.1 to network 0.0.0.0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.10.0 is directly connected, Serial2/0

S* 0.0.0.0/0 [1/0] via 172.16.10.1

4. Всі мережеві інтерфейси в мережі пінгуються з кожного мережевого пристрою. Перевірте це.

2.8.7 Loopback

1. Визначимо інтерфейс петлю на пристрої Router4

Router4(config)# **int loopback 0**

Router4(config-if)#**ip address 1.1.1.1 255.255.255.0**

2. Пропишемо до пристрою Router1 маршрут на мережу петлі

Router1(config)# **ip route 1.1.1.0 255.255.255.0 172.16.10.2**

3. Приєднаємося до пристрою Router2 і пропінгуємо створену петлю

Router2#**ping 1.1.1.1**

Збережіть проект і конфігурацію кожного роутера окремо в текстовий файл.

2.9 Контрольні питання

1. Що таке CDP, для чого він служить і як їм користуватися?
2. Яку інформацію повертає команда ping?
3. Чи можна, знаходячись на одному пристрої, попарно пропінгувати всі пристрої в мережі?
4. Для чого служить команда traceroute?
5. Для чого служить протокол telnet?
6. Яким пристроєм може виступати маршрутизатор для послідовної лінії зв’язку?
7. На якому пристрої при послідовному з’єднанні можна встановлювати частоту синхронізації?
8. Чому можуть не проходити пінги між пристроями?
9. Як призупинити і відновити telnet – сесію?
10. Як закрити telnet з’єднання?
11. Як відправник дізнається MAC адресу одержувача?
12. Як подивиться ARP таблицю?
13. Коли в ARP таблиці з’являються нові рядки?
14. Що таке таблиця маршрутів? Якщо адміністратор не налаштовує ніяких маршрутів, то що вона буде містити?
15. Чим статична маршрутизація відрізняється від динамічної?
16. Які дві формі завдання статичної маршрутизації ви знаєте?

17. Як в команді маршрутизації визначається мережа призначення?
18. Чому для мереж типу Ethernet рекомендується завжди використовувати форму (2) команди маршрутизації?
19. Поясніть значення полів в командах маршрутизації.
20. Чому в якості поля Адреса рекомендують використовувати адресу наступного хопа по шляху до мережі призначення?
21. Коли використовується маршрутизація за замовчуванням?
22. Коли використовується інтерфейс петля?
23. Як працює команда трасіровки?

2.10 Перелік літератури

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. – 944 с.: ил.
2. Коломоец Г.П. Организация компьютерных сетей: учебное пособие. Запорожье: КПУ, 2012. – 156 с.
3. Кравец, О.Я. Практикум по вычислительным сетям и телекоммуникациям : учебное пособие / О. Я. Кравец. – Изд. 2-е, перераб. и доп. – Воронеж: Научная книга, 2006. – 156 с.

2.11 Варіанти завдань для самостійної роботи

1. Побудувати в Packet Tracer топологію, що представлена на рис.2.2. Використовувати необхідні маршрутизатори. В мережі шість підмереж, кожний маршрутизатор підключений до трьох підмереж.

2. На кожному маршрутизаторі підійміть інтерфейси, що використовуються, і подивіться сусідів командою show cdp neighbors. Зробіть скріншот.

3. Призначте інтерфейсам мережі адреси згідно рис.2.2 і табл..2.3, в котрих v – це номер варіанту. Всі маски 255.255.255.0. Не забудьте призначити шлюзи за замовчуванням для комп'ютерів згідно таблиці.

4. Перевірте факт призначення адрес шляхом виконання на кожному маршрутизаторі команд show running-config і show ip interface brief. Для комп'ютерів використовуйте команду ipconfig.

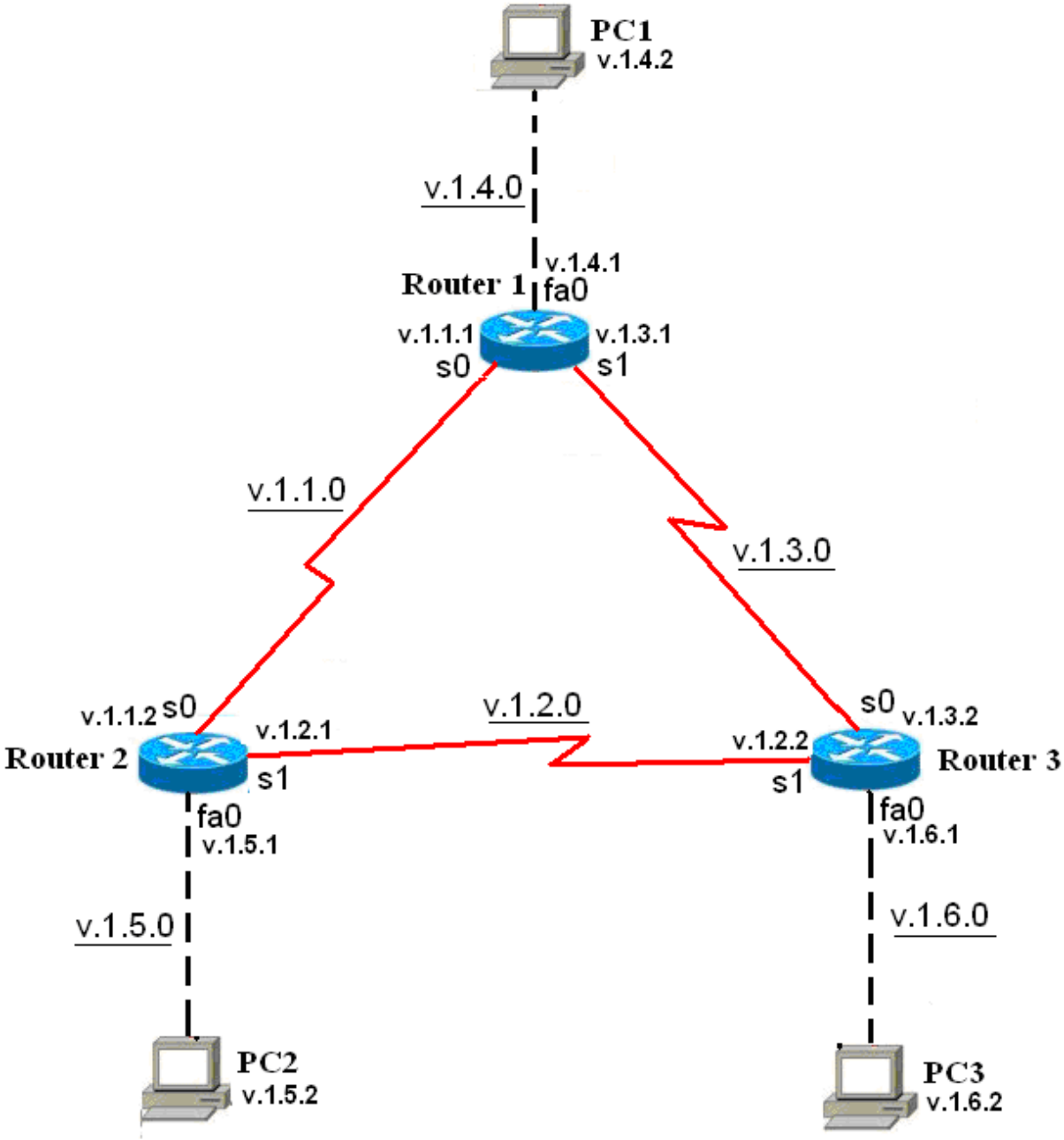


Рисунок 2.2 – Топологія мережі для виконання самостійної роботи

Таблиця 2.3 – Адреси інтерфейсів

Адреси підмереж	v.1.1.0	v.1.2.0	v.1.3.0	v.1.4.0	v.1.5.0	v.1.6.0
Router1	S0:v.1.1.1		S1:v.1.3.1	E0:v.1.4.1		
Router2	S0:v.1.1.2	S1:v.1.2.1			E0:v.1.5.1	
Router3		S0:v.1.2.2	S1:v.1.3.2			E0:v.1.6.1
PC1				E0:v.1.4.2		
PC2					E0:v.1.5.2	
PC3						E0:v.1.6.2

5. Перевірте правильність призначення адрес шляхом виконання на кожному маршрутизаторі команд ping до безпосередніх сусідів. Наприклад, на маршрутизаторі Router1 виконайте

Router1#ping v.1.1.2

Router1#ping v.1.3.2

Router1#ping v.1.4.2

6. Поставимо перед собою завдання зв'язати між собою комп'ютери PC1, PC2 і PC3. Для цього здійснимо на маршрутизаторах настройку статичної маршрутизації. В кожному маршрутизаторі пропишемо маршрути на віддалені Ethernet мережі. Для вирішення поставленого завдання маршрутизувати пакети на віддалені мережі послідовних з'єднань не треба.

У кожного маршрутизатора є по два маршруту на віддалені Ethernet мережі. Всього треба прописати шість статичних маршрутів.

Щоб з маршрутизатора Router1 досягти віддалену Ethernet мережу v.1.5.0/24, пакети можна направляти на IP адресу v.1.1.2 найближчого зовнішнього інтерфейсу на шляху в цю мережу. Це зробить команда

Router1(config)#ip route v.1.5.0 255.255.255.0 v.1.1.2

Задайте інші п'ять команд маршрутизації.

7. На кожному маршрутизаторі подивіться таблицю маршрутизації командою show ip route. Зробіть скріншоти.

8. На кожному маршрутизаторі зробить скріншоти розширених пінгів
   a) на маршрутизаторі Router1 від PC2 до PC3
   b) на маршрутизаторі Router2 від PC1 до PC3
   c) на маршрутизаторі Router3 від PC1 до PC2

Наприклад, результат розширеного пінгу на маршрутизаторі Router1 від PC2 до PC3 для варіанта 12 (v=12) має вигляд:

```
Router1#ping
Protocol [ip]:
Target IP address: 12.1.6.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.1.5.2
% Invalid source
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 62/62/63 ms
```

9. На кожному комп’ютері зробіть скріншоти виконання команд трасіровкі tracert інших комп’ютерів. Всього шість скріншотів. Наприклад, трасіровка з PC1 на PC2 для варіанта 12 (v=12)

```
PC>tracert 12.1.5.2
Tracing route to 12.1.5.2 over a maximum of 30 hops:
  1   17 ms     31 ms     32 ms     12.1.4.1
  2   47 ms     63 ms     63 ms     12.1.1.2
  3   94 ms     94 ms     78 ms     12.1.5.2
Trace complete.
```

10. Збережіть проект

3. Прилади, устаткування та інструменти

Для виконання лабораторної роботи використовуються ПЕОМ, об'єднані в локальну мережу, програмний емулятор IP-мереж Cisco Packet Tracer.

4. Правила техніки безпеки та охорони праці

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

5. Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Виконати в Packet Tracer практичну частину лабораторної роботи.
4. Отримати у викладача варіант і виконати в Packet Tracer завдання для самостійної роботи.
5. Продемонструвати викладачу результати виконання пунктів 8 і 9 завдання для самостійної роботи.
6. Оформити звіт.
7. Захистити звіт.

6. Оформлення та захист звіту

Звіт готується в електронному вигляді і роздруковується. Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Найменування лабораторної роботи.
2. Відомості про виконавця, номер варіанта.
3. Завдання до лабораторної роботи.
4. Скріншот топології, створеної при виконанні практичної частини
5. Конфігурації трьох маршрутизаторів з .txt файлів, створених при виконанні практичної частини.
6. Скріншот топології для свого варіанту з вказаними адресами.
7. Таблиця конфігурації згідно свого варіанту.
8. Конфігурації трьох маршрутизаторів з .txt файлів, створених при виконанні завдання для самостійної роботи.
9. Всі скріншоти, що вказані в завданні для самостійної роботи.

Лабораторна робота № 5

Технології локальних комп'ютерних мереж

1. Мета роботи

1. Вивчення особливостей методів доступу і специфікацій фізичного середовища базових технологій локальних мереж;
2. Отримання практичних навичок розрахунку конфігурації мережі Ethernet і Fast Ethernet.

2. Завдання до лабораторної роботи

Лабораторна робота спирається на знання й уміння, отримані при вивченні наступних тем лекційного курсу: „Технології локальних мереж" і „Стандарти технології Ethernet". Тому при підготовці до лабораторної роботи рекомендується повторити зазначені розділи дисципліни. Стислий конспект цього теоретичного матеріалу наводиться нижче.

2.1 Специфікації фізичного середовища Ethernet

Технологія Ethernet використовує метод доступу CSMA/CD - метод колективного доступу з впізнанням несучої та виявленням колізій. Випадковий метод доступу обумовлює наявність у мережі Ethernet колізій - ситуацій, коли дві станції одночасно намагаються передати кадр даних по загальній шині. Правильний вибір параметрів мережі, зокрема дотримання співвідношення між мінімальною довжиною кадру та максимально можливим діаметром мережі, дозволяє чітко розпізнавати колізію.

Фізичні специфікації технології Ethernet на сьогоднішній день включають наступні середовища передачі даних.

- **10 Base-5** – коаксіальний кабель діаметром 0,5 дюймів ("товстий" коаксіал). Має хвильовий опір 50 Ом. Максимальна довжина сегменту - 500 м (без повторювачів).
- **10 Base-2 –** коаксіальний кабель діаметром 0,25 дюйма ("тонкий" коаксіал). Має хвильовий опір 50 Ом. Максимальна довжина сегменту - 185 м (без повторювачів). Використання повторювачів для збільшення діаметра коаксіальних варіантів мереж підпорядковується правилу « 5-4-3».
- **10 Base-T –** кабель на основі неекранованої крученої пари (Unshielded Twisted Pair, UTP). Утворює зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом - не більше 100 м.

– **10 Base-F -** оптичний кабель. Топологія аналогічна топології стандарту 10 Base-T. Є кілька варіантів цієї специфікації - FOIRL (відстань до 1000 м), 10 Base-FL (відстань до 2000 м), 10 Base-FB (відстань до 2000 м). Використання повторювачів для збільшення діаметра мереж Ethernet, побудованих на крученій парі та на оптичному кабелі, підпорядковується правилу «4 хабів».

Загальні обмеження для всіх стандартів Ethernet і параметри специфікацій фізичного рівня для стандарту Ethernet наведені у табл.А.1 і табл. А.2 додатка А.

Число 10 у зазначених вище назвах позначає номінальну пропускну здатність мережі - 10 Мбіт/с, а слово "Base" - метод передачі на одній базовій частоті 10 Мгц (на відміну від методів, що використовують кілька несучих частот). Останній символ у назві стандарту фізичного рівня позначає тип кабелю.

2.2 Специфікації фізичного середовища Fast Ethernet

Стандарт Fast Ethernet IEEE 802.3u з'явився значно пізніше стандарту Ethernet – в 1995 році. Його розробка була пов'язана з вимогами підвищення швидкості передачі інформації.

Якщо порівнювати набір стандартних сегментів Ethernet і Fast Ethernet, то головна відмінність – відсутність в Fast Ethernet шинних сегментів і коаксіального кабелю. Залишилися лише сегменти на крученій парі і оптичному кабелі.

Фізичні специфікації технології Fast Ethernet включають наступні середовища передачі даних.

Параметр	100BASE-TX	100BASE-T4	100BASE-FX
Кабель	UTP кат.5	UTP кат. 3 або 5	Оптичний
Кіл-ть ВП	2	4	–
Довжина	100 м (90 м)	100 м (90 м)	412 м
Код	4B/5B + MLT-3	8B/6T	4B/5B + NRZI
Топологія	Пасивна зірка	Пасивна зірка	Пасивна зірка

– **100 Base-TX** – мережа з топологією пасивна зірка з концентратором в центрі. Використовується вита пара (UTP) категорії 5 або вище, що пов'язане з необхідною пропускною здатністю кабелю. Для приєднання кабелю використовуються 8-контактні рознімання типу RJ-45. Довжина кабелю не

може перевищувати 100 метрів (стандарт рекомендує 90 метрів для 10-відсоткового запасу). Стандарт передбачає також можливість використання екранованого кабелю з двома витими парами проводів (хвильовий опір – 150 Ом). В цьому випадку використовується 9-контактне екрановане рознімання DB-9. На сьогоднішній день 100 Base-TX самий популярний тип мережі Fast Ethernet.

– **100 Base-T4** – передача здійснюється не двома, а чотирма неекранованими витими парами (UTP). При цьому кабель може бути менш якісним (категорії 3, 4 або 5). Прийнята в 100BASE-T4 система кодування сигналів забезпечує ту ж саму швидкість 100 Мбіт/с на любому з цих кабелів, але стандарт рекомендує все ж використовувати кабель категорії 5. Обмін даними іде по одній передавальної витої парі, по одній приймальній витої парі і по двом двонаправленим витим парам з використанням трьохрівневих диференціальних сигналів.

– **100 Base-FX** – використовується топологія пасивна зірка з підключенням комп'ютерів до концентратору за допомогою двох різнонаправлених оптичних кабелів. Кабелі підключаються до адаптера (трансивера) і до концентратора за допомогою рознімань типу SC, ST бо FDDI. Максимальна довжина кабелю між комп'ютером і концентратором - 412 метрів (це обмеження визначається не якістю кабелю, а встановленими часовими співвідношеннями). Згідно стандарту, застосовується мультимодовий або одномодовий кабель з довжиною хвилі світла 1,35 мкм. В останньому випадку втрати потужності сигналу в сегменті (в кабелі и розніманнях) не повинні перевищувати 11 дБ.

2.3 Контрольні питання

1. Наведіть алгоритми роботи випадкового методу доступу CSMA/CD?
2. Опишіть методику розрахунку конфігурації Fast Ethernet.
3. У яких випадках у мережах Ethernet виникають колізії? Що таке домен колізій?
4. Опишіть характеристики та апаратуру сегменту 100 Base - TX.
5. Дайте характеристику та опис апаратури сегментів Gigabit Ethernet?

2.4 Перелік літератури

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб.: Питер, 2010. 944 с.: ил.
2. Коломоец Г.П. Организация компьютерных сетей: учебное пособие. Запорожье: КПУ, 2012. 156 с.

3. Новиков Ю.В. Основы локальных сетей: курс лекций : учеб. пособие: для студентов вузов, обучающихся по специальностям в обл. информ. технологий . М.: Интернет-ун-т информ. технологий, 2005. 360 с.

2.5 Варіанти завдань для самостійної роботи

2.5.1 Розрахунок конфігурації мережі Ethernet

Перевірте коректність конфігурації мережі Ethernet, представленої на рис.2.1. При розрахунку конфігурації мережі Ethernet необхідно використовувати дані, що представлені у додатку А.

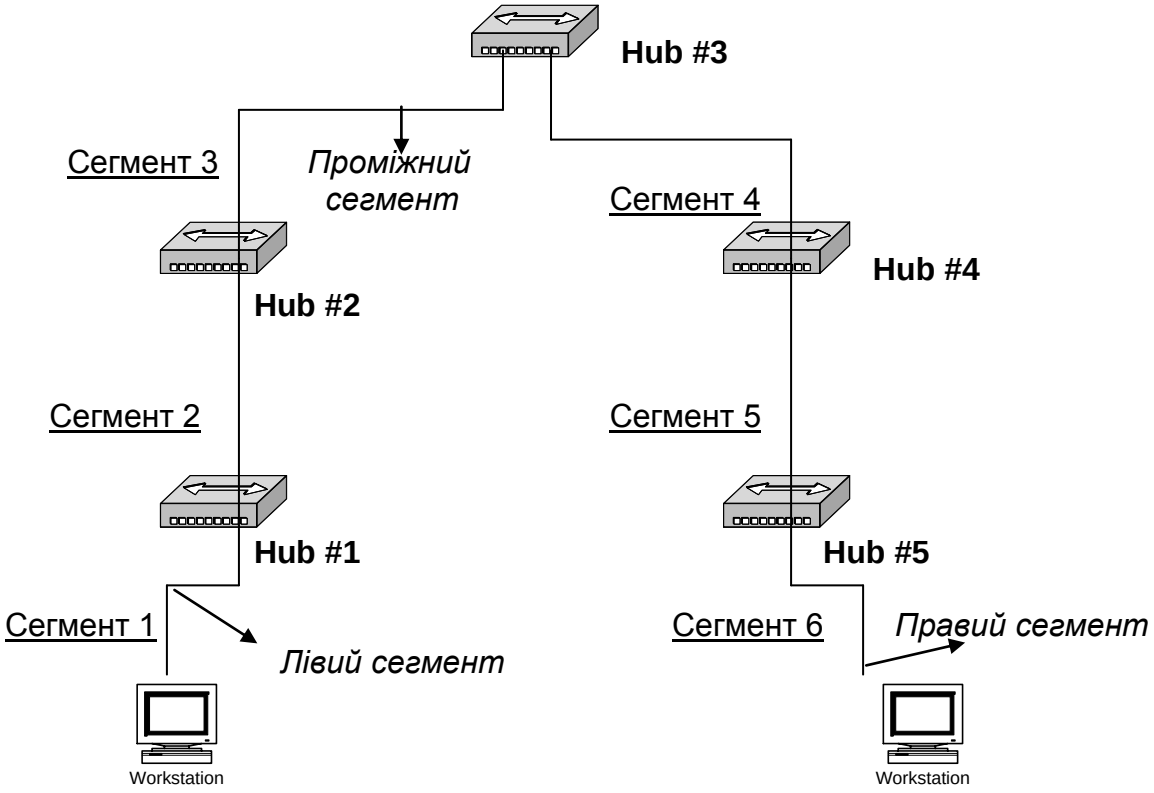


Рисунок 2.1 – Топологія мережі для розрахунку

Зауваження до розрахунку конфігурації мережі Ethernet:

Щоб мережа Ethernet, яка складається із сегментів різної фізичної природи, працювала коректно, необхідно виконання чотирьох основних умов:

- кількість станцій у мережі не більше 1024;
- максимальна довжина кожного фізичного сегмента не більше величини, що визначена відповідним стандартом фізичного рівня;
- час подвійного обороту сигналу (Path Delay Value, PDV) між двома самими далекими станціями мережі не більше 512 бітових інтервалів (bt);

- скорочення міжкадрового інтервалу IPG (Path Variability Value, PVV) при проходженні послідовності кадрів через всі повторювачі повинне бути не більше, ніж 49 бітових інтервалів (bt).

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування, що визначають максимальну кількість повторювачів і загальну довжину мережі в 2500 м.

Таблиця 2.1 – Варіанти завдань для розрахунку (сегменти мережі на рис.2.1)

Варіант	Тип сегмента					
	сегмент 1	сегмент 2	сегмент 3	сегмент 4	сегмент 5	сегмент 6
1	80м, 10Base-T	100м, 10Base-T	1500м, 10Base-FB	500м, 10Base-FB	100м, 10Base-T	60м, 10Base-T
2	100м, 10Base-FL	1000м, 10Base-FL	200м, 10Base-FB	500м, 10Base-FB	1000м, 10Base-FL	80м, 10Base-T
3	60м, 10Base-T	500м, 10Base-FB	400м, 10Base-FL	600м, 10Base-FB	600м, 10Base-FL	1000м, 10Base-FL
4	1000м, 10Base-FL	60м, 10Base-T	700м, 10Base-FB	50м, 10Base-T	1200м, 10Base-FB	1500м, 10Base-FL
5	90м, 10Base-T	1000м, 10Base-FL	80м, 10Base-T	500м, 10Base-FB	70м, 10Base-T	500м, 10Base-FL
6	1400м, 10Base-FL	800м, 10Base-FB	1800м, 10Base-FB	500м, 10Base-FB	500м, 10Base-FB	60м, 10Base-T
7	80м, 10Base-T	100м, 10Base-T	1100м, 10Base-FL	800м, 10Base-FL	80м, 10Base-T	1000м, 10Base-FL
8	800м, 10Base-FL	1200м, 10Base-FB	700м, 10Base-FB	700м, 10Base-FB	700м, 10Base-FL	100м, 10Base-T
9	80м, 10Base-T	50м, 10Base-T	1100м, 10Base-FB	600м, 10Base-FL	50м, 10Base-T	1200м, 10Base-FL
10	750м, 10Base-FL	500м, 10Base-FB	1000м, 10Base-FL	60м, 10Base-T	900м, 10Base-FB	75м, 10Base-T

2.5.2 Розрахунок конфігурації мережі Fast Ethernet

Виконайте завдання на розрахунок конфігурації мережі Fast Ethernet. Використовуйте відповідні схеми підключення и дані, що наведені в завданнях. Моделі за якими проводять розрахунки конфігурації і табличні дані стандарту наведені у додатку Б. Обов'язково зробіть висновки після всіх розрахунків.

Завдання 1. Мережа складається з двох повторювачів класу II і сегментів різного стандарту, як показано на рис. 2.2. Відстань між повторювачами (B) і довжини сегментів A і C надані в табл.2.2. В табл.2.2 також вказано, який стандарт кабелю використовується в даному сегменті.

Визначити максимальну відстань D, на якій можна встановити комутатор.

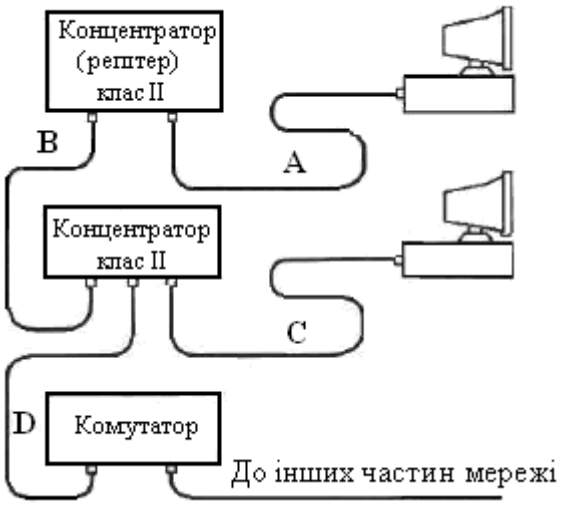


Рисунок 2.2 – Топологія мережі для завдання 1

Таблиця 2.2 – Варіанти завдання 1

Варіант	Всі сегменти стандарту	Довжини сегментів, м		
		A	B	C
1	100Base-T4	90	10	80
2	100Base-FX	50	15	10
3	100Base-TX	100	5	100
4	100Base-T4	50	20	30
5	100Base-FX	60	25	40
6	100Base-TX	70	7	20
7	100Base-T4	80	12	50
8	100Base-FX	90	15	30
9	100Base-TX	40	17	50
10	100Base-T4	10	20	90

Завдання 2. Є повторювач класу I. До нього підключені сегменти Tx, T4 як показано на рис.2.3. Всі довжини сегментів A, B, C, D, E, F наведені в табл.2.3.

a) Перевірте, чи буде відповідати дана мережа умовам коректної мережі.

Необхідно підключити до цієї мережі один сегмент оптики Fx.

b) Яка буде максимальна довжина цього сегменту (x)?

Необхідно підключити додатково ще один сегмент Fx.

c) Розрахуйте максимальну довжину і для цього сегменту Fx (y).

ЗАУВАЖЕННЯ. У кожному із завдань мається на увазі, що при підключенні нового сегмента, інші залишаються працездатними.

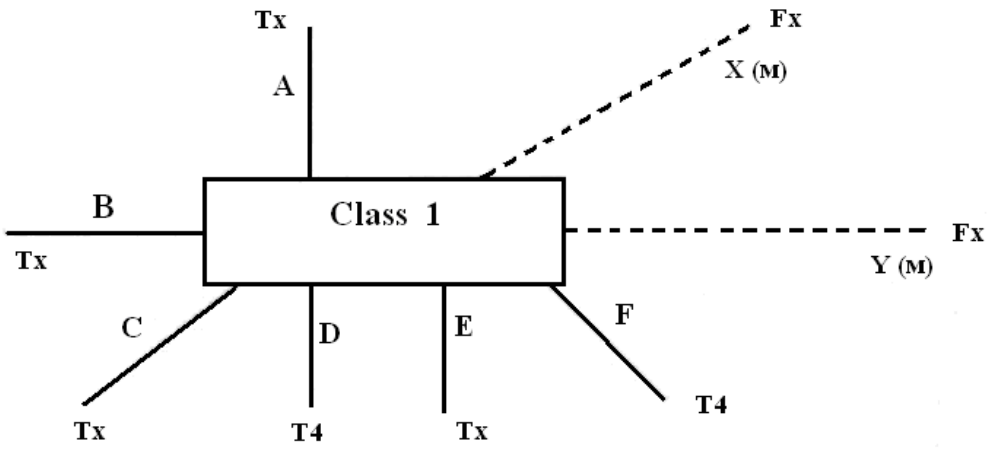


Рисунок 2.3 – Топологія мережі для завдання 2

Таблиця 2.3 – Варіанти завдання 2

Варіант	Довжини сегментів, м					
	A	B	C	D	E	F
1	100	30	50	70	50	90
2	90	40	100	100	30	50
3	60	50	40	20	100	90
4	70	60	10	25	100	100
5	80	80	100	50	30	40
6	50	20	40	40	100	90
7	30	100	10	50	70	100
8	100	90	80	100	40	60
9	90	90	50	30	40	70
10	20	50	60	90	100	100

Завдання 3. Мережа складається з двох повторювачів класу II і оптичних сегментів, як показано на рис.2.4. Відстань між повторювачами (E) і довжини сегментів (A, B, C, D) надані в табл.2.4.

a) Перевірте, чи буде відповідати дана мережа умовам коректної мережі. Необхідно підключити по черзі сегменти з довжинами X, Y, Z.
b) Обчисліть максимально можливі довжини для цих сегментів по черзі (X, Y, Z).
c) Зробіть висновки після всіх розрахунків.

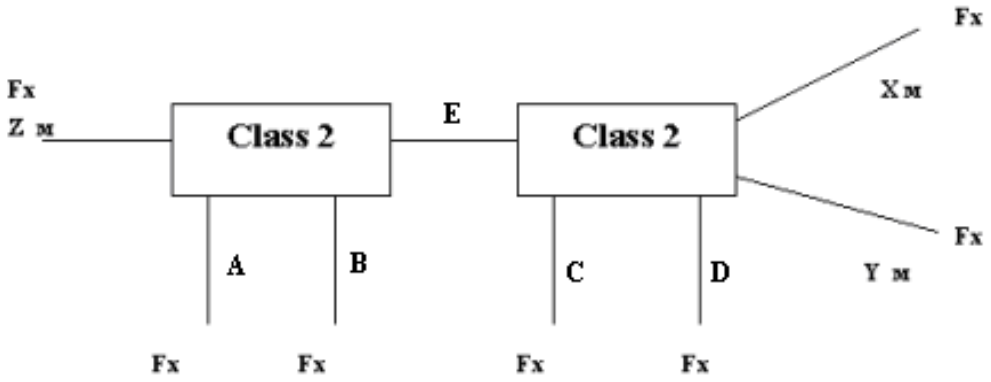


Рисунок 2.4 – Топологія мережі для завдання 3

Таблиця 2.4 – Варіанти завдання 3

Варіанти	Довжини сегментів, м				
	A	B	C	D	E
1	90	40	100	100	30
2	100	30	50	70	10
3	70	60	10	25	10
4	80	80	100	50	30
5	60	50	40	20	20
6	20	50	60	90	10
7	30	100	10	50	10
8	100	90	80	100	20
9	10	50	20	60	30
10	90	90	50	30	30

Завдання 4. Перевірте коректність конфігурації мережі Fast Ethernet, представленої на рис.2.5. Типи і довжини сегментів (A, B, C, D) надані в табл.2.5.

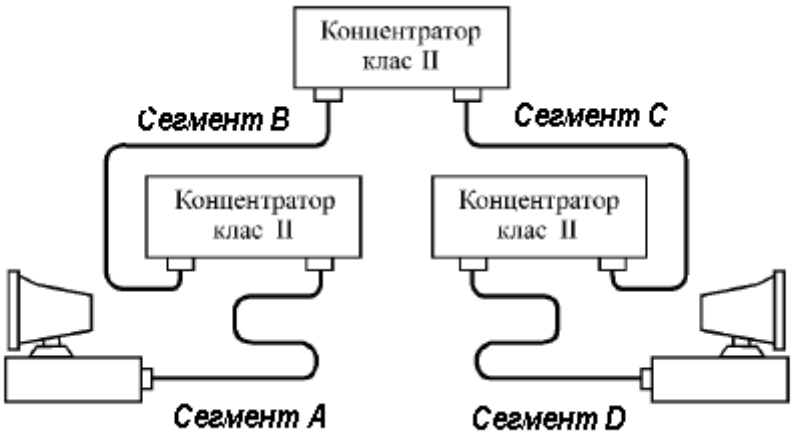


Рисунок 2.5 – Топологія мережі для завдання 4

Таблиця 2.5 – Варіанти завдання 4

Варіанти	Характеристики сегментів			
	A	B	C	D
1	TX, STP1, 50 м	STP1, 8 м	Fiber Optic, 3 м	TX, UTP5, 50 м
2	T4, UTP5, 56 м	UTP3, 5 м	UTP3, 5 м	T4, UTP5, 56 м
3	TX, STP1, 70 м	UTP5, 5 м	Fiber Optic, 5 м	TX, UTP5, 50 м
4	T4, UTP3, 20 м	UTP5, 1 м	UTP5, 9 м	T4, UTP3, 100 м
5	FX, Fiber Optic, 70 м	Fiber Optic, 5 м	Fiber Optic, 5 м	TX, UTP5, 70 м
6	T4, UTP5, 67 м	UTP3, 5 м	UTP3, 5 м	T4, UTP5, 73 м
7	TX, UTP5, 56 м	Fiber Optic, 5 м	Fiber Optic, 6 м	TX, STP1, 56 м
8	T4, UTP5, 56 м	UTP5, 7 м	UTP3, 5 м	T4, UTP5, 74 м
9	TX, STP1, 70 м	Fiber Optic, 5 м	Fiber Optic, 5 м	TX, UTP5, 50 м
10	T4, UTP5, 80 м	UTP3, 2 м	UTP3, 5 м	T4, UTP5, 50 м

3. Прилади, устаткування та інструменти

Для виконання лабораторної роботи використовуються ПЕОМ, об'єднані в локальну мережу під керуванням ОС Windows і текстовий редактор.

4. Правила техніки безпеки та охорони праці

Правила техніки безпеки при виконанні лабораторної роботи регламентуються: «Правилами техніки безпеки при роботі в комп'ютерній лабораторії».

5. Порядок проведення лабораторної роботи

Для виконання роботи кожен повинен:

1. Вивчити теоретичну частину лабораторної роботи.
2. Відповісти на контрольні запитання.
3. Отримати у викладача варіант і виконати розрахунок конфігурації мережі Fthernet і Fast Ethernet.
4. Зробити висновки до кожного завдання щодо працездатності мережі.
5. Оформити звіт.
6. Захистити звіт.

6. Оформлення та захист звіту

Звіт готується в електронному вигляді і роздруковується. Підготовлений до захисту звіт до лабораторної роботи повинен містити:

1. Найменування лабораторної роботи.
2. Відомості про виконавця, номер варіанта.
3. Завдання до лабораторної роботи.
4. Розрахунки до кожного завдання лабораторної роботи.
5. Висновки щодо працездатності мережі кожного завдання, а у випадку її некоректної конфігурації – пропозиції щодо заходів, які забезпечать її працездатність.

Додаток А

Дані для проведення розрахунку конфігурації мережі Ethernet

Таблиця А.1 – Загальні обмеження для всіх стандартів Ethernet

Характеристика	Значення
Номінальна пропускна здатність	10 Мбіт/с
Максимальне число станцій у мережі	1024
Максимальна відстань між вузлами мережі	2500м (в 10Base –FB 2750м)
Максимальне число коаксіальних сегментів у мережі	5

Таблиця А.2 – Параметри специфікацій фізичного рівня стандарту Ethernet

Параметр	10Base - 5	10Base - 2	10Base-T	10Base-F
Кабель	товстий коаксіальний кабель RG-8 або RG-11	тонкий коаксіальний кабель RG-58	неекранована кручена пара категорій 3,4,5	багатомодовий волокняно-оптичний кабель
Максимальна довжина сегмента, м	500	185	100	2000
Максимальна відстань між вузлами мережі (при використанні повторювачів), м	2500	925	500	2500 (2740 для 10Base –FB)
Максимальне число станцій у сегменті	100	30	1024	1024
Максимальне число повторювачів між будь-якими станціями мережі.	4	4	4	4 (5 для 10Base –FB)

Таблиця А.3 – Дані для розрахунку значення PDV

Тип сегмента	База лівого сегмента, bt	База проміжного сегмента, bt	База правого сегмента, bt	Затримка середо-вища на 1м, bt	Максимальна довжина сегмента, м
10Base -5	11.8	46.5	169.5	0.0866	500
10Base -2	11.8	46.5	169.5	0.1026	185
10Base -T	15.3	42.0	165.0	0.113	100
10Base -FB	-	24.0	-	0.1	2000
10Base -FL	12.3	33.5	156.5	0.1	2000
FOIRL	7.8	29.0	152.0	0.1	1000
AUI(>2 м)	0	0	0	0.1026	2+48

*******Щоб не потрібно було два рази складати затримки, які вносяться кабелем, у таблиці даються подвоєні величини затримок для кожного типу кабелю.

У таблиці під базою сегмента розуміється затримки, що вносяться повторювачем. Лівим сегментом названий сегмент, з якого починається шлях сигналу від виходу передавача кінцевого вузла, правим називається найбільш далекий сегмент мережі, у якому і виникає колізія, інші сегменти є проміжними. З кожним сегментом зв'язана затримка поширення сигналу уздовж кабелю сегмента, що залежить від довжини сегмента і обчислюється шляхом множення часу поширення сигналу за один метр кабелю (у бітових інтервалах) на довжину кабелю в метрах. Загальне значення PDV не повинне перевищувати 512 bt.

Лівий і правий сегменти мають різні величини базової затримки, тому у випадку різних типів сегментів на самих далеких краях мережі необхідно виконати розрахунки двічі: один раз прийняти у якості лівого сегменту один тип, а в другий - сегмент іншого типу. Результатом можна вважати максимальне значення PDV.

Таблиця А.4 – Зменшення міжкадрового інтервалу повторювачами

Тип сегмента	Передавальний сегмент, bt	Проміжний сегмент, bt
10Base -5 или 10Base -2	16	11
10Base -FB	-	2
10Base -FL	10,5	8
10Base -T	10,5	8

При розрахунку зменшення міжкадрового інтервалу повторювачами аналізують тільки лівий і проміжні сегменти. Значення PVV не повинне перевищувати 49 bt.

Додаток Б

Дані для вибору конфігурації мережі Fast Ethernet

Для визначення працездатності мережі Fast Ethernet стандарт IEEE 802.3 пропонує дві моделі, які називаються Transmission System Model 1 і Transmission System Model 2. Перша модель заснована на кількох нескладних правилах. Вона виходить з того, що всі компоненти мережі (зокрема, кабелі) мають найгірші з можливих часових характеристик, тому завжди дає результат зі значним запасом.

Друга модель використовує систему точних розрахунків з реальними часовими характеристиками кабелів. У зв'язку з цим її застосування дозволяє іноді подолати жорсткі обмеження моделі 1.

Правила моделі 1

– Сегменти, які виконані на електричних кабелях (кручених парах) не повинні бути довше 100 метрів. Це відноситься до кабелів усіх категорій - 3, 4 і 5, до сегментів 100BASE-T4 і 100BASE-TX.

– Сегменти, які виконані на оптичних кабелях, не повинні бути довше 412 метрів.

– Якщо використовуються адаптери з зовнішніми (виносними) трансиверами, то трансиверні кабелі (MII) не повинні бути довше 50 сантиметрів.

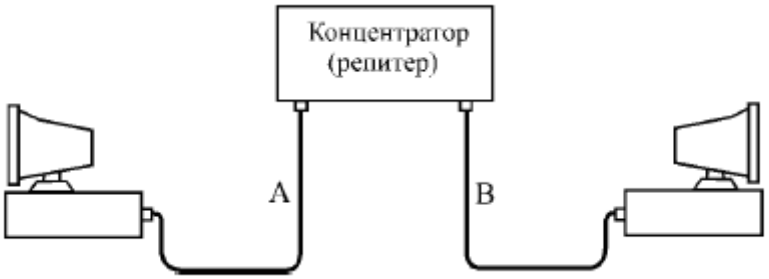
Модель 1 виділяє три можливі конфігурації мережі Fast Ethernet:

1) З'єднання двох абонентів (вузлів) мережі безпосередньо, без репітера або концентратора.

Абонентами при цьому можуть виступати не тільки комп'ютери, але і мережевий принтер, порт комутатора, моста чи маршрутизатора. Таке поєднання називається з'єднанням DTE-DTE або двоточковим.

Правила моделі 1 для даного випадку прості: електричний кабель не повинен бути довше 100 метрів, напівдуплексний оптоволоконний - не більше 412 метрів, повнодуплексний оптоволоконний - 2000 метрів (при цьому затримка сигналу в кабелі не має значення, так як метод CSMA / CD не працює).

2) З'єднання двох абонентів мережі за допомогою одного репітерного концентратора класу I чи класу II.

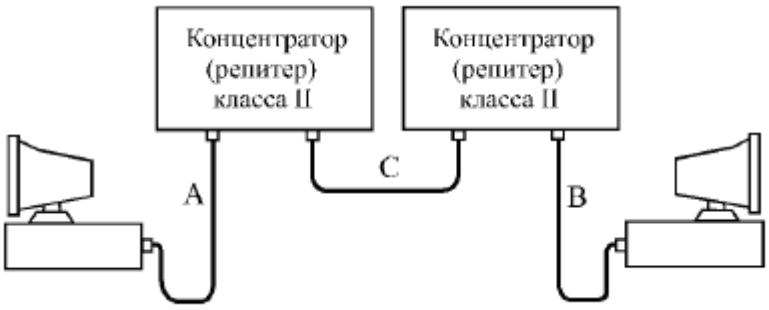


В даному випадку треба обмежувати довжину кабелів A і B мережі відповідно до таблиці Б.1.

Таблиця Б.1 – Максимальна довжина кабелів у конфігурації з одним концентратором

Вид кабелю A	Вид кабелю B	Клас концентратора	Макс. довжина кабелю A, м	Макс. довжина кабелю B, м	Макс. розмір мережі, м
TX, T4	TX, T4	I или II	100	100	200
TX	FX	I	100	160,8	260,8
T4	FX	I	100	131	231
FX	FX	I	136	136	272
TX	FX	II	100	208,8	308,8
T4	FX	II	100	204	304
FX	FX	II	160	160	320

3) З'єднання двох абонентів мережі за допомогою двох репітерних концентраторів класу II. При цьому передбачається, що для зв'язку концентраторів завжди використовується електричний кабель довжиною не більше 5 метрів.



Концентратори класу II мають меншу затримку, тому їх може бути два. Використання трьох концентраторів відповідно до моделі 1 не допускається.

В даному випадку треба обмежувати довжину кабелів A і B відповідно до таблиці. При цьому за умовчанням передбачається, що кабель C має довжину 5 метрів.

Таблиця Б.2 – Максимальна довжина кабелів у конфігурації з двома концентраторами

Вид кабелю A	Вид кабелю B	Макс. довжина кабелю A, м	Макс. довжина кабелю B, м	Макс. розмір мережі, м
TX, T4	TX, T4	100	100	205
TX	FX	100	116,2	221,2
T4	FX	136,3	136,3	241,3
FX	FX	114	114	233

***У всіх перерахованих випадках під розміром мережі розуміється розмір зони конфлікту (області колізії, collision domain).

В обох конфігураціях з концентраторами при використанні одночасно електричного і оптоволоконного кабелів можна за рахунок зменшення довжини електричного кабелю збільшити довжину оптоволоконного. Причому зменшення довжини електричного кабелю на 1 метр відповідає збільшення довжини оптоволоконного кабелю на 1,19 метра. Наприклад, зменшивши кабель TX на 10 метрів, можна збільшити кабель FX на 11,9 метра, і його гранична довжина складе при двох концентраторах 128,1 метра.

У разі використання двох оптоволоконних кабелів можна зменшувати один з кабелів за рахунок збільшення іншого. При зменшенні одного кабелю на 10 метрів можна збільшити другий теж на 10 метрів. Якщо ж використовується два електричні кабелі, то збільшувати один з них за рахунок зменшення іншого не можна, так як їх довжина в принципі не може перевищувати 100 метрів через загасання сигналу в кабелі.

Розрахунок за моделлю 2

Друга модель для мережі Fast Ethernet, як і у випадку Ethernet, заснована на обчисленні сумарного подвійного часу проходження сигналу по мережі. Проводити розрахунки величини скорочення межпакетного інтервалу (IPG) не треба. Це пов'язано з тим, що навіть максимальна кількість репітерів і концентраторів, допустимих у Fast Ethernet (два), не може викликати неприпустимого скорочення межпакетного інтервалу.

Для розрахунків відповідно до другої моделі спочатку треба виділити у мережі шлях з максимальним подвійним часом проходження і максимальним

числом репітерів (концентраторів) між комп'ютерами, тобто шлях максимальної довжини. Якщо таких шляхів кілька, то розрахунок повинен проводитися для кожного з них. Розрахунок ведеться на підставі таблиці Б.3.

Таблиця Б.3 – Подвійні затримки компонентів мережі Fast Ethernet (величини затримок надані в бітових інтервалах)

Тип сегменту	Затримка на метр	Макс. затримка
Два абонента TX/FX	-	100
Два абонента T4	-	138
Один абонент T4 і один TX/FX	-	127
Сегмент на кабелі категорії 3	1,14	114 (100 м)
Сегмент на кабелі категорії 4	1,14	114 (100 м)
Сегмент на кабелі категорії 5	1,112	111,2 (100 м)
Екранована вита пара	1,112	111,2 (100 м)
Оптичний кабель	1,0	412 (412 м)
Репітер (концентратор) класу I	-	140
Репітер (концентратор) класу II з портами TX/FX	-	92
Репітер (концентратор) класу II з портами T4	-	67

Для обчислення повного подвійного (кругового) часу проходження для сегмента мережі необхідно помножити довжину сегмента на величину затримки на метр, взяту з другого стовпця таблиці. Якщо сегмент має максимальну довжину, то можна відразу взяти величину максимальної затримки для даного сегмента з третього стовпця таблиці.

Потім затримки сегментів, що входять в шлях максимальної довжини, треба підсумувати і додати до цієї суми величину затримки для прийомопередавальних вузлів двох абонентів (це три верхні рядки таблиці) і величини затримок для всіх репітерів (концентраторів), що входять в даний шлях (це три нижні рядки таблиці).

Сумарна затримка повинна бути менше, ніж 512 бітових інтервалів. При цьому треба пам'ятати, що стандарт IEEE 802.3u рекомендує залишати запас в межах 1 - 4 бітових інтервалів для урахування кабелів всередині з'єднувальних шаф і похибок вимірювання. Краще порівнювати сумарну затримку з величиною 508 бітових інтервалів, а не 512 бітових інтервалів.

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни “Комп’ютерні мережі”
частина ІІ
для студентів ІІІ курсу денної форми навчання
Напрям підготовки – комп’ютерні науки, спеціальність
7.080.401 “Інформаційні управляючі системи та технології”.

Викладач: доц. Кузніченко С.Д.

Підп. до друку Формат 60х84/16

Папір офс. Наклад прим.

Замовлення №

Надруковано з готового оригінал – макета.

Одеський державний екологічний університет,
65016, м. Одеса, вул. Львівська, 15