Міністерство освіти і науки, молоді та спорту України

Одеський державний екологічний університет

МЕТОДИЧНІ ВКАЗІВКИ
до виконання контрольної роботи
за курсом «Комп'ютерні мережі»
для студентів 4 курсу заочної форми навчання

Викладач – доц. Кузніченко Світлана Дмитрівна

Одеса 2012

Зміст

Передмова

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. Головна увага приділяється аналізу використовуваних протоколів передачі даних як основи побудови механізмів функціонування сучасних комп'ютерних мереж.

Методичні вказівки призначені для студентів IV курсу заочної форми навчання. Мета виконання контрольної роботи – закріплення теоретичного лекційного матеріалу та надбання практичних навиків у використанні стандартних мережних утиліт, які дозволяють одержати статистику щодо конфігурації мережі, розрахунках пропускної здатності і конфігурації локальних мереж. Для досягнення поставленої мети розглянуті наступні завдання: ознайомлення студентів з основними принципами, методами та можливостями 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.

Внаслідок вивчення дисципліни студент повинен

- **знати:** архітектури комп'ютерних мереж, принципи структурування 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; призначення основних мережних утиліт операційних систем сімейства Windows; етапи діагностики мережі; структуру та основні протоколи стека TCP/IP; типи адресації в IP-мережах;
- **вміти:** аналізувати конфігурацію мережі; одержувати IP–адреси, ім'я домена, імена комп'ютерів, що входять у домен; переглядати і підключати загальні ресурси; визначати причини неполадок у мережі; одержувати інформацію про використання портів; пересилати повідомлення; робити розрахунок пропускної здатності мережі і конфігурації мережі Ethernet.

У процесі самостійного вивчення курсу студент повинен керуватися його програмою та вивчити за конспектом лекцій і літературою, що рекомендована викладачем, відповідний теоретичний матеріал. Ці методичні вказівки містять перелік тем, які повинні бути розглянуті, знання які є необхідними для рішення поставленої задачі, контрольні запитання та завдання.

Номер варіанту контрольного завдання визначається останньою цифрою номера залікової книжки.

Список літератури

1. Кузніченко С.Д. «Комп'ютерні мережі» Конспект лекцій. – Одеса: Вид-во «Екологія», 2007.– 123 с.
2. Методичні вказівки до виконання самостійної роботи студентів з дисципліни «Комп'ютерні мережі» частина 1 для студентів IV курсу денної форми навчання/ Кузніченко С.Д. – Одеса, ОДЕКУ, 2007. – 34 с.
3. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд./В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2010. – 918 с.: ил.
4. Джеймс Бони. Руководство по Cisco IOS. – СПб.: Питер, М: Издательство «Русская редакция», 2008. – 784 с.: ил.
5. Джо Хабракен. Как работать с маршрутизаторами Cisco. – СПб.: Издательство «ДМК-Пресс», 2005. – 317 с.: ил.
6. Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. Изд. 4-е. – М.: Издательский дом «Вильямс», 2005. – 1040 с.: ил.
7. Брайан Хилл. Полный справочник по Cisco. – М.: Издательский дом «Вильямс», 2007. – 1088 с.: ил.

Звіт з контрольної роботи повинен містити:

1. Відповіді на теоретичні питання до всіх завдань контрольної роботи (завдання №1-4 – відповідь тільки на запитання згідно свого варіанта, завдання №5-6 – на всі контрольні запитання). Відповіді повинні бути повними, за необхідністю забезпечені відповідними поясненнями, рисунками та схемами.
2. Рішення завдань контрольної роботи.

Завдання №1
на тему: «Основи мереж передачі даних»

Мета завдання №1:

Вивчення основних топологій комп'ютерних мереж;

Закріплення теоретичного матеріалу щодо фізичної і логічної структуризації мережі за допомогою мережного комунікаційного обладнання;

Отримання практичних навиків у використанні стандартних мережних утиліт.

Перелік тем лекційного курсу щодо виконання завдання №1:

1. Огляд топологій фізичних зв'язків.
2. Фізична і логічна структуризації мережі за допомогою мережного комунікаційного обладнання.
3. Багаторівнева модель OSI.

Загальні рекомендації до виконання завдання №1

1.1 Класифікація мереж за територіальною ознакою. Локальні і глобальні мережі

Комп'ютерні мережі – це сукупність комп'ютерів, з'єднаних лініями зв'язку. Лінії зв'язку утворені кабелями, мережними адаптерами та іншими комунікаційними пристроями. Все мережне встаткування працює під керуванням системного і прикладного програмного забезпечення. Розрізняють локальні і глобальні комп'ютерні мережі.

Глобальні мережі (Wide Area Networks, WAN) поєднують комп'ютери, розосереджені на відстані сотень і тисяч кілометрів.

Локальні мережі (Local Area Networks, LAN) – це об'єднання комп'ютерів, зосереджених на невеликій території, звичайно в радіусі не більше 1-2 км (іноді кілька десятків кілометрів), за допомогою високоякісних ліній зв'язку, які дозволяють приймати прості методи передачі даних і досягають високих швидкостей обміну даних порядку 100Мбіт/с.

1.2 Класифікація мереж за способом доступу до мережевих ресурсів

Всі існуючі комп'ютерні мережі можна розділити по типу розподілу ресурсів між комп'ютерами на **одноранговi** мережі і мережі на базі **файлового сервера**.

Мережа є **одноранговою**, якщо кожний ПК може бути одночасно і файловим сервером, і робочою станцією. Комп'ютери, за допомогою яких користувачі одержують доступ до комп'ютерної мережі, називають робочими станціями. В одноранговій ЛОМ (локальної обчислювальної мережі) дисковий простір і файли на комп'ютерах стають загальними. Інакше кажучи, кожний мережний комп'ютер має рівні права (перебуває в одному ранзі) з усіма іншими мережними комп'ютерами.

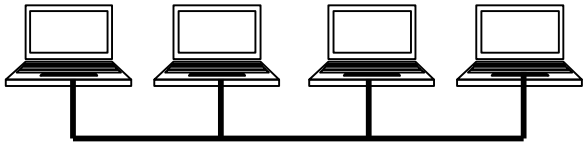


Рис.1.1 - Однорангова ЛОМ

У мережах з архітектурою клієнт/сервер основна частина спільно використовуваних ресурсів зосереджена на окремих комп'ютерах, які називаються серверами. На серверах звичайно немає основних користувачів і вони є багатокористувальницькими комп'ютерами, що надають можливість спільного використання своїх ресурсів клієнтам мережі. У результаті клієнти звільняються від навантаження, що пов'язане з функціонуванням у ролі сервера для інших клієнтів.

Сервер- це будь-який комп'ютер, підключений до локальної мережі, на якому перебувають ресурси, які використовуються іншими пристроями локальної мережі. Клієнт - це будь-який комп'ютер, що через локальну мережу звертається до ресурсів, які зберігаються на сервері.

Файловий сервер

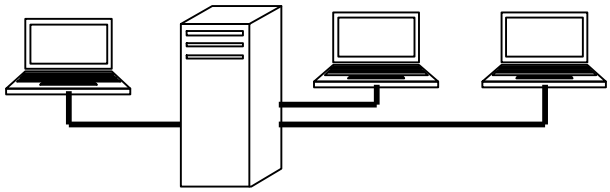


Рис.1.2 - ЛОМ із виділеним файловим сервером

1.3 Топологія фізичних зв'язків

Однією з основних характеристик комп'ютерних мереж є топологія їхньої побудови. **Мережна топологія** - це геометрична форма (або фізична связність) мережі. Конфігурація **фізичних зв'язків** визначається електричними з'єднаннями комп'ютерів між собою і може відрізнятися від конфігурації **логічних зв'язків** між вузлами мережі. Логічні зв'язки являють собою маршрути

передачі даних між вузлами мережі і утворюються шляхом відповідного налагодження комунікаційного встаткування.

Розрізняються повнозв'язні та неповнозв'язні топології (рис.1.3(а,б)). **Повнозв'язна топологія** відповідає мережі, у якій кожний комп'ютер мережі зв'язаний з усіма іншими, а неповнозв'язна **топологія** виходить із повнозв'язної шляхом видалення деяких можливих зв'язків.

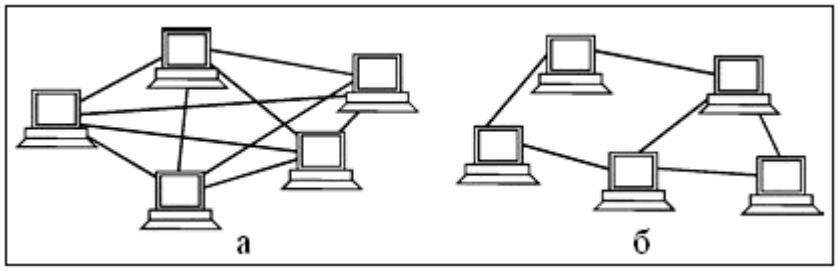


Рис. 1.3 - Мережна топологія: повна (а) і неповнозв'язна (б)

Загальна шина (рис.1.4) є дуже розповсюдженою і простою топологією для локальних мереж. У цьому випадку комп'ютери підключаються до одного коаксіального кабелю за схемою «монтажного АБО». Передана інформація може поширюватися в обидва боки і доступна одночасно всім комп'ютерам.

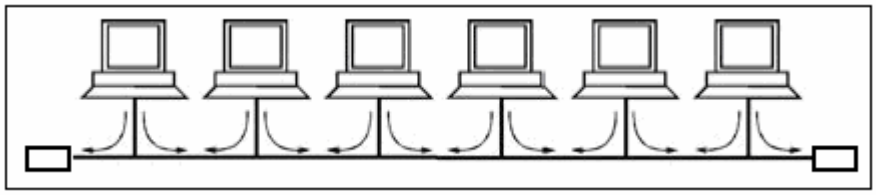


Рис. 1.4 - Мережна топологія шина

У мережах, побудованих відповідно до топології ***кільце*** (рис.1.5), передача даних походить від одного комп'ютера до іншого по кільцю через мережні адаптери, поки інформація не дійде до адресата, записується в його внутрішній буфер, потім далі рухається по кільцю до відправника і відправник її видаляє. Мережна топологія може бути побудована і на основі двох кілець, як, наприклад, у технології FDDI. Вузли, які хочуть скористатися цим підвищеним потенціалом надійності, повинні бути підключені до обох кілець. У нормальному режимі роботи мережі дані проходять через всі ділянки кабелю тільки основного кільця. У випадку якої-небудь відмови основне кільце поєднується з резервним, знову утвориться єдине кільце. Операція згортання виконується засобами концентраторів і/або мережних адаптерів FDDI.

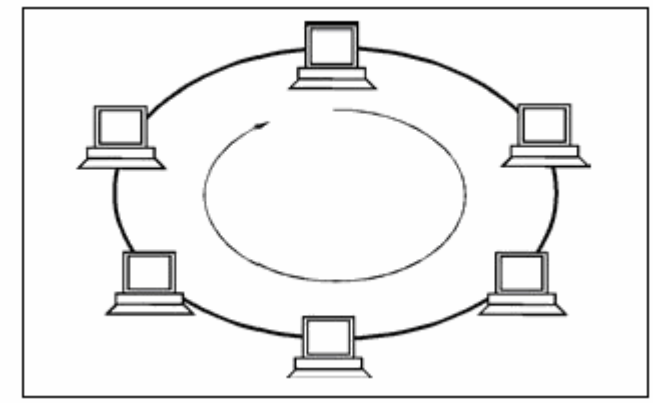


Рис. 1.5 - Мережна топологія кільце

У випадку використання топології ***зірка*** (рис.1.6) кожний комп'ютер приєднується окремим кабелем до загального пристрою, що перебуває в центрі мережі і називається ***концентратором***. У функції концентратора входить направлення переданої комп'ютером інформації одному або всім іншим комп'ютерам мережі.

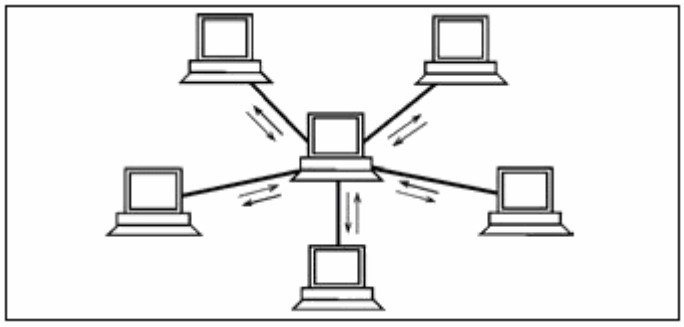


Рис. 1.6 - Мережна топологія зірка

Мережа, яка будується з використанням декількох концентраторів, ієрархічно з'єднаних між собою зв'язками типу зірка, називається **деревом (**рис.1.7**)**. У цей час ієрархічна зірка або дерево є найпоширенішим типом топології зв'язків як у локальних, так і глобальних мережах.

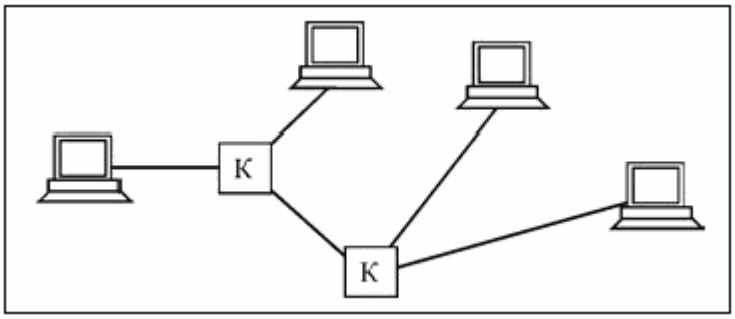


Рис. 1.7 - Мережна топологія дерево

1.4 Фізична та логічна структуризації мереж

Для структуризації мережі використовують спеціальне комунікаційне устаткування - **повторювачі, концентратори, мости, комутатори, маршрутизатори**.

Повторювач (repeater) - використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної довжини мережі і дозволяє перебороти обмеження на довжину ліній зв'язку за рахунок поліпшення якості переданого сигналу.

Повторювач, що має кілька портів і з'єднує кілька фізичних сегментів, часто називають **концентратором (concentrator)**, або **хабом (hub)** - вони повторюють сигнали, що прийшли з одного порту, на інших своїх портах. Концентратор завжди змінює фізичну топологію мережі, але при цьому залишає без зміни її логічну топологію. Фізична структуризація мережі за допомогою концентраторів збільшує відстані між вузлами мережі і підвищує її надійності. Концентратор може блокувати некоректно працюючий вузол, виконуючи роль деякого керуючого вузла.

Однак фізична структуризація не вирішує проблеми перерозподілу переданого трафіка між різними фізичними сегментами мережі. У такому випадку необхідно робити логічну структуризацію мережі.

Поширення трафіка, призначеного для комп'ютерів деякого сегмента мережі, тільки в межах цього сегмента, називається ***локалізацією*** трафіка. **Логічна структуризація** мережі - це процес розбивки мережі на сегменти з локалізованим трафіком.

Для логічної структуризації мережі використовуються такі комунікаційні пристрої, як мости, комутатори, маршрутизатори і шлюзи.

Міст (bridge) ділить поділюване середовище передачі мережі на частині (логічні сегменти), передаючи інформацію з одного сегмента в іншій тільки в тому випадку, якщо така передача дійсно необхідна, тобто якщо адреса комп'ютера призначення належить інший підмережі. Тим самим міст ізолює трафік однієї підмережі від трафіка іншої, підвищуючи загальну продуктивність передачі даних у мережі. Локалізація трафіка не тільки економить пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних. Для локалізації трафіка мости використовують апаратні адреси комп'ютерів.

Комутатор (switch, switching hub) за принципом обробки кадрів нічим не відрізняється від мосту. Основна його відмінність від мосту полягає в тому, що він є свого роду комунікаційним мультипроцесором, тому що кожний його порт оснащений спеціалізованим процесором, що обробляє кадри по алгоритму мосту незалежно від процесорів інших портів. За рахунок цього загальна продуктивність комутатора звичайно набагато вище продуктивності традиційного мосту, що має один процесорний блок.

Маршрутизатор (router) - ізолює трафік окремих частин мережі друг від друга, утворюючи логічні сегменти за допомогою явної адресації, оскільки використовує не плоскі апаратні, а складові числові адреси. У цих адресах є **поле**

номера мережі, так що всі комп'ютери, у яких значення цього поля однакові, належать до одного сегмента, який називається в цьому випадку **підмережою (subnet).** Також маршрутизатори здійснюють вибір найбільш раціонального маршруту з декількох можливих. Іншою дуже важливою функцією маршрутизаторів є їхня здатність зв'язувати в єдину мережу підмережі, що побудовані з використанням різних мережних технологій.

Крім перерахованих пристроїв окремі частини мережі може з'єднувати **шлюз (gateway).** Звичайно основною причиною, по якій у мережі використовують шлюз, є необхідність об'єднати мережі з різними типами системного і прикладного програмного забезпечення, а не бажання локалізувати трафік. Проте, шлюз забезпечує і локалізацію трафіка як деякий побічний ефект.

1.5 Багаторівнева модель OSI

Для спрощення відкритої взаємодії комп'ютерних систем наприкінці 70-х років минулого століття Міжнародна організація по стандартизації (ISO, International Organization for Standartization) розробила еталонну **модель взаємодії відкритих систем (OSI, Open System Interconnection)**. Модель OSI розділяє процеси, які беруть участь у сеансі зв'язку, на сім функціональних рівнів. Структура рівнів відповідає природній послідовності подій, що відбуваються під час сеансу зв'язку. На рис.1.8 зображена схема еталонної моделі OSI.

Рівень OSI	Номер OSI
Прикладний рівень	7
Представницький рівень	6
Сеансовий рівень	5
Транспортний рівень	4
Мережний рівень	3
Канальний рівень	2
Фізичний рівень	1

Рис. 1.8 - Еталонна модель OSI

Наведемо коротке визначення кожного рівня моделі OSI:

1. **Фізичний рівень** виконує передачу бітів по фізичним каналам зв'язку: коаксіальному кабелю, крученій парі або оптоволокняному кабелю, визначає характеристики електричних сигналів, які передають дискретну

інформацію (рівні напруги або струм сигналу, тип кодування, швидкість передачі сигналів) та стандартизує типи гнізд і призначення кожного контакту.

2. **Канальний рівень** групує біти у набори, які називаються кадрами, та забезпечує коректність передачі кожного кадру, додаючи для перевірки контрольну суму. Цей рівень здійснює також перевірку доступності середи передачі і реалізує механізми виявлення та корекції помилок
3. **Мережний рівень** служить для утворення єдиної транспортної системи, що об'єднує декілька мереж, і вирішує проблему маршрутизації.
4. **Транспортний рівень** забезпечує додаткам передачу даних з тим ступенем надійності, котрий їм потрібний, у відповідності з обумовленими даним рівнем класами сервісу.
5. **Сеансовий рівень** забезпечує управління взаємодією: фіксує, яка із сторін є активною в даний момент, надає засоби синхронізації.
6. **Представницький рівень** надає засоби, що дозволяють перебороти синтаксичні розходження у представленні даних або ж розходження у кодах символів і може виконувати шифрування і дешифрування даних.
7. **Прикладний рівень** - це набір різноманітних протоколів, дозволяючих користувачам мережі отримувати доступ до загальних ресурсів і організовувати свою спільну роботу.

Завдання до контрольної роботи:

Контрольні питання

1. Дайте опис функцій всіх рівнів моделі OSI і приведіть приклади стандартних протоколів для кожного рівня.
2. Приведіть порівняльну характеристику фізичних топологій локальних мереж. Їхні дпереваги і недоліки.
3. Логічна структуризація мережі. Чи завжди логічна структура збігається з фізичною топологією локальної мережі? Види логічних організацій мережі: кільцева, лінійна. Поясніть наступні твердження: логічна зірка на основі фізичної загальної шини і логічне кільце на основі фізичної зірки.
4. Визначите функціональне призначення основних типів комунікаційного обладнання - повторювачів, концентраторів, мостів, комутаторів, маршрутизаторів.
5. Поясніть різницю у вживанні термінів «протокол» і «інтерфейс» стосовно до багаторівневої моделі взаємодії пристроїв у мережі.
6. Дайте визначення обчислювальної мережі. З яких основних елементів вона складається?
7. Приведіть загальну порівняльну характеристику серверних, гібридних і однорангових мереж. Їхні переваги і недоліки.
8. Дайте характеристику топології “зірка”.
9. Дайте характеристику топології “кільце”.
10. Опишіть сутність і принципи взаємодії розподіленої програми.

Варіанти завдань

Використовуючи стандартні мережеві утиліти, треба проаналізувати конфігурацію мережі на платформі ОС Windows, тобто одержати свою IP - адресу, довідатися ім'я домена, імена комп'ютерів, що входять у домен, переглянути загальні ресурси. Укажіть область застосування даної утиліти, формат запису та приведіть роздруківку результату її роботи.

Варіант	Список мережевих утиліт
1	ping, net view, tracert
2	ipconfig, netstat, hostname
3	ping, net use, tracert
4	ipconfig, net view, net send
5	ping, netstat, hostname
6	ipconfig, net use, net send
7	ping, net view, tracert
8	ipconfig, netstat, hostname
9	ping, net use, net send
10	ipconfig, net view, tracert

Завдання №2
на тему: «Передача даних на фізичному і канальному рівнях»

Мета завдання №2:

1. Вивчення основних характеристик ліній зв’язку;
2. Закріплення теоретичного матеріалу щодо використання різноманітних методів передачі даних;
3. Отримання практичних навиків у розрахунках пропускної здатності локальної мережі.

Перелік тем лекційного курсу щодо виконання завдання №2:

1. Характеристики ліній зв’язку.
2. Види кодування сигналів.
3. Методи передачі даних.

Загальні рекомендації до виконання завдання №2

2.1 Фізичне середовище передачі даних

До кабельних середовищ передачі даних належать:

- Коаксіальний кабель
- Кручена або вита пара
- Оптичний кабель

Коаксіальний кабель (coaxial) складається із двох концентричних провідників. Його назва пов'язана з тим, що обидва провідника розташовані на одній загальній осі. У найпоширенішому варіанті цей кабель складається з однієї провідної мідної жили, оточеної діелектричним матеріалом. Цей діелектричний матеріал екранується ще одним циліндричним провідником. Після цього йде ще один шар ізоляції, і вся ця конструкція розташовується в захисну зовнішню оболонку з полівінілхлориду або тефлону (рис.2.1).

1 - центральний провідник (жила), 2 - ізолятор центрального провідника,
3 - провідник, що екранує (екран), 4 - зовнішній ізолятор і захисна оболонка.

Рис. 2.1 – Бічний переріз коаксіального кабелю

Коаксіальні кабелі діляться на різні класи за опором. Для цього застосовується шкала Radio Grade (RG). RG-8 і RG-11 - «товстий» коаксіальний кабель. Має хвильовий опір 50 Ом і зовнішній діаметр 0,5 дюйма. RG-58/U і RG-58 A/U - різновиди «тонкого» коаксіального кабелю. Кабель RG-58/U має суцільний внутрішній провідник, а кабель RG-58 A/U - багатожильний. Хвильовий опір 50 Ом.

Скручена пара проводів називається **крученою парою (twisted pair).** Кабелі на основі крученої пари називаються симетричними кабелями через те, що вони складаються із двох однакових у конструктивному відношенні провідників. Скручування проводів знижує вплив зовнішніх перешкод на корисні сигнали, які передаються по кабелю. У локальних мережах звичайно використовується кабель із чотирьох кручених пар у загальній оболонці, що складається з полівінілхлориду або тефлону.

Кручена пара існує в екранованому варіанті (Shielded Twistedpair, STP), коли провідники покриваються додатковою металевою фольгою, що створює ізоляційний екран, і неекранованому (Unshielded Twistedpair, UTP), коли ізоляційна обгортка відсутня.

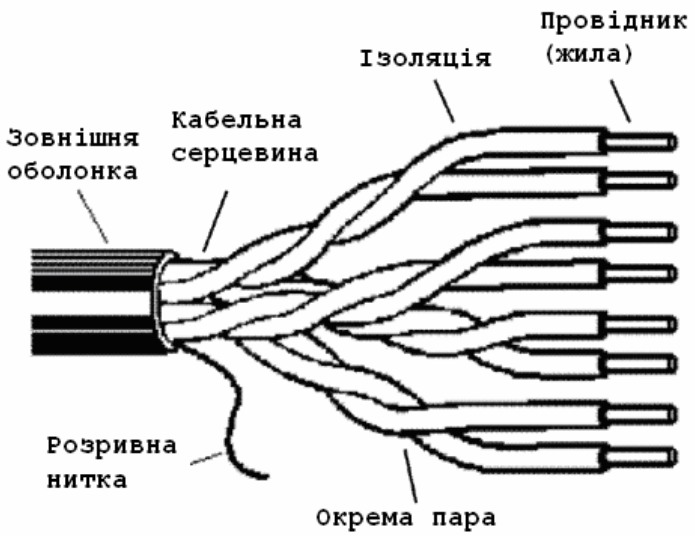


Рис. 2.2 - Кабель «кручена пара»

Екранована кручена пара призначена для прокладки кабелю в середовищі, чутливому до впливу електромагнітних перешкод. Покриття провідника металевим екраном захищає сигнали від зовнішніх випромінювань. Основним стандартом, що визначає параметри екранованої крученої пари, є фірмовий стандарт IBM. У цьому стандарті кабелі діляться не на категорії, а на типи: Type 1, Type 2,..., Type 9.

Всі кабелі UTP незалежно від їхньої категорії виробляються в 4-парному виконанні. Звичайно дві пари призначені для передачі даних, а дві - для передачі голосу. Для з'єднання кабелів з устаткуванням використовуються розетки RJ-45. Найбільш популярним у цей час є кабель UTP категорії 5, який використовується для передачі даних зі швидкістю до 100 Мбіт/с включно і тактується частотою 100 Мгц.

Оптичний кабель (optical fiber) складається з тонких (5-60 мікрон) гнучких скляних волокон, по яких поширюються світлові сигнали. Це найбільш якісний тип кабелю - він забезпечує передачу даних з дуже високою швидкістю (до 10 Гбіт/с і вище) і до того ж краще інших типів передавального середовища забезпечує захист даних від зовнішніх перешкод. Кожний світлодіод складається із центрального провідника світла (серцевини) - скляного волокна, і скляної оболонки, що володіє меншим показником переломлення, чим серцевина. Поширюючись по серцевині, промені світла не виходять за її межі, відбиваючись від покриваючого шару оболонки.

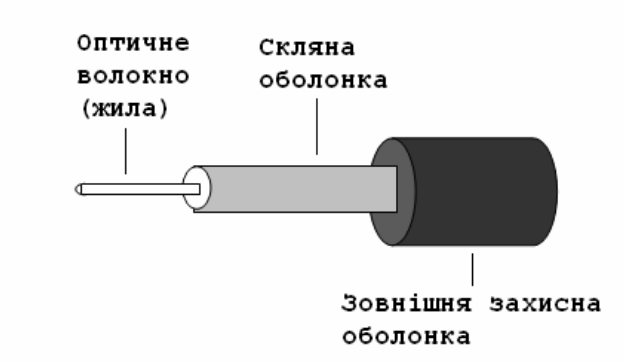


Рис.1.3 - Оптичний кабель

2.2 Характеристики ліній зв'язку

Наведемо короткий опис найбільш важливих характеристик ліній зв'язку:

- **Загасання** показує, на скільки зменшується потужність еталонного синусоїдального сигналу на виході лінії зв'язку стосовно потужності сигналу на вході цієї лінії. Загасання звичайно вимірюється в децибелах, дБ (d) і обчислюється $\mathbf{A = 10\log_{10} P_{вих} / P_{вх}}$, де p - потужність сигналу на виході і вході лінії.
- **Абсолютний рівень потужності сигналу** обчислюється по наступній формулі: $\mathbf{p = 10\ \log_{10} P/1мВт\ [дБм]}$, де p - потужність сигналу в міліватах. При цьому як базове значення потужності сигналу, до якого вимірюється поточна потужність, приймається значення в 1 мВт.
- **Смуга пропущення (bandwidth)** визначає діапазон частот синусоїдального сигналу, при якому цей сигнал передається по лінії зв'язку без значних перекручувань. Ширина смуги пропущення впливає на максимально можливу швидкість передачі інформації. Граничними частотами вважаються частоти, на яких потужність вихідного сигналу зменшується в 2 рази стосовно вхідного, що відповідає загасанню -3дб.
- **Пропускна здатність (throughput)** лінії характеризує максимально можливу швидкість передачі даних по лінії зв'язку. Пропускна здатність виміряється в бітах за секунду - біт/с, а також у похідних одиницях, таких як кілобіт за секунду (Кбіт/с), мегабіт за секунду (Мбіт/с), гигабіт за секунду (Гбіт/с) і т.д.

Зв'язок між смугою пропущення лінії і її максимально можливою пропускною здатністю, поза залежністю від прийнятого способу фізичного кодування, установив **Клод Шеннон:**

$$\mathbf{C = F \log2 (1 + P_c/P_ш),} \qquad (2.1)$$

де C - максимальна пропускна здатність лінії в бітах за секунду,
F - ширина смуги пропущення лінії в герцах,
P_c - потужність сигналу,
$P_ш$ - потужність шуму.

Пропускна здатність залежить від спектра сигналу, що у свою чергу залежить від способу кодування По формулі **Найквиста** визначається максимально можлива пропускна здатність лінії зв'язку, але без обліку шуму на лінії:

$$\mathbf{C = 2F \log_2 M,} \qquad (2.2)$$

де M - кількість станів інформаційного параметра.

2.3 Види кодування сигналів

При передачі даних по каналах зв'язку використовується два види фізичного кодування:

- аналогова модуляція;
- цифрове кодування.

При аналоговій модуляції інформація кодується зміною амплітуди, частоти або фази синусоїдального сигналу несучої частоти.

При цифровому кодуванні дискретної інформації застосовують потенційні та імпульсні коди.

У потенційних кодах для представлення логічних одиниць і нулів використовується тільки значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, в увагу не приймаються. Імпульсні коди дозволяють представити двійкові дані або імпульсами визначеної полярності, або частиною імпульсу - перепадом потенціалу визначеного напрямку. Докладніше про цифрове кодування сказано у конспекті лекцій та у [2] стор. 200-210, там же наведені діаграми деяких методів потенційного та імпульсного кодування.

2.4 Види логічного кодування

Логічне кодування використовується для поліпшення потенційних кодів типу AMI, NRZI або 2Q1B. Логічне кодування повинне замінювати довгі послідовності біт, що приводять до постійного потенціалу, вкрапленнями

одиниць. Для логічного кодування характерні два методи - надлишкові коди і скремблірування.

Надлишковий код 4В/5В, який використовується у технологіях FDDI і Fast Ethernet, замінює вихідні символи довжиною в 4 біти на символи довжиною в 5 біт. У коді 4В/5В результуючі символи можуть містити 32 бітові комбінації, у той час як вихідні символи - тільки 16. Тому в результуючому коді можна відібрати 16 таких комбінацій, які не містять великої кількості нулів, а інші прийнято вважати забороненими кодами. Якщо приймач приймає заборонений код, виходить, на лінії відбулося перекручування сигналу.

Скремблірування - це перемішування даних по відповідному алгоритму скремблером перед передачею їх у лінію за допомогою потенційного коду, так щоб кількість 0 і 1 у результуючому коді було приблизно однаковим. Методи скремблірування полягають у побітному обчисленні результуючого коду на підставі біт вихідного коду і отриманих у попередніх тактах бітах результуючого коду. Наприклад, скремблер може реалізовувати наступне співвідношення:

$$\mathbf{B_i = A_i \oplus B_{i-3} \oplus B_{i-5}} \qquad (2.3)$$

де Bi - двійкова цифра результуючого коду, отримана на і-му такті роботи скремблера,

Ai - двійкова цифра вихідного коду, що надходить на і-му такті на вхід скремблера,

Bi-3 і Bi-5 - двійкові цифри результуючого коду, отримані на попередніх тактах роботи скремблера, відповідно на 3 і на 5 тактах раніше поточного такту,

$\oplus$ - операція додавання по модулю 2.

Після одержання результуючої послідовності приймач передає її дескремблеру, який відновлює вихідну послідовність на підставі зворотного співвідношення.

2.5 Методи виявлення і корекції помилок

Методи виявлення помилок засновані на передачі в складі кадру даних службової надлишкової інформації **- контрольної суми**, по якій можна судити про вірогідність прийнятих даних. Контрольна сума обчислюється як функція від основної інформації. Приймаюча сторона повторно обчислює контрольну суму кадру по відомому алгоритму і у випадку її збігу з контрольною сумою, обчисленою передавальною стороною, робить висновок про коректність прийнятих даних.

У цей час найбільш популярним методом контролю в обчислювальних мережах є **циклічний надлишковий контроль (Cyclic Redundancy Check, CRC).** Докладніше про даний метод і про **метод контролю по паритету** розказано у конспекті лекцій та у [2] стор. 220-222.

Методи відновлення перекручених і загублених кадрів ґрунтуються на тім, що якщо кадр не доходить до одержувача, то він повторно передається

адресатові. Для цього відправник нумерує кадри даних, і для кожного кадру даних очікує від приймача **позитивної квитанції** - службового кадру, що сповіщає про те, що вихідний кадр був отриманий і дані в ньому виявилися коректними. Час очікування обмежений - при відправленні кожного кадру передавач запускає таймер, і, якщо за його витіканням позитивна квитанція не отримана, кадр вважається загубленим. Приймач у випадку одержання кадру з перекрученими даними може відправити **негативну квитанцію** - вказівка на те, що даний кадр потрібно передати повторно.

На даному принципі роботи ґрунтується **метод із простоями** і **метод «ковзного вікна»**. У методі із простоями вузол, що послав кадр, очікує одержання квитанції (позитивної або негативної) від приймача і тільки після цього посилає наступний кадр (або повторює перекручений). Якщо ж квитанція не приходить протягом тайм-ауту, то кадр (або квитанція) вважається загубленим і його передача повторюється. У методі «ковзного вікна» джерело передає деяку кількість кадрів у безперервному режимі, без одержання на ці кадри позитивних квитанцій. Метод із простоями є окремим випадком методу ковзного вікна, коли розмір вікна дорівнює одиниці. Діаграми роботи методу ковзного вікна наводяться у [2] стор. 222-225.

Завдання до контрольної роботи:

Контрольні питання

1. Опишіть найбільш популярні методи виявлення та корекції помилок у протоколах канального рівня. (Циклічно надлишкові коди CRC і метод повторної передачі на основі квитанцій).
2. Опишіть найбільш популярні методи відновлення викривлених і загублених кадрів. Приведіть діаграму роботи методу «ковзного вікна».
3. Опишіть структуру SPT і UPT кабелів. Чим розрізняються їхні конструкції?
4. Що являють собою волокняно-оптичні кабелі? Опишіть їхню будову і експлуатаційні характеристики.
5. Лінії зв'язку, їхня класифікація залежно від середовища передачі даних.
6. Дайте визначення пропускної здатності лінії зв'язку. Від яких внутрішніх параметрів лінії зв'язку залежить її пропускна здатність?
7. Зв'язок між пропускною здатністю та смугою пропущення лінії. Формула Шеннона. Формула Найквиста.
8. Опишіть основні типи і характеристики коаксіальних кабелів.
9. Опишіть методи логічного кодування. Яким способом логічне кодування сприяє поліпшенню потенційних кодів?
10. Методи фізичного кодування. Потенційні і імпульсні коди..Їхні переваги й недоліки. У чому проявляється недолік потенційних кодів? Яким чином можна їх поліпшити?

Варіанти завдань

1. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 20 кГц, якщо потужність передавача становить 0,063 мВт, а потужність шуму в каналі дорівнює 0,001 мВт?

2. Визначте теоретичну пропускну здатність каналу зв'язку, якщо відомо, що його смуга пропущення дорівнює 500 кГц, а в методі кодування використовується 8 станів сигналу.

3. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 40 кГц, якщо потужність передавача становить 0,031 мВт, а потужність шуму в каналі дорівнює 0,001 мВт?

4. Визначте теоретичну пропускну здатність каналу зв'язку, якщо відомо, що його смуга пропущення дорівнює 200 кГц, а в методі кодування використовується 4 стани сигналу.

5. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 15 кГц, якщо потужність передавача становить 0,015 мВт, а потужність шуму в каналі дорівнює 0,001 мВт?

6. Визначте теоретичну пропускну здатність каналу зв'язку, якщо відомо, що його смуга пропущення дорівнює 100 кГц, а в методі кодування використовується 2 стани сигналу.

7. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 35 кГц, якщо потужність передавача становить 0,126 мВт, а потужність шуму в каналі дорівнює 0,002 мВт?

8. Визначте теоретичну пропускну здатність каналу зв'язку, якщо відомо, що його смуга пропущення дорівнює 150 кГц, а в методі кодування використовується 4 стани сигналу.

9. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 18 кГц, якщо потужність передавача становить 0,062 мВт, а потужність шуму в каналі дорівнює 0,002 мВт?

10. Якою буде теоретична межа швидкості передачі даних по каналу з шириною смуги пропущення в 35 кГц, якщо потужність передавача становить 0,060 мВт, а потужність шуму в каналі дорівнює 0,004 мВт?

Завдання №3
на тему: «Технології локальних комп'ютерних мереж»

Мета завдання №3:

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

Перелік тем лекційного курсу щодо виконання завдання №3:

1. Структура стандартів IEEE 802.x. Технологія Ethernet.
2. Особливості побудови мережі на базі технологій Token Ring і FDDI.

Загальні рекомендації до виконання завдання №3

3.1 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.1 і табл. 2 додатка.

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. Докладніше про базову технологію Ethernet розказано у конспекті лекцій та у [2] стор. 307-322.

3.2 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 екранованe 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.

3.3 Технологія Token Ring

Мережі Token Ring будуються на основі кільцевої топології і використовують маркерний метод доступу, що гарантує кожної станції одержання доступу до поділюваного кільця протягом часу обороту маркера. Через цю властивість цей метод іноді називають детермінованим. Мережі Token Ring працюють на двох швидкостях: 4 і 16 Мбіт/с. Збільшення швидкості передачі даних до 16 Мбіт/с стало можливим за рахунок використання ***алгоритму раннього вивільнення маркера***. Маркер передається відразу ж, як тільки дана станція закінчила передачу одного або декількох кадрів за час утримання маркера, не чекаючи повернення по кільцю цього кадру з бітом підтвердження прийому. У цьому випадку пропускна здатність кільця використовується більш ефективно, тому що по кільцю одночасно просуваються кадри декількох станцій.

Для контролю мережі одна зі станцій у кільці виконує роль активного монітора, що безупинно контролює наявність маркера, а також час обороту маркера і кадрів даних. Активний монітор виконує в кільці також роль повторювача - він ресинхронізує сигнали, що проходять по кільцю. Метод доступу заснований на пріоритетах: від 0 (нижчий) до 7 (вищий). Станція сама визначає пріоритет поточного кадру і може захопити кільце тільки у тому випадку, коли у кільці немає більше пріоритетних кадрів.

Фізична специфікація технології Token Ring використовує як середовище передачі даних екрановану кручену пару, неекрановану кручену пару, а також волокняно-оптичний кабель. Максимальна кількість станцій у кільці - 260, а максимальна довжина кільця - 4 км.

У мережі Token Ring станції в кільце поєднують за допомогою концентраторів MSAU. Пасивний концентратор MSAU з'єднує вихід попередньої станції в кільці із входом наступної. Максимальна відстань від станції до MSAU - 100 м для STP і 45 м для UTP.

Кільце може бути побудоване на основі активного концентратора MSAU, що у цьому випадку називають повторювачем.

3.4 Технологія FDDI

Технологія FDDI першою використовувала волокняно-оптичний кабель у локальних мережах, а також роботу на швидкості 100 Мбіт/с.

Для технології FDDI характерні кільцева топологія і маркерний метод доступу. Мережа будується на основі двох кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. При однократних відмовах кабельної системи або станції мережа, за рахунок «згортання» подвійного кільця в одинарне, залишається цілком працездатною.

Алгоритми маркерного методу доступу FDDI має певні розходження для синхронних і асинхронних кадрів (тип кадру визначає станція). Для передачі синхронного кадру станція завжди може захопити маркер, що прийшов, на фіксований час. Для передачі асинхронного кадру станція може захопити маркер тільки в тому випадку, коли маркер виконав оборот по кільцю досить швидко, що говорить про відсутність перевантажень кільця. Такий метод доступу, по-перше, віддає перевагу синхронним кадрам, а по-друге, регулює завантаження кільця, притримуючи передачу нетермінових асинхронних кадрів.

Як фізичне середовище технологія FDDI використовує волокняно-оптичні кабелі і UTP категорії 5. Максимальна кількість станцій подвійного підключення в кільці - 500, максимальний діаметр подвійного кільця - 100 км. Максимальні відстані між сусідніми вузлами для багатомодового кабелю дорівнюють 2 км, для крученої пари UTP категорії 5-100 м, а для одномодового - залежать від його якості.

Завдання до контрольної роботи:

Контрольні питання

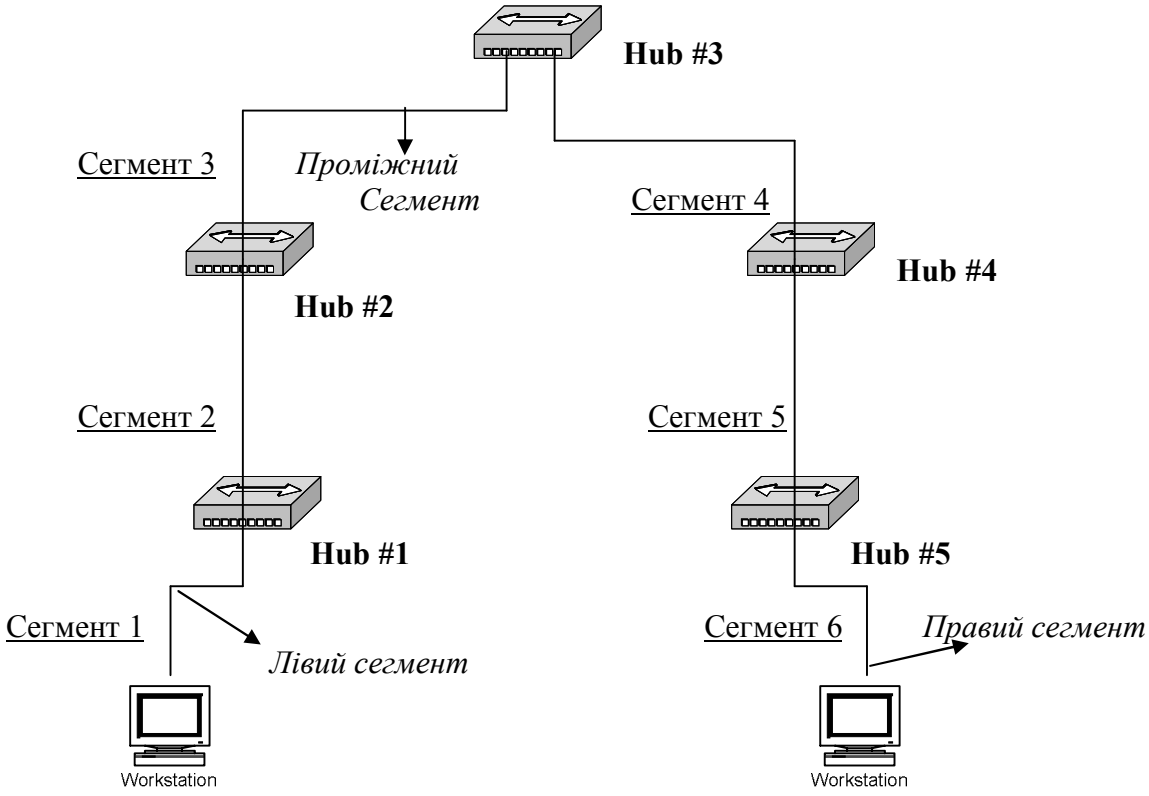
1. Наведіть алгоритми роботи випадкового методу доступу CSMA/CD?
2. Наведіть порівняльний аналіз випадкового та маркерного методів доступу. Їхні недоліки та переваги.
3. Дайте характеристику технології Ethernet 10 Base-T. Побудова сегментів і принципи їхнього об'єднання. Яка довжина фізичного сегмента в локальній мережі 10 BASE - T? Яка максимальна швидкість може бути досягнута в локальній мережі 10 BASE - T?
4. Опишіть методику розрахунку конфігурації Fast Ethernet.

5. Дайте характеристику технології побудови мереж Ethernet. Метод доступу до середовища в Ethernet.
6. Які принципи побудови локальних мереж на основі технології Token Ring і FDDI? У чому складається подібність і розходження цих технологій?
7. Приведіть порівняльний аналіз керування доступом до середовища в Token Ring і FDDI.
8. У яких випадках у мережах Ethernet виникають колізії? Що таке домен колізій?
9. Опишіть характеристики та апаратуру сегменту 100 Base - TX.
10. Дайте характеристику та опис апаратури сегментів Gigabit Ethernet?

Варіанти завдань

Розрахунок конфігурації мережі Ethernet

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



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.

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-	500м, 10Base-	1000м, 10Base-	60м, 10Base-T	900м, 10Base-	75м, 10Base-T

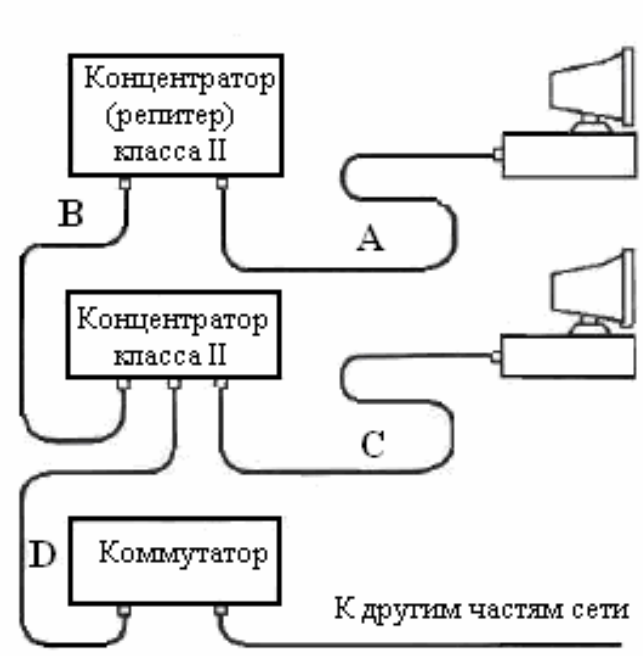
Варіант	Тип сегмента					
	сегмент 1	сегмент 2	сегмент 3	сегмент 4	сегмент 5	сегмент 6
	FL	FB	FL		FB	

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.

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

Визначити максимальну відстань D, на якої можна установити комутатор.



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

3. Є повторювач класу I. До нього підключені сегменти Tx, T4 як показано на малюнку. Всі довжини сегментів A, B, C, D, E, F наведені в таблиці.

3.1 Перевірте, чи буде відповідати дана мережа умовам коректної мережі.

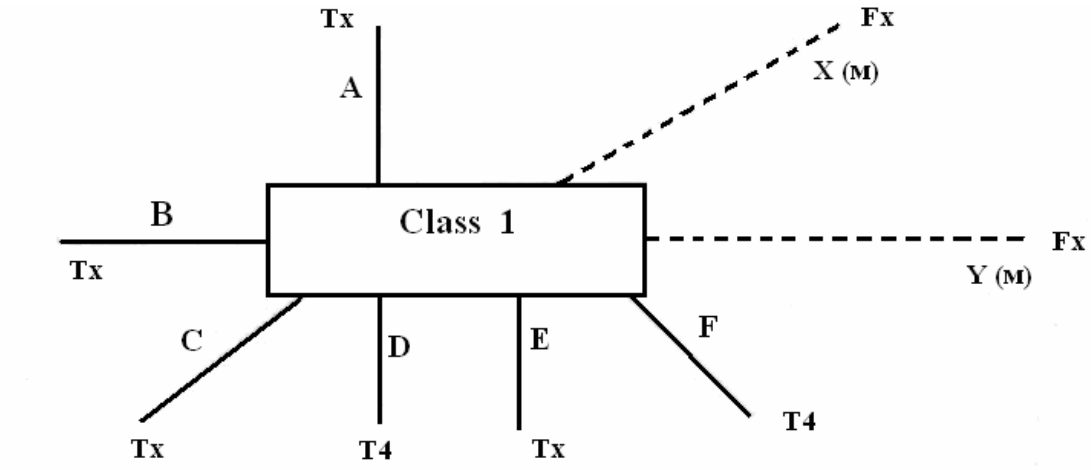
Необхідно підключити до цієї мережі один сегмент оптики Fx.

3.2 Яка буде максимальна довжина цього сегменту (x)?

Необхідно підключити додатково ще один сегмент Fx.

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

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



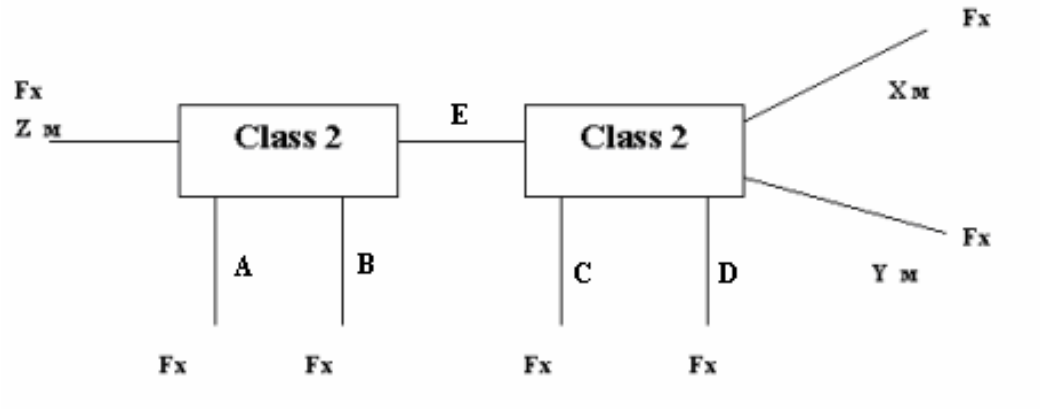
Варіант	Довжини сегментів, м					
	A	B	C	D	E	F
1	100	30	50	70	50	90
2	90	40	100	100	30	50
3	60	50	40	20	100	90
4	70	60	10	25	100	100
5	80	80	100	50	30	40

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

4. Мережа складається з двох повторювачів класу II і оптичних сегментів, як показано на малюнку. Відстань між повторювачами (E) і довжини сегментів (A, B, C, D) надані в таблиці.

4.1 Перевірте, чи буде відповідати дана мережа умовам коректної мережі. Необхідно підключити по черзі сегменти з довжинами X, Y, Z.

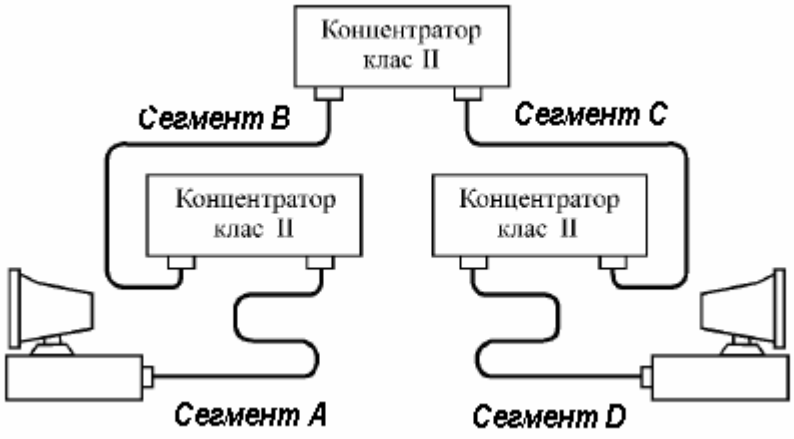
4.2 Обчисліть максимально можливі довжини для цих сегментів по черзі (X, Y, Z).



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

5. Перевірте коректність конфігурації мережі Fast Ethernet, представленої на малюнку. Типи і довжини сегментів (A, B, C, D) надані в таблиці.

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



Завдання №4
на тему: «Об'єднання мереж на основі мережного рівня»

Мета завдання №4:

1. Вивчення принципів роботи транспортних протоколів Інтернет;
2. Отримання практичних навиків у використанні адресації в IP-мережах та масок IP-адрес .

Перелік тем лекційного курсу щодо виконання завдання №4:

1. Багаторівнева структура стека TCP/IP.
2. Протокол IP.
3. Протоколи транспортного рівня TCP і UDP.
4. Адресація в IP-мережах.

Загальні рекомендації до виконання завдання №4

4.1 Типи адрес стека TCP/IP

Кожний комп'ютер у мережі TCP/IP може мати адреси трьох рівнів:

- локальні, або апаратні, адреси, які використовуються для адресації вузлів у межах підмережі;
- мережні, або IP-адреси, які використовуються для однозначної ідентифікації вузлів у межах всієї складеної мережі;
- доменні імена, або DNS-імена - символьні ідентифікатори вузлів, до яких часто звертаються користувачі.

4.2 Адресація в протоколі IP. Визначення маски підмережі

Класи IP-адрес. Адресація (IPv4) припускає використання 32-бітного коду. IP-адресу прийнято записувати у вигляді чотирьох октетів, у десятковій системі числення, наприклад:

IP-адреса ***192.168.7. 129*** – це код ***11000000 10101000 00000111 10000001***.

IP-адреса складається із двох частин: адреси мережі (***net***) і адреси вузла (***host***). Для зменшення трафіка в мережах з великою кількістю вузлів застосовується розділення вузлів за підмережами потрібного розміру. Адреса підмережі використовує кілька старших бітів хост–частини IP–адреси, решта молодших бітів – нульові. Тому в цілому IP–адреса складається з адреси мережі, підмережі та локальної хост–адреси, яка є унікальною для кожного вузла. Для

виділення номерів мережі, підмережі та хоста (вузла) використовується маска підмережі (***net mask***) – бітовий шаблон, в якому бітам, що використовуються для адреси підмережі, присвоюються значення 1, а бітам адреси вузла – значення 0. Так, маска мережі ***255.255. 255.0 (11111111 11111111 11111111 00000000)*** визначає, що поле адреси мережі містить 24 біта, а поле адреси вузла – 8 біт. Для наведеного вище прикладу адреси це означає: ***192.168.7*** – мережна частина (адресу мережі прийнято записувати ***192.168.7. 0)***, а ***129*** – адреса вузла в цій мережі.

Вузол може входити в кілька IP-мереж. У цьому випадку він повинен мати кілька IP-адрес, за числом мережевих зв'язків. Тоді IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

Існує 5 класів IP-адрес:

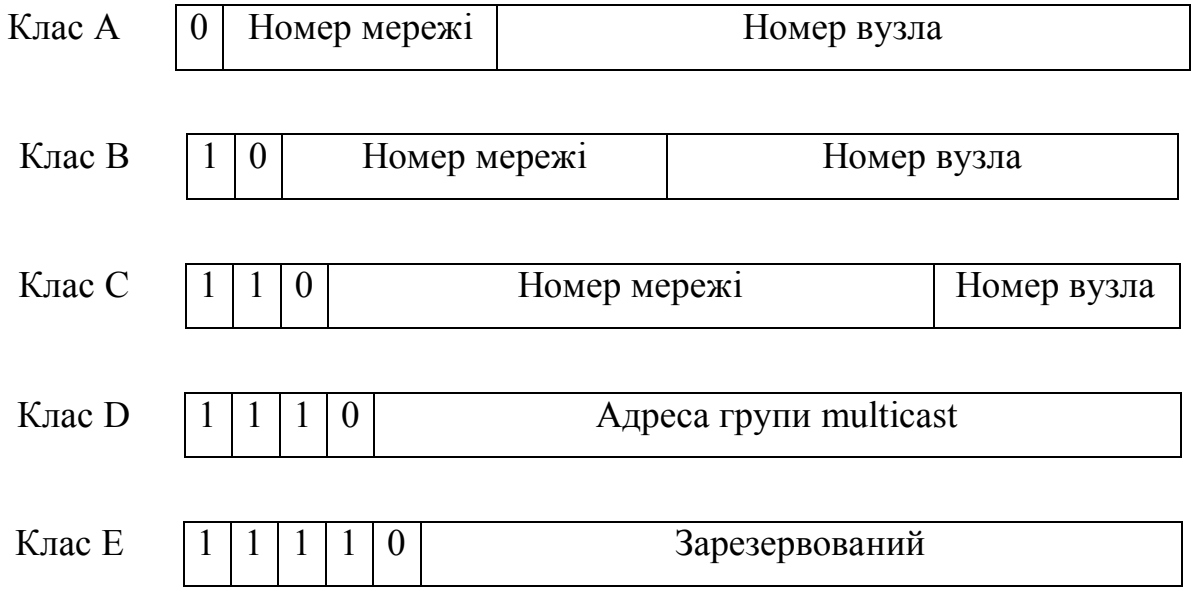


Рис.4.1 - Структура IP-адрес

У таблиці 4.1 наведені діапазони номерів мереж, що відповідають кожному класу мереж.

Особливі IP-адреси. У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес:

- якщо IP-адреса складається тільки із двійкових нулів, то вона позначає адресу того вузла, що згенерував цей пакет;
- якщо в полі номера мережі стоять 0, то за замовчуванням вважається, що цей вузол належить тій же самій мережі, що й вузол, який відправив пакет;
- якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, які перебувають у тій же

мережі, що й джерело цього пакета. Таке розсилання називається обмеженим широкомовним повідомленням (***limited broadcast***);

- якщо в полі адреси призначення стоять всі 1, то пакет, що має таку адресу розсилається всім вузлам мережі із заданим номером. Таке розсилання називається широкомовним повідомленням (***broadcast***);
- адреса 127.0.0.1 зарезервована для організації зворотного зв'язку при тестуванні роботи програмного забезпечення вузла без реального відправлення пакета по мережі. Ця адреса має назву ***loopback***.

Таблиця 4.1 - Характеристики адрес різного класу

Клас	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі	Маска
A	1.0. 0.0	126.0.0.0	2^{24}	255.0. 0.0
B	128.0. 0.0	191.255.0.0	2^{16}	255. 255.0.0
C	192.0. 1.0	223.255.255.0	2^{8}	255. 255.255.0
D	224.0. 0.0	239.255.255.255	multicast	
E	240.0. 0.0	247.255.255.255	зарезервований	

Форма групової IP-адреси - ***multicast*** - означає, що даний пакет повинен бути доставлений одразу декільком вузлам, які складають групу з номером, зазначеним у полі адреси. Вузли самі ідентифікують себе, тобто визначають, до якій із груп вони ставляться. Той самий вузол може входити в кілька груп. Такі повідомлення на відміну від широкомовних називаються мультимовним.

Використання підмереж. Одним зі способів вирішити проблему дефіциту IP-адрес і зростанню розмірів таблиць маршрутизації складається у використанні механізму підмереж (***subnetting***). Суть цього механізму складається в розбитті вузлової частини IP-адреси на два поля: поле адреси підмережі і поле адреси вузла (хоста). При цьому внутрішня структура мережі (розбиття її на підмережі) «не видна ззовні», що означає незалежність зовнішньої маршрутизації (доставки пакетів **до** або **від** даної мережі) від її внутрішньої структури. Для виділення підмереж у мережі адміністраторові необхідно визначити кількість сегментів і кількість вузлів у кожному сегменті з урахуванням потреб мережі. Наприклад, якщо необхідно розбити мережу 192.168.7. 0 (блок містить 256 адрес) на 8 підмереж з максимальною кількістю вузлів 30 у кожній підмережі, то по-перше, потрібно визначити кількість біт у полі адреси підмережі (3 біти тому що $2^3=8$) і в полі адреси вузла (5 біт тому що $2^5=32$). Максимальна кількість вузлів у підмережі дорівнює 30-ти, а не 32, тому що коди, що містять всі одиниці і всі

нулі, не можуть бути адресою вузла. Визначивши поля адреси підмережі і вузла, запишемо маску підмережі:

11111111 11111111 11111111 11100000 – ***255.255. 255. 224***.

Адреси підмереж, отримані в результаті застосування маски підмережі:

192. 168.7. 0 підмережа №0
192. 168.7.32 підмережа №1
192. 168.7.64 підмережа №2
192. 168.7.96 підмережа №3
192. 168.7. 128 підмережа №4
192. 168.7. 160 підмережа №5
192. 168.7. 192 підмережа №6
192. 168.7. 224 підмережа №7

Призначення IP-адрес. IP-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів, при цьому номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу ***Internet (Network Information Center, NIC)***, якщо мережа повинна працювати як складова частина Internet. У великих мережах підтримується автоматичний розподіл адрес на основі протоколу ***Dynamic Host Configuration Protocol (DHCP).*** Протокол DHCP працює відповідно до моделі клієнт-сервер. Комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на одержання IP-адреси. DHCP-сервер відгукується і посилає повідомлення відповідь, що містить IP-адресу з діапазону вільних для розподілу адрес. Передбачається, що DHCP-клієнт і DHCP-сервер перебувають в одній IP-мережі.

Фізична адреса. Фізична, або апаратна адреса вузла, визначається технологією, за допомогою якої побудована мережа, до якої входить даний вузол. Для вузлів, що входять у локальні мережі - це MAC-адреса мережевого адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, тому що управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти - ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним чином самим виробником.

Крайній лівий біт числа називається ознакою ***індивідуальної*** або ***групової*** адреси (I/G). Якщо біт дорівнює 0, то інші біти визначають індивідуальну адресу; значення 1 вказує на те, що інші біти визначають групову адресу. Якщо другий біт (U/L) дорівнює 0, то адреса підмережі є ***універсальною***, тобто призначеною комітетом IEEE, у противному випадку адреса є ***локальною***.

1 біт	1 біт	22 біта	24 біта
I/G	U/L		

Рис.4.2 - Структура MAC-адреси

Щоб відправити дейтаграму з одного комп'ютера на інший у локальній або глобальній мережі, відправник повинен знати фізичну адресу одержувача. Повинен існувати механізм перетворення IP-адрес, які задаються додатками, у фізичні адреси устаткування, що з'єднують комп'ютери з мережею. Для рішення цієї проблеми був розроблений протокол перетворення адрес ***ARP (Address Resolution Protocol).*** ARP веде таблицю відповідності між IP-адресами і фізичними адресами, яка називається ***таблицею APR***.

Доменні імена. Доменне, або символьне ім'я, наприклад, SERV1.IBM.COM – адреса, що призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домена. Така адреса, названа також DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet. Ієрархія доменних імен аналогічна ієрархії імен файлів, однак запис доменного імені починається із наймолодшої складової, а закінчується найстаршою. Наприклад, в імені partnering.microsoft.com складова partnering є ім'ям одного з комп'ютерів у домені microsoft.com. Сукупність імен, у яких кілька старших складових частин збігаються, утворять домен (domain) імен. Наприклад, імена www.chip.kiev.ua, www.itc.kiev.ua і www.infocity.kiev.ua входять у домен kiev.ua.

4.3 Транспортний протокол TCP

TCP (Transmission Control Protocol) - це один із самих широко розповсюджених протоколів транспортного рівня. Головна функція TCP полягає в доставці повідомлень без втрат, чого не може гарантувати протокол більш низького рівня IP (Internet Protocol). Для доставки повідомлень попередньо встановлюється з'єднання між процесом-відправником і процесом-одержувачем. Дане з'єднання здійснює надійну доставку дейтаграм. Протокол TCP робить повторну передачу перекрученого або загубленого пакета.

Процес обміну даними починається з передачі запиту на встановлення з'єднання від машини-відправника до машини-одержувача. У запиті втримується спеціальне ціле число - номер сокета **(socket).** У відповідь одержувач посилає номер свого сокета. Номера сокетів відправника й одержувача однозначно визначають з'єднання (звичайно, з'єднання також не можливо без вказівки IP-адреси відправника й одержувача, але це завдання вирішується протоколами більш низького рівня - IP).

Після встановлення з'єднання TCP починає передавати сегменти повідомлення. На більш низькому IP-рівні відправника сегменти розбиваються на одну або декілька дейтаграм. Пройшовши через мережу, дейтаграми надходять до одержувача, де IP-рівень знову збирає з них сегменти й передає їх TCP. TCP збирає всі сегменти в повідомлення. Від TCP повідомлення надходить до процесу-одержувача, де обробляється протоколом прикладного рівня.

4.4 Протокол передачі повідомлень UDP

Протокол ***UDP (User Datagram Protocol)*** є більш простим транспортним протоколом, чим протокол TCP. Він надає прикладним процесам послуги транспортного рівня, які мало чим відрізняються від послуг більш низького рівня, наданих протоколом IP. Протокол UDP забезпечує доставку дейтаграм, але не вимагає підтвердження їхнього одержання. Тому він не вимагає встановлення з'єднання між передавальним і приймаючим процесами.
Протокол UDP використовується в тих випадках, коли потрібно передати дані без установлення з'єднання, у клієнт-серверних запитах і додатках, у яких важлива швидкість обміну даними, наприклад при передачі інформації в інтерактивному режимі.

4.5 Номера портів і сокети

Додаток (процес), що використовує TCP однозначно визначається числом - номером порту (сокета). Номера портів можна призначати процесам довільно, але для полегшення взаємодії між різними програмами прикладного рівня прийняті угоди про номери портів, які закріплені за певними службами Internet. Номера портів найбільш відомих служб мережі наведені у файлі SERVICES .

У форматі повідомлення протоколу TCP під номер порту приділяється 16 біт, тому максимально можливим номером порту є число 65535. Номера портів від 0 до 255 строго зарезервовані під системні потреби, їх не допускається використовувати в прикладних програмах. В інтервалі від 256 до 1023 багато портів також використовуються мережевими службами, тому і їх не рекомендується застосовувати для прикладних потреб. Як правило, більшість прикладних додатків, побудованих на основі TCP/IP використовують номери портів у діапазоні від 1024 до 5000. Рекомендується використовувати номери від 3000 до 5000, номери вище 5000 використовуються найчастіше для короткострокового застосування.

Будь-який канал зв'язку в TCP визначається двома числами - ця комбінація називається сокетом. Таким чином, сокет визначається IP-адресою вузла й номером порту, використаним програмним забезпеченням TCP. При з'єднанні будь-яка машина однозначно визначена IP-адресою, а кожний процес - портом,

тому з'єднання між двома процесами однозначно визначається сокетом. Наприклад, якщо кілька машин пошлють запити на з'єднання, у яких зазначені однакові порти джерела й одержувачі, плутанини із з'єднаннями не виникає, тому що IP-адреси у всіх машин різні, отже, кожне з'єднання буде однозначно визначено своїм сокетом.

Завдання до контрольної роботи:

Контрольні питання

1. Опишіть структура стека протоколів TCP/IP? Як рівні стека TCP/IP відповідають рівням моделі OSI?
2. Опишіть типи адрес стека TCP/IP і порядок призначення IP адрес.
3. Наведіть форми запису і класи IP - адрес? Які існують особливі IP - адреси. Що таке маски адрес і яким чином вони використовуються при IP-адресації?
4. Дайте визначення поняттю «домен». Що являє собою доменна система символьних імен у стеці TCP/IP? Яким чином установлюється відповідність між доменними іменами і IP - адресами? Служба доменних імен DNS.
5. Дайте характеристику протоколу IP. Основні завдання протоколу. Структура IP- пакета.
6. Дайте характеристику протоколу транспортного рівня TCP. Як у протоколі TCP реалізований алгоритм ковзного вікна?
7. Яким чином установлюється TCP-з'єднання між двома прикладними процесами? Дайте визначення поняттю сокет.
8. Опишіть принципи роботи протоколу дозволу адрес ARP.
9. Опишіть принципи роботи протоколу передачі повідомлень UDP. У чому його відмінність від протоколу TCP ?
10. Дайте характеристику протоколам маршрутизації RIP і OSPF.

Варіанти завдань

1. а) IP адреса деякого вузла підмережі дорівнює 198.65.12.135, а значення маски для цієї підмережі - 255.255.255.128. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цій підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 127.0.0.1
2) 4) 13.130.118.51

3) 193.64.81.256
4) 13.45.14.255
5) 3) 198.4.37.15
6) 175.15.0.0

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу А - **115.0.0.0** на 16 підмереж. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **115.84.36.1.**

2. а) IP адреса деякого вузла підмережі дорівнює 195.165.30.94, а значення маски для цій підмережі - 255.255.255.192. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 125.0.0.1
2) 123.0.0.0
3) 198.13.321.252
4) 127.0.0.3
5) 11.4.37.255
6) 193.256.1.0

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу А - **125.0.0.0** на 32 підмережі. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **125.35.13.1**.

3. а) IP адреса деякого вузла підмережі дорівнює 193.175.41.68, а значення маски для цій підмережі - 255.255.255.224. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 197.60.74.0
2) 127.0.0.0
3) 121.0.1.1
4) 114.0.3.255
5) 129.0.1.0
6) 195.256.1.16

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу А - **113.0.0.0** на 64 підмережі. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **113.10.12.1**.

4. а) IP адреса деякого вузла підмережі дорівнює 198.22.54.11, а значення маски для цій підмережі - 255.255.255.240. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 128.256.12.5
2) 13.136.17.255
3) 127.0.0.2
4) 204.0.0.1
5) 221.4.37.0
6) 193.256.1.16

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу А - **121.0.0.0** на 128 підмережі. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **121.9.15.1**.

5. а) IP адреса деякого вузла підмережі дорівнює 198.155.160.38, а значення маски для цій підмережі - 255.255.255.252. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 197.255.255.0
2) 13.135.301.18
3) 121.13.123.255
4) 104.0.3.1
5) 196.4.37.105
6) 127.0.0.4

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу А - **118.0.0.0** на 256 підмереж. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **118.7.13.1**.

6. а) IP адреса деякого вузла підмережі дорівнює 192.55.16.42, а значення маски для цій підмережі - 255.255.255.248. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 127.0.2.1
2) 13.1.1.1
3) 21.13.128.255
4) 204.0.3.1
5) 216.40.137.105
6) 198.256.18.161

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу B - **185.115.0.0** на 16 підмереж. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **185.115.68.1**.

7. а) IP адреса деякого вузла підмережі дорівнює 129.122.158.15, а значення маски для цій підмережі - 255.255.192.0. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 128.90.10.256
2) 193.13.13.0
3) 124.1.0.0
4) 124.0.3.1
5) 127.0.8.2
6) 93.204.1.255

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу B - **134.98.0.0** на 32 підмережі. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **134.98.10.1**.

8. а) IP адреса деякого вузла підмережі дорівнює 129.34.124.36, а значення маски для цій підмережі - 255.255.224.0. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 128.0.255.255
2) 127.0.0.5
3) 221.13.123.0
4) 183.0.302.15
5) 216.4.37.15
6) 113.12.0.0

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу B - **129.76.0.0** на 64 підмережі. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **129.76.15.1**.

9. а) IP адреса деякого вузла підмережі дорівнює 129.38.64.52, а значення маски для цій підмережі - 255.255.240.0. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 127.0.0.6
2) 4) 134.131.313.13
3) 201.13.123.0
4) 87.0.3.255
5) 206.4.77.5
6) 193.255.1.16

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу B - **133.118.0.0** на 128 підмереж. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **133.118.13.1**.

10. а) IP адреса деякого вузла підмережі дорівнює 129.112.78.33, а значення маски для цій підмережі - 255.255.248.0. Визначте адресу підмережі. Яке максимальне число вузлів може бути в цієї підмережі?

б) Які з нижче наведених адрес не можуть бути використані в якості IP-адреси кінцевого вузла мережі, підключеної до Інтернет? Для синтаксично правильних адрес визначите їхній клас.

1) 197.20.50.0

2) 103.103.103.103
3) 122.256.123.205
4) 127.0.0.7
5) 186.4.255.255
6) 193.0.1.0

в) Визначите маску постійної довжини, що дозволяє розбити базову мережу класу В - **182.34.0.0** на 256 підмереж. Визначите адреси перших 8-ми із цих підмереж і максимально можливу кількість хостів у кожній підмережі. До якої підмережі належить хост із адресою **182.34.1.1**.

Завдання №5
на тему: «Устаткування локальних мереж»

Мета завдання №5:

Вивчення устаткування локальних мереж;

Закріплення теоретичного матеріалу щодо функціонального призначення мережного комунікаційного обладнання;

Отримання практичних навиків у конфігуруванні комп'ютерів, підключених до мережі.

Отримання практичні навики при роботі з мережною операційною системою комутаційного обладнання та маршрутизаторів Cisco.

Обладнання: Комутатор Cisco Catalyst 2950, Cisco Catalyst 2960, Packet Tracer 5.3.2

Перелік тем лекційного курсу щодо виконання завдання №5:

1. Огляд топологій фізичних зв'язків.
2. Фізична і логічна структуризації мережі за допомогою мережного комунікаційного обладнання.
3. Стек протоколів TCP/IP.

Загальні рекомендації до виконання завдання №5

Завдання слід виконати в середовищі програмного емулятора Cisco Packet Tracer 5.3.2. Докладніша інформація про емулятор, а також про обладнання Cisco, вбудовану операційну систему IOS наведена у додатках В, Г і Д.

Порядок виконання завдання №5

1. Вивчити теоретичний матеріал, наведений у додатках В, Г і Д.
2. Відповісти на всі контрольні запитання.
3. Виконати в Packet Tracer практичну частину завдання.
4. Виконати в Packet Tracer завдання згідно варіанту. Надати у контрольній роботі скріншоти, які демонструють працездатність побудованої мережі. (Обов'язково скріншот топології і скріншот виконання команди ping згідно варіанту). Оформити висновки.

Контрольні питання

1. Яку максимальну кількість пристроїв в мережі підтримує Packet Tracer?
2. Які типи мережевих пристроїв і з'єднань можна використовувати в Packet Tracer?

3. Яким способом можна перейти до інтерфейсу командного рядка устаткування?
4. Як конфігурувати пристрої з іншого комп'ютера?
5. Як додати в топологію і налаштувати нове устаткування?
6. Як зберегти конфігурацію устаткування в *.txt файл?

Практична частина

1. Додати на робочу область програми 2 комутатора Switch-PT. За замовчуванням вони мають ім'я – Switch0 і Switch1.
2. Додати 4 комп'ютера з іменами за замовчуванням PC0, PC1, PC2, PC3.
3. З'єднати устаткування в мережу Ethernet, як показано на рис.5.1.

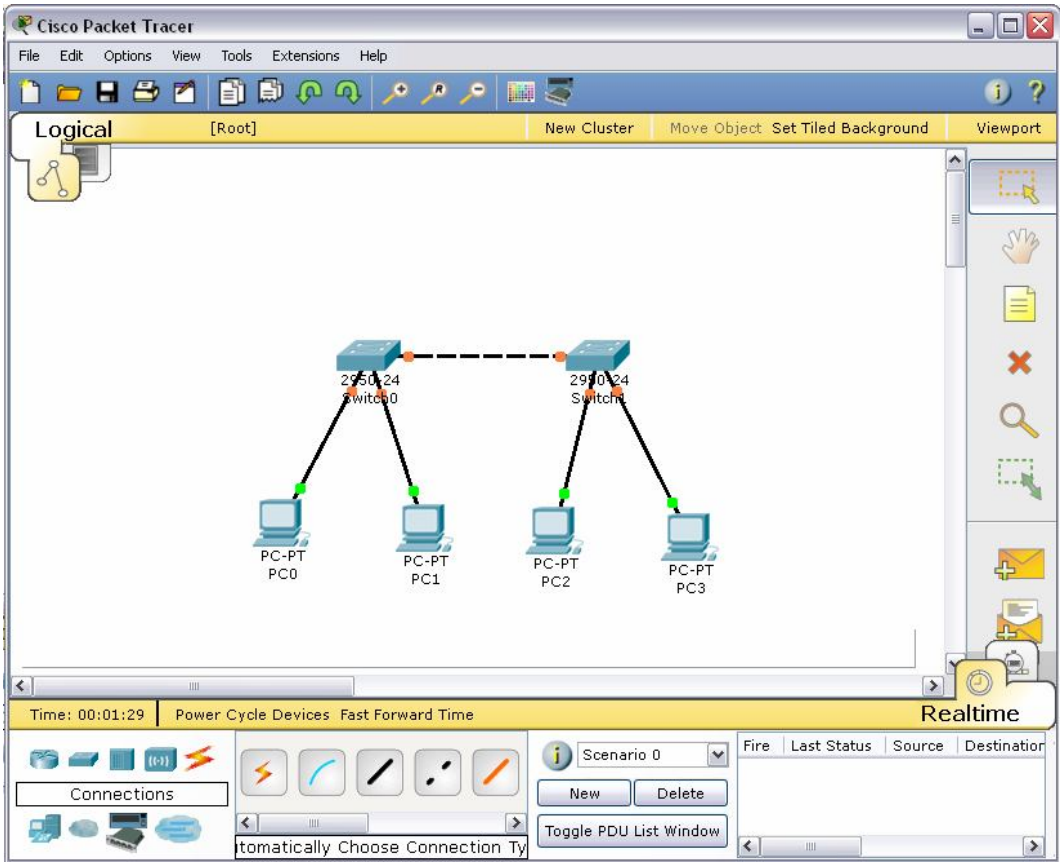


Рисунок 5.1 – Фізична топологія мережі для симуляції

4. Зберегти створену топологію, натиснувши кнопку Save (в меню File->Save).
5. Відкрити властивості устаткування PC0 натиснув на його зображені. Перейти до вкладки Desktop і виконати симуляцію роботи run натиснувши Command Prompt.

6. Перелік команд можна отримати, якщо ввести ? і натиснути Enter. Для конфігурування комп'ютера слід скористатися командой ipconfig з командного рядка, наприклад, ipconfig 192.168.1.2 255.255.255.0

IP адресу і маску також можна вводити в зручному графічному інтерфейсі устаткування (рис.5.2). Поле DEFAULT GATEWAY – адреса шлюзу не важна, тому що мережа, що створюється не потребує маршрутизації.

Аналогічним способом слід налаштувати кожний комп'ютер, надавши їм IP-адреси з табл.5.1.

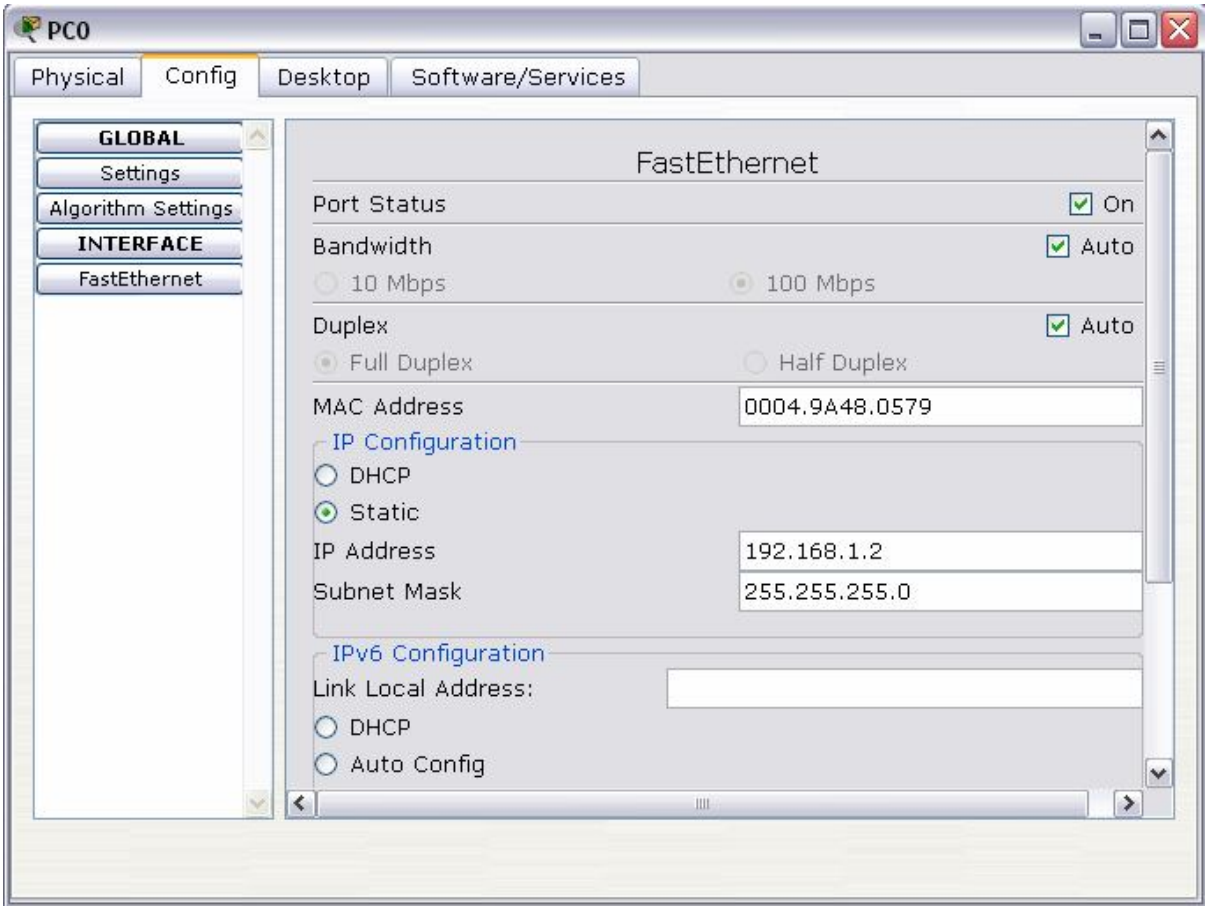


Рисунок 5.2 – Вкладка Config робочої станції PC0

Таблиця 5.1 – Перелік IP-адрес для конфігурації мережі

Устаткування	IP ADDRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

7. На кожному комп’ютері переглянути назначені адреси командою ipconfig без параметрів.

8. Якщо всі пункти виконані вірно, то можна пропінгувати будь-який комп’ютер з будь-якого іншого комп’ютера. Наприклад, з комп’ютера PC3 виконати пінгування до комп’ютера PC0. Звіт про виконання команди ping наведений на рис.5.3.

9.

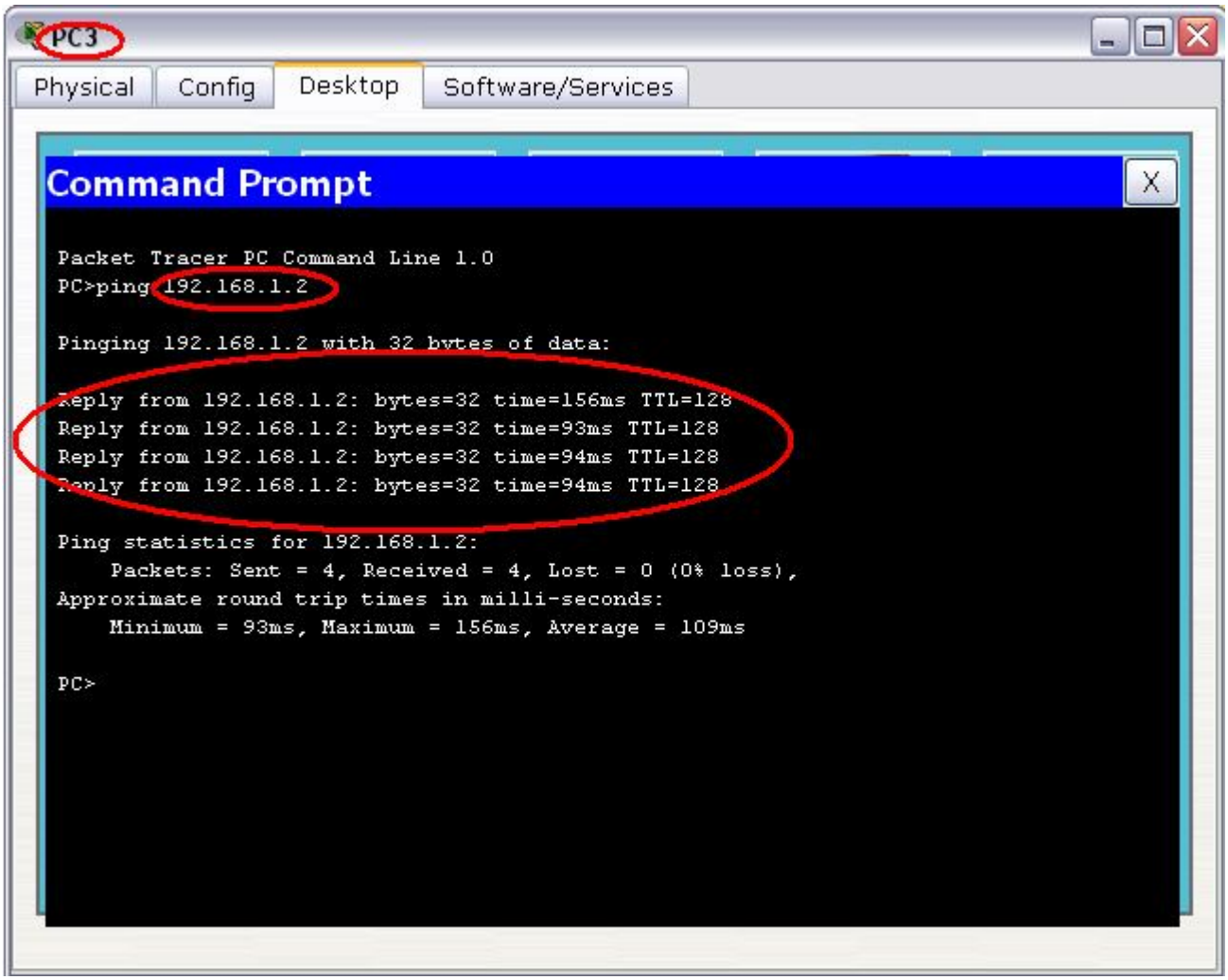
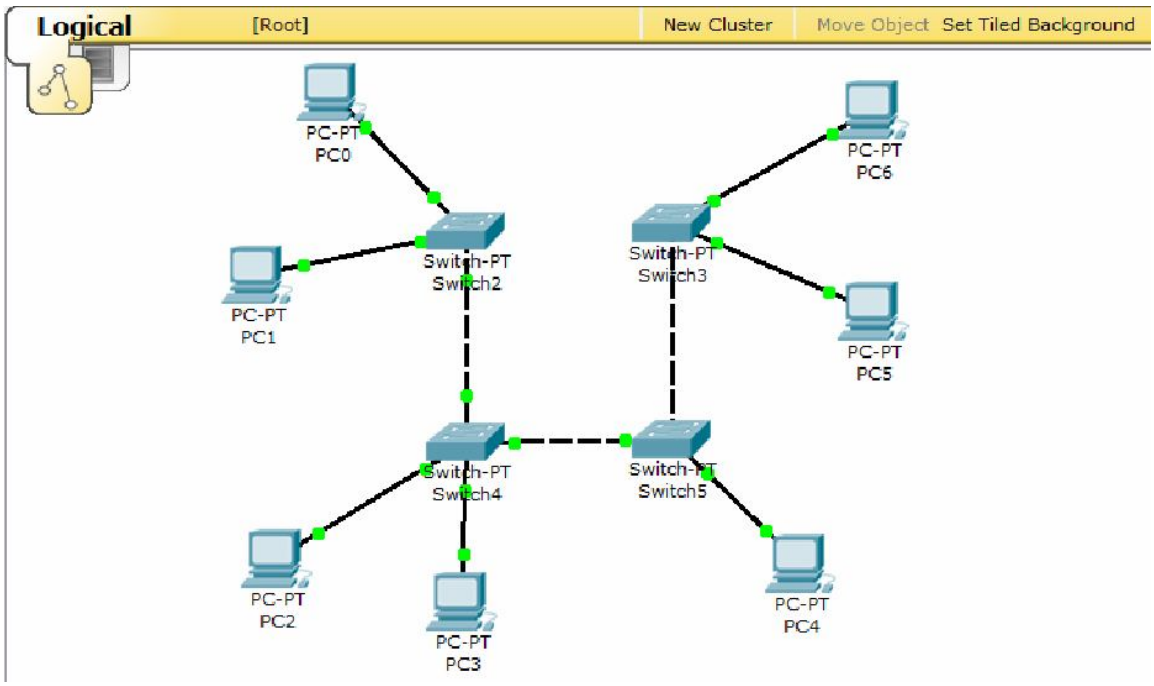


Рисунок 5.3 – Звіт про виконання команди ping між вузлами PC3 і PC0

Завдання для самостійної роботи

1. Створить топологію



2. Призначте комп'ютерам адреси згідно варіанту (v=1-10). Наприклад, для варіанту 7 (v=7) і комп'ютер PC1 має IP ADDRESS 7.1.1.1

Таблиця 5.2 – Варіанти для конфігурування комп'ютерів мережі

Устаткування	IP ADDRESS	SUBNET MASK
PC0	v.1.1.1	255.0.0.0
PC1	v.1.1.2	255.0.0.0
PC2	v.1.1.3	255.0.0.0
PC3	v.1.1.4	255.0.0.0
PC4	v.1.1.5	255.0.0.0
PC5	v.1.1.6	255.0.0.0
PC6	v.1.1.7	255.0.0.0

3. Призначте комп'ютерам різні ім'я в командному рядку.
4. Якщо все буде зроблено вірно, то стане можливим пропінгувати будь-який комп'ютер з іншого.

Таблиця 5.3 – Варіанти виконання команди ping для перевірки працездатності мережі

Варіант v	Ping з вузла	Ping до вузла	Варіант v	Ping з вузла	Ping до вузла
1	PC0	PC5	**7**	PC6	PC4
2	PC1	PC6	**8**	PC0	PC5
3	PC2	PC0	**9**	PC1	PC6

4	PC3	PC1	**10**	PC2	PC0
5	PC4	PC2			
6	PC5	PC3			

Завдання №6
на тему: «Конфігурування маршрутизаторів»

Мета завдання №6:

Закріплення теоретичного матеріалу щодо функціонального призначення мережного комунікаційного обладнання;

Отримання практичні навики при роботі з мережною операційною системою комутаційного обладнання та маршрутизаторів Cisco.

Перелік тем лекційного курсу щодо виконання завдання №6:

1. Огляд топологій фізичних зв'язків.
2. Фізична і логічна структуризації мережі за допомогою мережного комунікаційного обладнання.
3. Стек протоколів TCP/IP.

Загальні рекомендації до виконання завдання №6

Завдання слід виконати в середовищі програмного емулятора Cisco Packet Tracer 5.3.2. Докладніша інформація про емулятор, а також про обладнання Cisco, вбудовану операційну систему IOS наведена у додатках В, Г і Д.

Порядок виконання завдання №6

1. Вивчити теоретичний матеріал, наведений у додатках В, Г і Д.

2. Відповісти на всі контрольні запитання.

3. Виконати в Packet Tracer практичну частину завдання.

4. Виконати в Packet Tracer завдання згідно варіанту. Надати у контрольній роботі такі дані:

4.1 Таблицю розрахованих адрес підмереж

4.2 Скріншот логічної структури мережі

4.3 Таблицю з параметрами стеку TCP/IP для вузлів мережі

4.4 Листинг команд конфігурування маршрутизатора в Cisco IOS (з файлу *.txt)

4.5 Скріншот виконання команди show ip interface brief

4.6 Скріншот виконання команди ping між будь-якими двома вузлами мережі

4.7 Скріншот завантаження HTTP сторінки на будь-який вузол з серверу.

4.8 Висновок

Теоретична частина

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 к COM-порту мережевого пристрою, або в рамках сеансу протоколу Telnet, пристрій можна перевести в один з режимів. Нас цікавлять наступні режими.

Режим користувача – це режим перегляда, 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 по першим унікальним символам. При натисненні табуляції IOS сам доповнить команду до повного імені.

При введені 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 вимагають багаторядкових команд. Для входу в режим глобального конфігурування використовується команда привілейованого режиму configure. При введені 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 приватного 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 по протоколу Telnet:

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

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

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

Команда **enable password** обмежує доступ к 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 6.1 – 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.

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 приватний вид 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?

Практична частина

1. 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. 6.2.

Таблиця 6.2 – 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. 6.1). Використовуйте модель маршрутизатора за замовчуванням – Generic.

2. Сконфігуруємо стек протоколів кожного вузла мережі відповідно з даними табл.6.3.

3. Здійснімо тестування мережі використовуючи команду ping.

Таблиця 6.3 – 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	

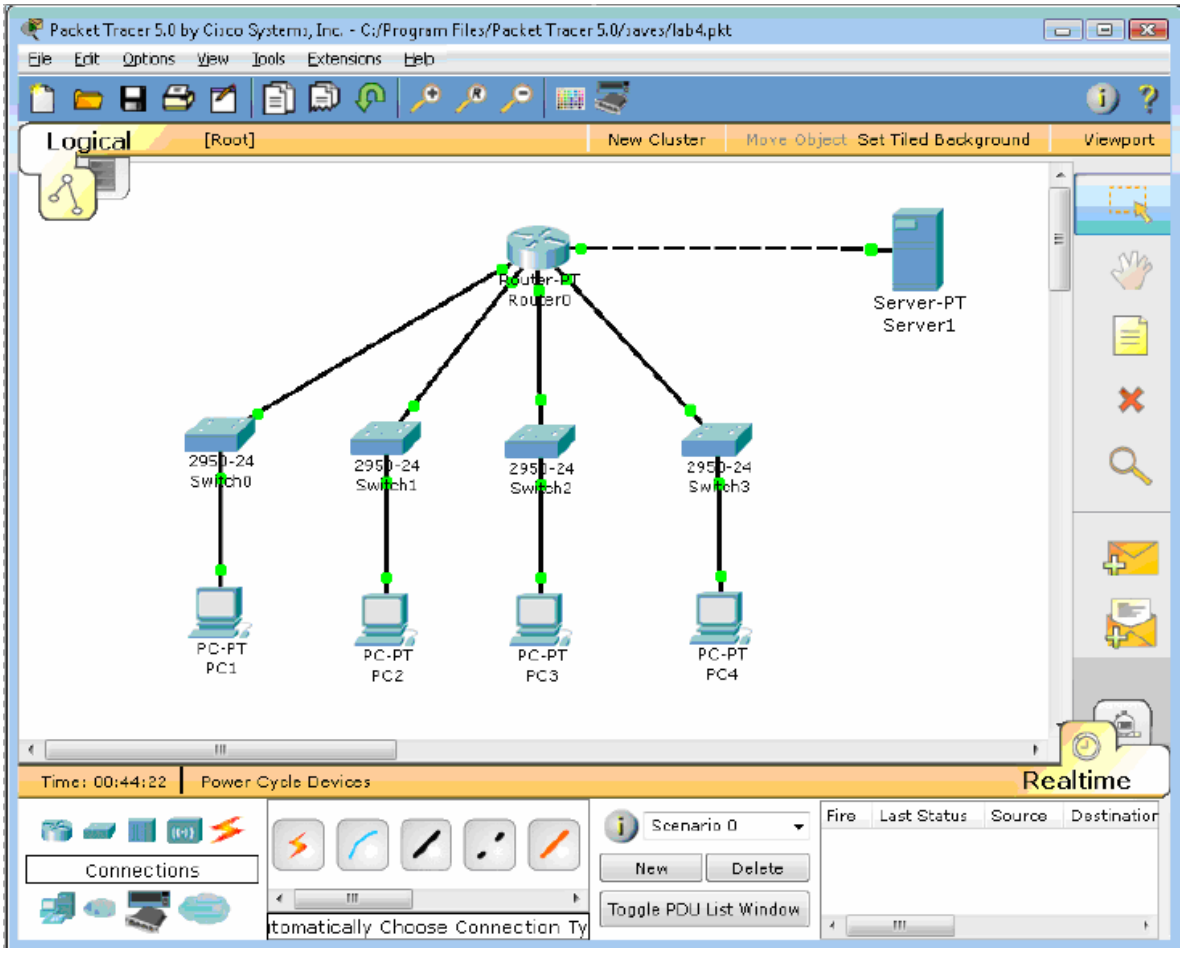


Рисунок 6.1 – Конфігурація мережі з 4-ма підмережами

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.

Основні Show команди

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

Router0>**show ?**

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

6. Можна побачити часи

Router0>**show clock**

7. Во флеш-пам'яті мереженого 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 збої живлення.

Router0>**show flash**

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

Router0>**show history**

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

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

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

Router0>**show hosts**

12.Наступна команда виводить детальну інформацію про кожний інтерфейс:

Router0>**show interfaces**

13.Команда

Router0>**show sessions**

Виведе інформацію про кожну telnet сесію.

14.Команда

Router0>**show terminal**

показує параметри конфігурації терміналу.

15. Список всіх користувачів, що приєднані до пристрою по термінальним лініям можна побачити використовуючи команду:

Router0>**show users**

16. Команда

Router0>**show controllers**

показує стан контролерів інтерфейсів.

17. Перейдемо до привілейованого режиму

Router0>**en**

18. Введіть команд для перегляду всіх доступних **show** команд.

Router0# **show ?**

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

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

Router0# **show running-config**

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

20. Наступна команда дозволяє переглянути поточний стан протоколів третього рівня

Router0# **show protocols**

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

Порядок виконання завдання №6 згідно варіанту

1. Розрахувати кількість підмереж згідно з даними табл.6.4.
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 6.4 – 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
10	182.207.120.0	/24	Розбити мережу на 4 підмережі

Додаток А

Дані для проведення розрахунку конфігурації мережі Ethernet

Таблиця 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 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 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 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.

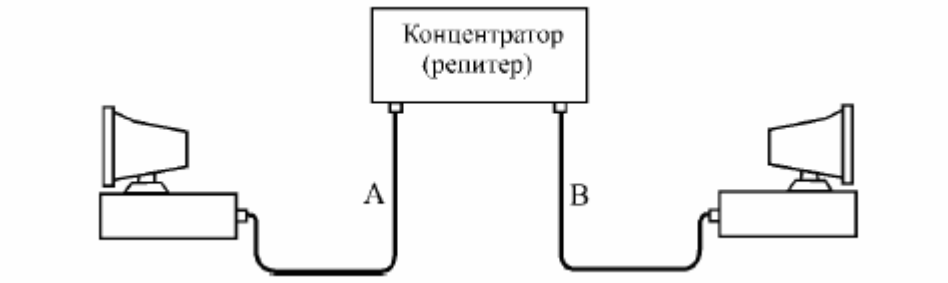
Модель 1 виділяє три можливі конфігурації мережі Fast Ethernet:

- 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).

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

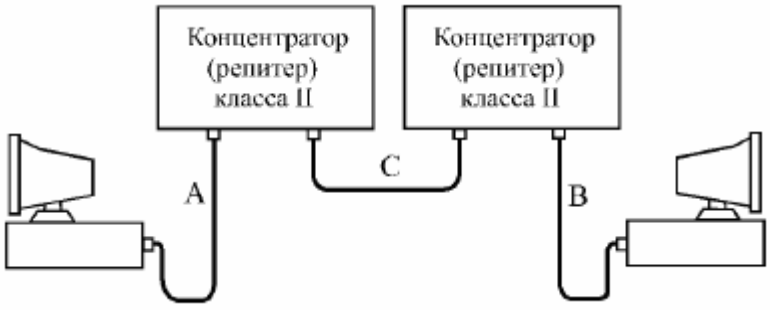


В даному випадку треба обмежувати довжину кабелів A і B мережі відповідно до таблиці.

Максимальна довжина кабелів у конфігурації з одним концентратором

Вид кабелю A	Вид кабелю B	Клас концентра-тора	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

- З'єднання двох абонентів мережі за допомогою двох репітерні 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.

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.

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.

Додаток В
Опис компонентів устаткування Cisco

Склад внутрішніх компонентів Cisco в певній мірі залежить від призначення устаткування, потужності блоку живлення, конструкції та складу модулів. Всі устаткування практично завжди мають деякі основні компоненти. Зокрема, будь-який маршрутизатор або комутатор можна розглядати як спеціалізований комп'ютер, в якому аналогічні компоненти можна використовувати для тієї ж мети. Устаткування Cisco можуть включати не тільки внутрішні компоненти, але і зовнішні, склад яких також залежить від моделі устаткування.

Внутрішні компоненти

До числа найбільш використовуваних компонентів відносяться модулі оперативної пам'яті (флеш-пам'ять, ПЗП), процесор, об'єднувальна плата и енергонезалежний ОЗП (рис.В.1)

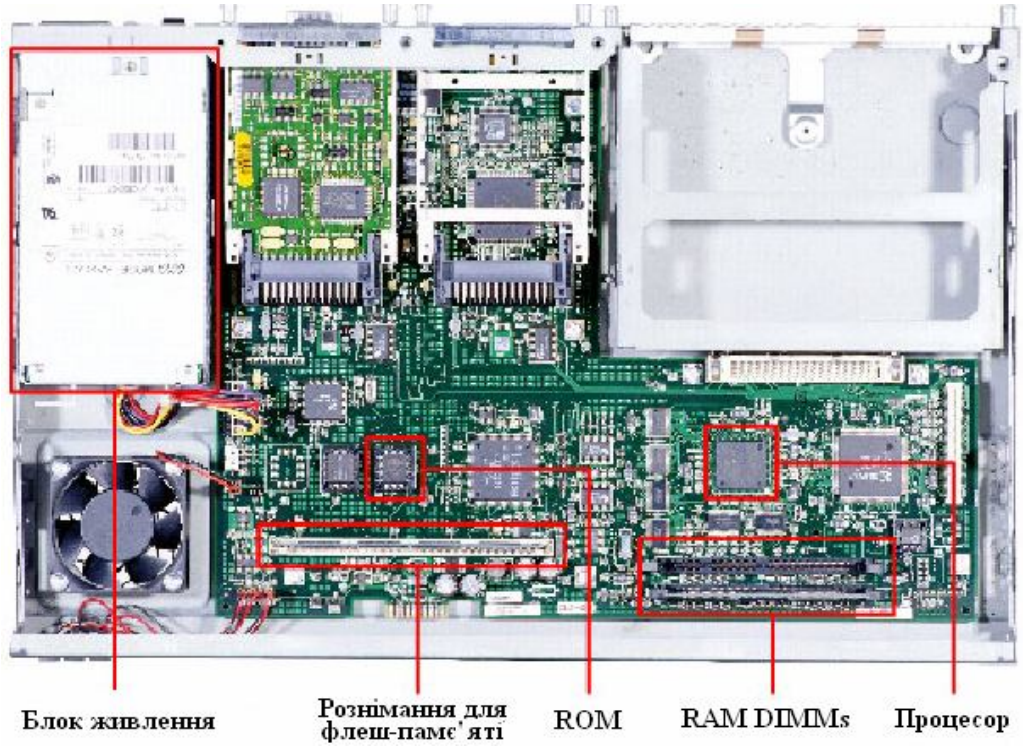


Рисунок В.1 – Внутрішні компоненти Cisco Router 2600

Оперативна пам'ять. Моделі DRAM (Dynamic RAM – динамічний ОЗП) застосовуються в устаткуваннях Cisco з тією ж метою, що і в персональному комп'ютері: в якості оперативної пам'яті. Оперативна пам'ять в маршрутизаторах Cisco має наступні характеристики:

– енергозалежна;

– пересаписувана;
– об’єм від 16 до 512 Мбайт;

і функції:

– зберігає таблицю маршрутизації (routing table);
– містить ARP кеш;
– буферізує пакети;
– під час роботи маршрутизатора містить файл робочої конфігурації (running-config file).

На маршрутизаторах Cisco виконується високопродуктивна операційна система IOS (Cisco Internetworking Operating System), створена на базі ОС UNIX, яка фізично розміщена в енергонезалежній пам’яті маршрутизатора (FLASH).

Флеш–пам’ять. Флеш–пам’ять в маршрутизаторах Cisco використовується приблизно з тією ж метою, що і жорсткий диск на комп’ютері. Флеш–пам’ять має наступні характеристики:

– енергонезалежна;
– пересаписувана;
– об’єм від 8 до 128 Мбайт;

і функції:

– зберігає образ або образи Cisco IOS;
– зберігає файли конфігурації.

Постійний запам’ятовуючий пристрій. Постійний запам’ятовуючий пристрій призначений тільки для читання. Для переходу на нову версію потрібно замінити мікросхему ПЗП, котрий має наступні характеристики:

– енергонезалежний;
– не пересаписуваний;

і функції:

– зберігає спрощену (резервну) версії Cisco IOS, призначену для використання у тому випадку, якщо всі інші способи загрузки устаткування не вдаються;
– містить код функції ROM Monitor, який застосовується у тому випадку, якщо програмне забезпечення Cisco IOS, яке знаходиться на флеш-пам’яті, спотворено і не завантажується. А також він служить для діагностики та перенастроювання конфігурації на низькому рівні (наприклад, в тому випадку, якщо хтось змінив пароль, виключив тим самим доступ мережевого адміністратора до маршрутизатора).

Енергонезалежний ОЗП. Енергонезалежний ОЗП (NVRAM) має наступні характеристики:

– енергонезалежний;
– пересаписуваний;
– об’єм від 32 до 256 Кбайт;

і функції:

– вказує шлях до образа Cisco IOS і файлу пускової конфігурації;
– зберігає файл пускової конфігурації (startup-config file).

Процесор. Процесор в устаткуваннях Cisco служать тієї ж меті, що і в ПК: він є «мозком» устаткування. В більшості устаткування Cisco програмне забезпечення виконує багато обчислень, і для цього використовується процесор. В комутаторах процесор – це не такий важливий елемент, як в маршрутизаторах, тому що загальна частина обчислень виконується комутатором за допомогою спеціалізованих апаратних компонентів, що називаються модулями ASIC.

Об’єднувальна плата. Об’єднувальну плату можна порівняти з магістраллю, по якій ідуть всі взаємодії всередині мереженого устаткування. Її продуктивність має велике значення в комутаторах і інших устаткуваннях з високою густотою розміщення інтерфейсів.

Зовнішні компоненти

До зовнішніх компонентів відноситься консольний інтерфейс, допоміжний (AUX) інтерфейс, інтерфейси Ethernet, послідовні інтерфейси і слоти PCMCIA (рис.В.2)

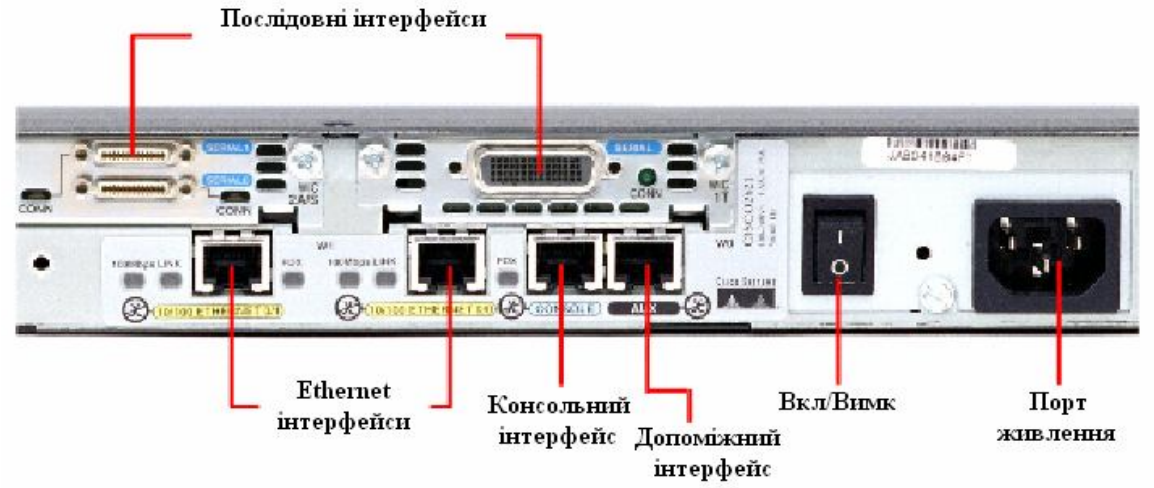


Рисунок В.2 – Внутрішні компоненти Cisco Router 2600

Консольний інтерфейс. Консольний інтерфейс використовується для введення до системи Cisco IOS первісної інформації про конфігурацію і є окремим рознімання (connector) RJ-45. Консольний інтерфейс – це низькошвидкісний асинхронний послідовний інтерфейс, який має особливе розташування виводів, і встановлює певні вимоги до типу кабелю, який повинен

використовуватися для підключення станції керування (рис.В.3). Консольні кабелі зазвичай поставляються разом з маршрутизатором.

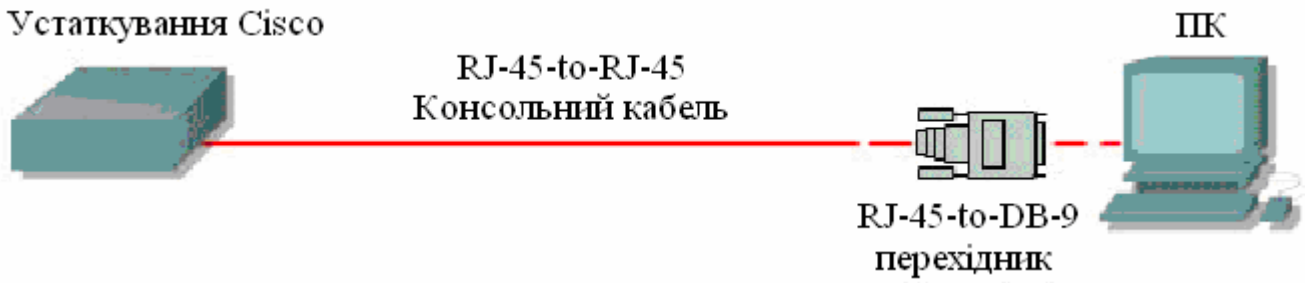


Рисунок В.3 – Схема підключення до консольного інтерфейсу

Допоміжний інтерфейс. Допоміжний інтерфейс (AUX) - це ще один низькошвидкісний асинхронний послідовній інтерфейс, який звичайно використовується для підключення модему, що дозволяє здійснювати дистанційне адміністрування.

Ethernet інтерфейси. Ethernet інтерфейс – це інтерфейс, який дозволяє підключити дане мережене устаткування к Ethernet мережі.

Послідовний інтерфейс. Існує шість загальних специфікацій послідовного підключення: EIA/TIA-232, X.21, V.35, EIA/TIA-449, EIA-530 и HSSI. Послідовний інтерфейс призначений для підключення DCE[1] и DTE[2] устаткування.

[1] DCE – Data Communications Equipment – Апаратура передачі даних. Як правило це модем (модуль даних або модулятор/демодулятор пакетів на боці мережі каналу зв'язку), призначений для забезпечення сумісності двійкових даних, що передаються послідовно від джерела або передавача, з каналом зв'язку.

[2] DTE – Data Terminal Equipment – Термінальне устаткування. Апаратура користувача лінії зв'язку, яка виробляє дані для передачі лінією зв'язку и підключається безпосередньо к апаратурі передачі даних DCE. Це, наприклад, комп'ютери, комутатори і маршрутизатори.

Додаток Г
Основні відомості про операційну систему Cisco IOS

На маршрутизаторах Cisco виконується високопродуктивна операційна система IOS (Cisco Internetworking Operating System), створена на базі ОС UNIX, яка фізично розміщена в енергонезалежній пам'яті маршрутизатора (FLASH).

Процес ініціалізації маршрутизатора виконується в наступній послідовності:

1) POST (Power On Self Test) – тестування обладнання після включення живлення.
2) Bootstrap IOS – програма завантаження основного IOS.
3) Cisco IOS – основна операційна система маршрутизатора.
4) Файл конфігурації із NVRAM. Виконуються команди, які зберігаються в цьому файлі.

Після автоперевірки включення живлення в процесі ініціалізації маршрутизатора відбуваються наступні події (рис.Г.1):

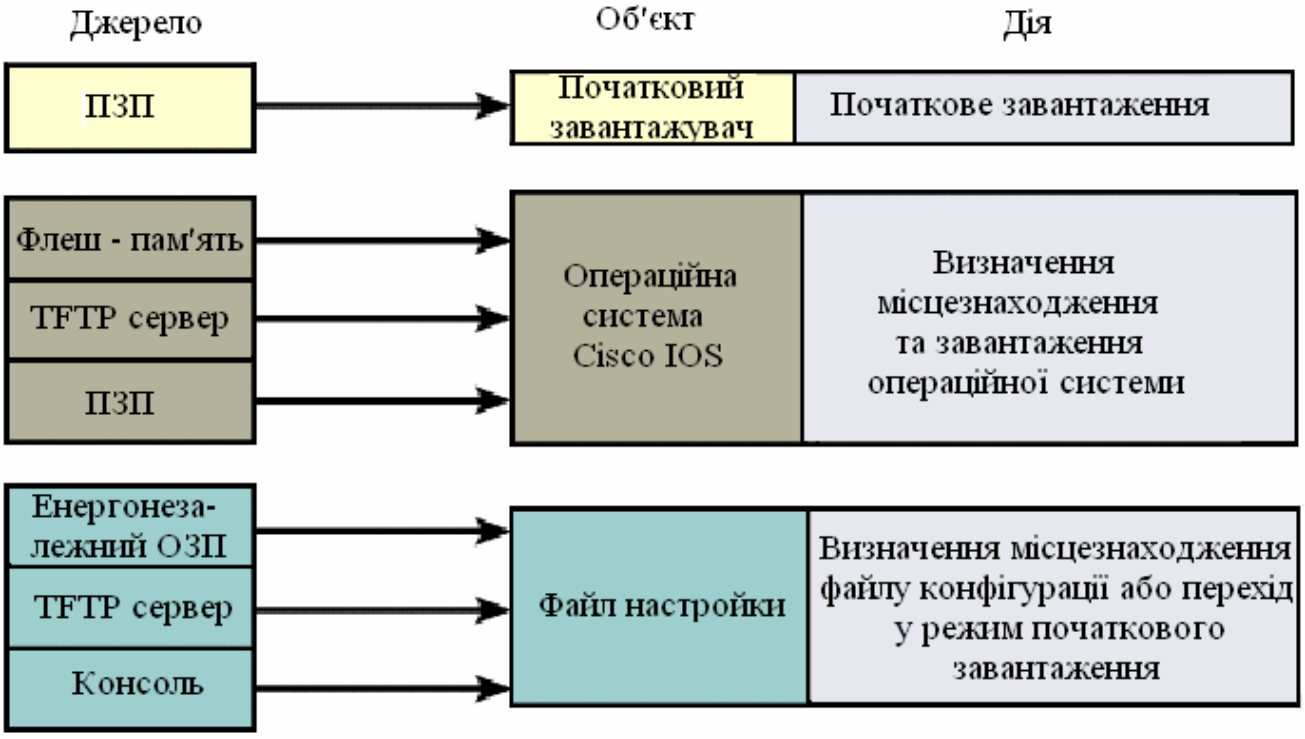


Рисунок Г.1 – Послідовність завантаження Cisco IOS

Підключення до маршрутизатора здійснюється програмою TELNET до IP-адреси будь-якого з його інтерфейсів або при посередництві будь-якої іншої термінальної програми через консольний порт маршрутизатора CON, або додатковій порт AUX. Останньому способу слід надати перевагу, оскільки в

процесі конфігурування маршрутизатора можуть змінюватися параметри IP – інтерфейсів, що може призвести до втрати з'єднання через TELNET. Окрім того, з міркувань безпеки доступ до маршрутизатора через TELNET слід заборонити.

Аварійне відключення оператора від консолі не реєструється маршрутизатором і сеанс залишається в тому ж стані. При повторному підключенні оператор опиниться в тому ж самому контексті, з якого відбулося аварійне відключення (якщо не спрацював автоматичний вихід по таймеру неактивності). Навпаки, при втраті TELNET - з'єднання маршрутизатор закриває сеанс роботи оператора.

При першому завантаженні IOS намагається завантажити конфігурацію з глобальної мережі. При невдалому завершенні цієї процедури IOS пропонує здійснити початкове конфігурування маршрутизатора за допомогою програми SETUP. Програма SETUP пропонує встановити деякі основні глобальні параметри конфігурації маршрутизатора шляхом діалогу питання-відповідь. До початкового конфігурування маршрутизатора відносяться наступні дії:

1) Завдання імені маршрутизатора (за замовчуванням пропонується "Router").
2) Завдання пароля enable secret.
3) Завдання пароля enable password.
4) Завдання пароля віртуального терміналу.
5) Конфігурування протоколів SNMP, IP, протоколів маршрутизації RIP IGRP.
6) Конфігурування інтерфейсів.

Кожен з наведених вище етапів, запропонованих програмою SETUP, може бути проігнорований, а необхідні конфігураційні параметри можуть встановлюватися без посередництва програми SETUP за допомогою відповідних команд Cisco IOS. Крім цього, запуск програми SETUP є можливим в довільний момент з привілейованого режиму.

Правила роботи з командним рядком Cisco IOS

Взаємодія з системою Cisco IOS відбувається при посередництві інтерфейсу командного рядка (Command Line Interface, CLI). В загальному випадку формат команди виглядає наступним чином:

Команда [параметри або опції]

Параметри або опції, залежно від команди, можуть бути обов'язковим, необов'язковими або відсутніми взагалі. Для орієнтування в системі команд в Cisco IOS передбачена залежна від контексту система допомоги.

Допомога може знадобитися при необхідності отримання переліку команд, які розпочинаються попередньо введеною послідовністю символів. В цьому випадку пропонується завершити введену послідовність символом “?” (знак питання) – у відповідь Cisco IOS надасть перелік команд, які починаються шуканою послідовністю символів. Наступний приклад демонструє використання допомоги слова:

Router# co?

configure connect copy

Допомога синтаксису дозволяє отримати перелік допустимих ключових слів та команд даного контексту або перелік допустимих параметрів команди. Для використання допомоги синтаксису пропонується одразу після ключового слова через пробіл ввести символ “?” (знак питання). В результаті буде видано перелік можливих команд чи параметрів команди.

У випадку введення невірної команди (помилка в слові, недопустима в даному контексті команда або невірно заданий параметр) Cisco IOS видасть відповідне повідомлення і вказівку імовірного місцезнаходження помилки в командному рядку. Ключове слово або невірний параметр в цьому випадку позначаються символом “^” (тильда). Наступний приклад демонструє реакцію системи на невірно введене ключове слово “Ethernet”.

Router(config)#interface ethernat

^Invalid input detected at ′^′ marker

Команди та ключові слова можна скорочувати до мінімально можливого – необхідно набрати кількість символів, яка є достатньою для однозначного трактування ключового слова чи команди. Якщо введена послідовність недостатня для однозначного трактування команди чи ключового слова – реакцією Cisco IOS на спробу виконати таку команду буде повідомлення, типу:

cisco(config)# Ambiguous command: "i"

Автозавершення – клавішею TAB можна завершити ввід команди, якщо кількість попередньо набраних символів команди задовольняє вище наведеній умові.

Для усунення необхідності повторного набору команд передбачено буфер історії команд, який надає можливість повторного використання введених раніше команд.

Контексти Cisco IOS

При роботі з командним рядком Cisco IOS передбачено декілька контекстів (режимів вводу команд). Поточний контекст ідентифікується символом

запрошення вводу команди, який виводиться вслід за іменем маршрутизатора, наприклад Router> - контекст користувача; Router# - контекст адміністратора. Замість сигнатури "Router" виводиться назва маршрутизатора, якщо вона була наперед визначена за допомогою відповідної команди.

Контекст користувача – відкривається при підключенні до маршрутизатора і допускає виконання лише обмеженого набору основних контрольних команд, що не впливають на конфігурацію маршрутизатора. Якщо на протязі тривалого часу відсутні будь-які дії в контексті адміністратора, Cisco IOS автоматично переходить в контекст користувача.

Контекст адміністратора – відкривається командою **enable**, поданої в контексті користувача. Контекст адміністратора надає доступ до всіх без винятку команд (команди, що дозволяють отримати повну інформацію про конфігурацію маршрутизатора та його поточний стан, команди переходу в режим конфігурування, команди збереження та завантаження конфігурації). Зворотній перехід до контексту користувача відбувається по команді **disable** або по закінченні встановленого часу неактивності.

Контексти користувача та адміністратора можуть бути захищені паролями з метою запобігання несанкціонованого доступу незареєстрованих операторів, тому при вході до одного з цих контекстів може відбуватися запит пароля (Password:). При вводі пароля останній із міркувань безпеки на екрані терміналу не відображається. При роботі через сеанс TELNET пароль передається мережею у відкритому форматі. TELNET не вживає жодних засобів по забезпеченню захисту пароля від можливого перехоплення. Завершення сеансу роботи відбувається по команді **exit**.

Команди Cisco IOS чітко структуровані і доступні в різних контекстах і для успішної роботи з системою команд важливим є розуміння того, в якому контексті які команди є доступними. Для спрощення орієнтування в ієрархії команд вигляд рядка запрошення має унікальний вигляд. На рис.1.6 наведена проста схематична діаграма деяких контекстів Cisco IOS.

Кожна команда доступна лише на певному рівні ієрархії CLI (в певному контексті CLI). Наприклад, команди конфігурації не будуть доступними, поки інтерфейс не буде переведено на рівень глобального конфігурування командою configure.

В табл. Г.1 наведено перелік можливих контекстів та доступних команд системи команд.

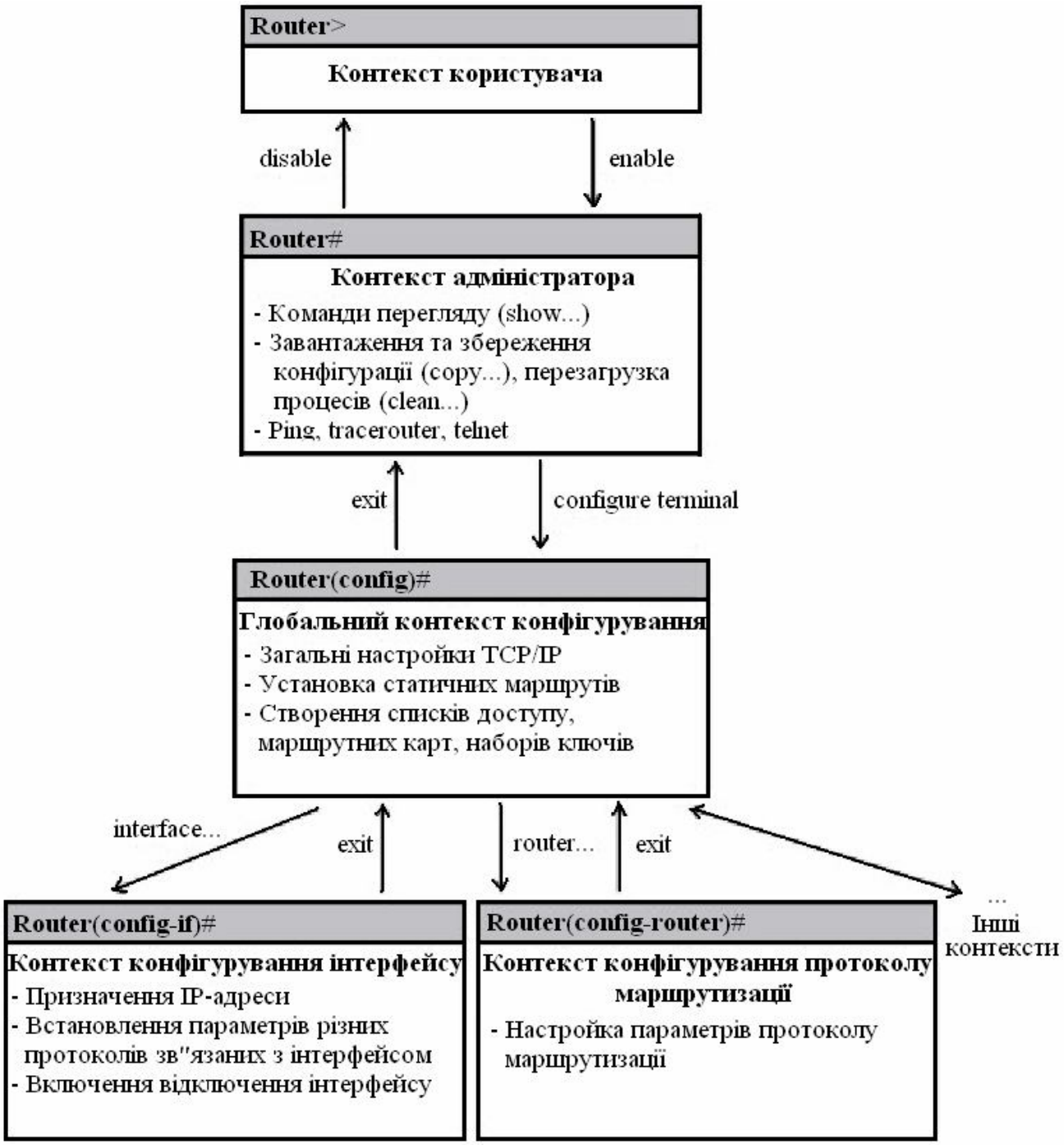


Рисунок 1.6 – Схематична ієрархія команд Cisco IOS

Таблиця Г.1 – Контексти та доступні команди системи команд Cisco IOS

Контексти	Опис
Router>	Режим користувача
Router#	Привілейований режим
Router(config)#	Режим глобального конфігурування
Router(config-if)#	Режим конфігурування інтерфейсу (контекст обраного інтерфейсу)
Router(config-router)#	Режим конфігурування маршрутизації
Router(config-line)#	Режим конфігурування віртуального терміналу

Вихід з контексту глобального конфігурування до контексту адміністратора, а також вихід з будь-якого контексту до контексту верхнього рівня виконується командою exit. Комбінація CTRL+Z приводить до переходу в контекст адміністратора з будь-якого під контексту, до цього ж приводить команда end будь-якого під контексту.

Відміна дії будь-якої команди реалізована за допомогою т.з. "негативних" команд – команд, яким передає префікс no, наприклад:

Router(config-if)#shutdown – виключає інтерфейс

Router(config-if)#no shutdown – включає інтерфейс.

Інколи при введенні негативних команд є потреба у вказуванні параметрів команд, дії яких вони відміняють.

Контекст адміністратора.

Команди конфігурування дозволяють маніпулювати поточним режимом роботи маршрутизатора шляхом зміни значень параметрів, які зберігаються в файлі конфігурації.

Маршрутизатор Cisco зберігає конфігурацію в двох копіях – файл поточної конфігурації (running-config) в RAM та файл стартової конфігурації (startup-config) в NVRAM. Файли конфігурації є текстовими файлами, що містять секції, кожна з яких відповідає одній із підсистем маршрутизатора; в секціях прописуються значення конкретних параметрів відповідних підсистем. При завантаженні Cisco IOS зчитує команди конфігурації з файлу startup-config (в NVRAM) до файлу running-config (в RAM). Поточна конфігурація є активною у процесі функціонування маршрутизатора.

Всі команди вступають в дію одразу ж після їх введення і прописуються до файлу поточної конфігурації (running-config) в RAM. Деякі настройки

маршрутизатора та його окремих підсистем мають значення за замовчуванням. До файлу конфігурації прописуються лише ті значення параметрів, які відрізняються від значень, прийнятих за замовчуванням.

Контекст адміністратора містить команди перегляду файлів поточної та стартової конфігурації:

– show running-config [options] – перегляд файлу поточної конфігурації;
– show startup-config [options] – перегляд файлу стартової конфігурації.

Параметри [options] дозволяють керувати процесом виводу і дозволяють, наприклад, здійснювати вивід не всього файлу, а вмісту деякої окремої його секції.

Якщо маршрутизатор втратить управління і буде перезавантажений, всі зміни, зафіксовані в running-config буде втрачено, якщо їх попередньо не було збережено до файлу стартової конфігурації (startup-config) в NVRAM. Для збереження змін у файлі стартової конфігурації слід користуватися командою:

Router# copy running-config startup-config

Конфігурація маршрутизатора може зберігатися на TFTP – сервері і завантажуватися з нього. Для цього необхідно вказувати IP – адресу TFTP – сервера та назву файлу, під якою буде збережено файл конфігурації. Команда збереження на TFTP має вигляд:

copy <файл-джерело>TFTP://<IP – адреса TFTP >/[<назва файлу>]

Якщо параметр <назва файлу> не буде вказано, Cisco IOS запропонує вказати його значення в процесі діалогу.

При збереженні однієї конфігурації поверх іншої можливі два варіанти: перезапис і злиття. При перезапису стара конфігурація попередньо видаляється, а при злитті – команди нової конфігурації дописуються до старої так, ніби вони вводилися вручну. При злитті конфігурацій можлива низка побічних ефектів, що має особливе значення при злитті списків доступу, оскільки порядок запису рядків списків має суттєве значення. Злиття може змінити цей порядок і суттєво спотворити роботу маршрутизатора.

Примусове перезавантаження маршрутизатора здійснюється командою:

reload

Якщо на момент перезавантаження виявлено факт попередньої зміни файлу поточної конфігурації running-config, Cisco IOS запропонує варіанти його збереження в файлі startup-config (або відмова від збереження).

Контекст глобального конфігурування

Перехід до контексту глобального конфігурування здійснюється з контексту адміністратора командою configure:

– з терміналу: configure terminal;
– з NVRAM: configure memory;
– з мережі: configure network.

В контексті глобального конфігурування виконуються команди, які впливають на функціонування системи в цілому, а також команди переходу до контекстів конфігурування конкретних підсистем маршрутизатора. Контекст глобального конфігурування ідентифікується рядком запиту (config)# і допускає виконання наступних команд:

1) hostname <назва маршрутизатора> - встановлює назву маршрутизатора замість назви за замовчуванням "Router".

2) [no] enable password <пароль> - команда парольного доступу до контексту адміністратора, який буде запитуватися під час виконання команди enable. Пароль прописується до файлу поточної конфігурації і зберігається там у відкритому (нешифрованому) вигляді. При відсутності цього пароля переключення до привілейованого режиму можна здійснити лише при використанні консолі, а з віртуального терміналу буде доступний лише контекст користувача.

3) [no] enable secret <пароль> - команда, за своєю дією аналогічна попередньо описаній, однак пароль зберігається в зашифрованому MD5 – алгоритмом вигляді і має вищий пріоритет виконання.

4) [no] ip domain-lookup – дозволити/заборонити звернення до DNS(Domain Name Service).

5) [no] cdp run – дозволяє/забороняє використання протоколу CDP(Cisco Discovery Protocol) виявлення безпосередньо підключеної апаратури Cisco, тобто доступної на канальному рівні. Протокол з періодичністю 60 с. опитує порти маршрутизатора на предмет наявності апаратури Cisco і заносить інформацію про виявлені пристрої до бази даних. Маршрутизатори до безпосередньо приєднаних мереж заносяться до таблиці маршрутизації автоматично одразу ж після конфігурування інтерфейсу, при умові, що цей інтерфейс працездатний (line protocol up). Для формування додаткових статичних маршрутів призначена команда:

6) [no] ip route <dest.address><dest.mask><next-hop>[options]

<destination address> - адреса цільової мережі

<destination mask> - маска цільової мережі

<next-hop> - адреса сусіднього маршрутизатора

< options> - додаткові параметри, наприклад – параметри метрики

В якості параметра <next-hop> можна вказувати:

– безпосередню адресу сусіднього (доступного на канальному рівні) маршрутизатора;

– адресу віддаленої мережі або віддаленого хоста (опосередкована маршрутизація);

– локальний інтерфейс.

Опосередкований маршрут вказує на запис в таблиці маршрутизації, в якому знаходиться прямий маршрут. Дозволяється формувати таким чином послідовності маршрутов будь-якої довжини. Локальний інтерфейс рекомендується вказувати лише для двоточкових інтерфейсів.

Статичні маршрути фіксуються в файлі стартової конфігурації, а до таблиці маршрутизації піднімаються тільки за умовою досяжності вказаного в них маршруту.

Для регулювання пріоритетами маршрутів слід користуватися параметром <адміндистанція>, який може приймати значення від 0 до 255. Рівень пріоритету зворотно пропорційний значенню адміністративної дистанції і в таблицю маршрутизації з усіх активних маршрутів, що ведуть до даного префікса піднімається лише маршрут з найменшим значенням адміндистанції. За замовчуванням адміндистанція статичних маршрутів рівна 1.

Нульове значення зарезервоване системою Cisco IOS і не може бути використане в явному вигляді, однак неявно нульову адміндистанцію мають також маршрути до безпосередньо приєднаних мереж. Маршрути, які в якості адміндистанції містять значення 255, до таблиці маршрутів не піднімаються.

7) [no] ip default network <адреса віддаленої мережі> - дозволяє вказати маршрут за замовчуванням, відмінний від стандартного. Параметр <адреса віддаленої мережі > повинен бути статично описаний в таблиці маршрутизації. Можливим є визначення декількох маршрутів за замовчуванням – в цьому випадку при обранні маршруту Cisco IOS користується значенням адміністративної дистанції та метричною інформацією. Маршрути за замовчуванням в таблиці маршрутизації позначаються символом "*".

Наведений нижче приклад демонструє використання маршруту в мережу 10.0.0.0 в якості маршруту за замовчуванням:

ip route 10.0.0.0 255.0.0.0 10.108.3.4

ip default-network 10.0.0.0

Cisco IOS має за замовчуванням зарезервований маршрут для використання його в якості маршруту за замовчуванням – 0.0.0.0/0. Cisco IOS надає можливість активації (деактивації) цього маршруту командою:

[no] ip classless

Команда ip classless активує зарезервований Cisco IOS маршрут за замовчуванням (0.0.0.0/0), а команда no ip classless деактивує цей маршрут. За замовчуванням цей маршрут активований, але не описаний.

Лінії керування

Настройка ліній керування маршрутизаторів здійснюється окремо для кожної лінії в контексті обраної лінії, перехід до якого здійснюється з контексту глобального конфігурування командою:

line [aux | console | tty | vty] line-number [ending-line-number]

Дана команда приводить до зміни поточного контексту на контекст обраної лінії керування, який ідентифікується зміною рядка запрошення на (config-line)#

В якості параметрів команди вказуються:

– aux – додатковий EIA/TIA-232 DTE – порт. Повинен задаватися, як відносна лінія 0. Додатковий порт може використовуватися для підтримки модема та асинхронних зв’язків;

– con – консольна термінальна лінія (DTE);

– tty – стандартна асинхронна лінія;

– vty – віртуальна термінальна лінія, що використовується для віддаленого доступу до консолі;

– line-number – відносний номер останньої лінії (при конфігуруванні декількох ліній одночасно).

За замовчуванням маршрутизатор виводить діагностичні повідомлення тільки на консоль, а перенаправлення таких повідомлень на обрану лінію керування реалізується командою: **terminal monitor**.

Дія цієї команди відміняється командою: **no monitor**.

За замовчуванням маршрутизатор виводить системні повідомлення поверх вводу оператора і для продовження вводу оператор повинен пам’ятати, в якому місці його перервали. Для того, щоб дозволити після виводу кожного системного повідомлення вивід частини попередньо введеного оператором рядка, слід використовувати команду:

logging synchronous

Якщо по завершенню деякого проміжку часу (інтервал неактивності) спостерігається відсутність вводу з терміналу, Cisco IOS розриває поточну сесію. Інтервал неактивності встановлюється командою:

exec timeout <хвилини>[<секунди>]

Будь-яка команда X, введена в контексті оператора або адміністратора, сприймається маршрутизатором, як команда telnet X. Це приводить до того, що будь-який помилковий ввід примушує маршрутизатор опитувати сервер DNS для перетворення помилково введеного рядка в IP – адресу, що зумовлює затримки в роботі оператора. Уникнути таких затримок допомагає команда:

transport preffered none

З міркувань безпеки, доступ до маршрутизатора через віртуальний термінал слід обмежити за допомогою пароля. Встановити пароль можна командою:

[**no] password <текст пароля>**

Активація запиту пароля при в ході в Cisco IOS через віртуальний термінал виконується командою:

[no] login

При відсутності парольного захисту контексту адміністратора використовується пароль захисту лінії CON, якщо цей пароль встановлено.

Слід зауважити, що в робочому режимі з міркувань безпеки віртуальні термінали потрібно заблокувати, а доступ до маршрутизатора здійснювати лише по консольній лінії або через термінальний сервер.

Конфігурування інтерфейсів.

Конфігурування інтерфейсів здійснюється окремо для кожного інтерфейсу в контексті обраного інтерфейсу, перехід до якого здійснюється командою контексту глобального конфігурування:

interface <тип><номер>

В якості параметру <тип> допускаються наступні слова: Ethernet, Fast Ethernet, Serial, Loopback, Null.

Вказана команда приводить до зміни поточного контексту на контекст конфігурування обраного інтерфейсу (config-if#).

На інтерфейсах Ethernet, окрім встановлення IP – адреси, як правило більше нічого робите не потрібно, однак Fast Ethernet може потребувати деяких примусових настройок дуплексного режиму або встановлення фіксованої швидкості (за замовчуванням ці параметри встановлюються шляхом переговорів, однак в окремих випадках переговори можуть не дати необхідних результатів).

Послідовні інтерфейси за замовчуванням на фізичному рівні є інтерфейсами DTE, а на канальному рівні – інтерфейсами HDLC (фірмову модифікацію Cisco HDLC). Якщо інтерфейс переведено в режим DCE, для нього слід задавати тактову частоту синхронізації передачі даних.

Для надання фізичному інтерфейсу IP – адреси слід використовувати команду:

ip address <IP-address><address-mask>

де <IP-address> - IP – адреса інтерфейсу;

<address-mask> - маска підмережі.

В деяких випадках може бути необхідність встановлення ширини смуги пропускання командою:

bandwith <ширина-смуги-пропускання, кБіт/с>

За замовчуванням bandwith може мати наступні значення:

– для Ethernet 10000;
– для Fast Ethernet 100000;
– для Serial 1544.

Слід зауважити, що значення параметра bandwith не впливає на фізичну швидкість передачі, а використовується деякими протоколами маршрутизації для оцінки маршруту.

Тип середовища передачі вказується командою:

media-type <тип-середовища-передачі>

Параметр <тип-середовища-передачі> може приймати значення:

– для Ethernet "10BASE-T";
– для Fast Ethernet "100BASE-T", "100BASE-TX".

Для послідовних інтерфейсів, які використовують функції DCE, необхідно вказати фізичну швидкість передачі даних. Це можна зробити командою:

clock rate <фізична-швидкість-передачі, кБіт/с>

Параметр <фізична-швидкість-передачі, кБіт/с> може приймати фіксовані значення, перелік яких можна попередньо проглянути, ввівши clock rate?.

Для послідовного інтерфейсу, що виконує функцію DTE також може бути вказаний цей параметр, однак він буде проігнорований Cisco IOS і жодного впливу на роботу інтерфейсу не матиме, оскільки обладнання DTE запозичує цей параметр від DCE.

За замовчуванням фізичні інтерфейси виключені (неактивні – administratively down). Для їх активації використовується команда:

[no] shutdown

Ця команда переводить інтерфейс до стану manual up. Якщо зовнішнє обладнання вимкнено, то Cisco IOS автоматично переведе фізичний інтерфейс до стану manual down, а при активізації зовнішнього обладнання фізичний інтерфейс підніметься до стану manual up автоматично.

Для послідовних інтерфейсів іноді виникає необхідність використовувати протокол канального рівня, відмінний від протоколу за замовчуванням (HDLC). Cisco IOS надає можливість вказати тип використовуваного протоколу командою:

encapsulation <протокол>

Параметр <протокол> може приймати фіксовані значення, для яких Cisco IOS передбачені зарезервовані ключові слова, наприклад PPP, Frame-Relay і т.п. Повний перелік значень параметра <протокол> доступний для перегляду командою encapsulation?.

Логічні інтерфейси конфігуруються командами, які наведені вище, за винятком того, що параметри media-type, clock rate та операція [no] shutdown для них не мають сенсу.

Додаток Д
Опис емулятора Cisco Packet Tracer 5.3.2

Cisco Packet Tracer – емулятор мережі передачі даних, який випускається компанією Cisco System. Програмні продукти Packet Tracer надають можливість створювати мережеві топології із широкого спектру маршрутизаторів і комутаторів Cisco, робочих станцій та мережевих з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Ця функція може бути виконана як для навчання, так і для роботи. Наприклад, щоб провести настройку мережі ще на етапі планування або щоб створити копію робочій мережі з метою усування недоліків.

Загальний вигляд програми представлений на рис.Д.1

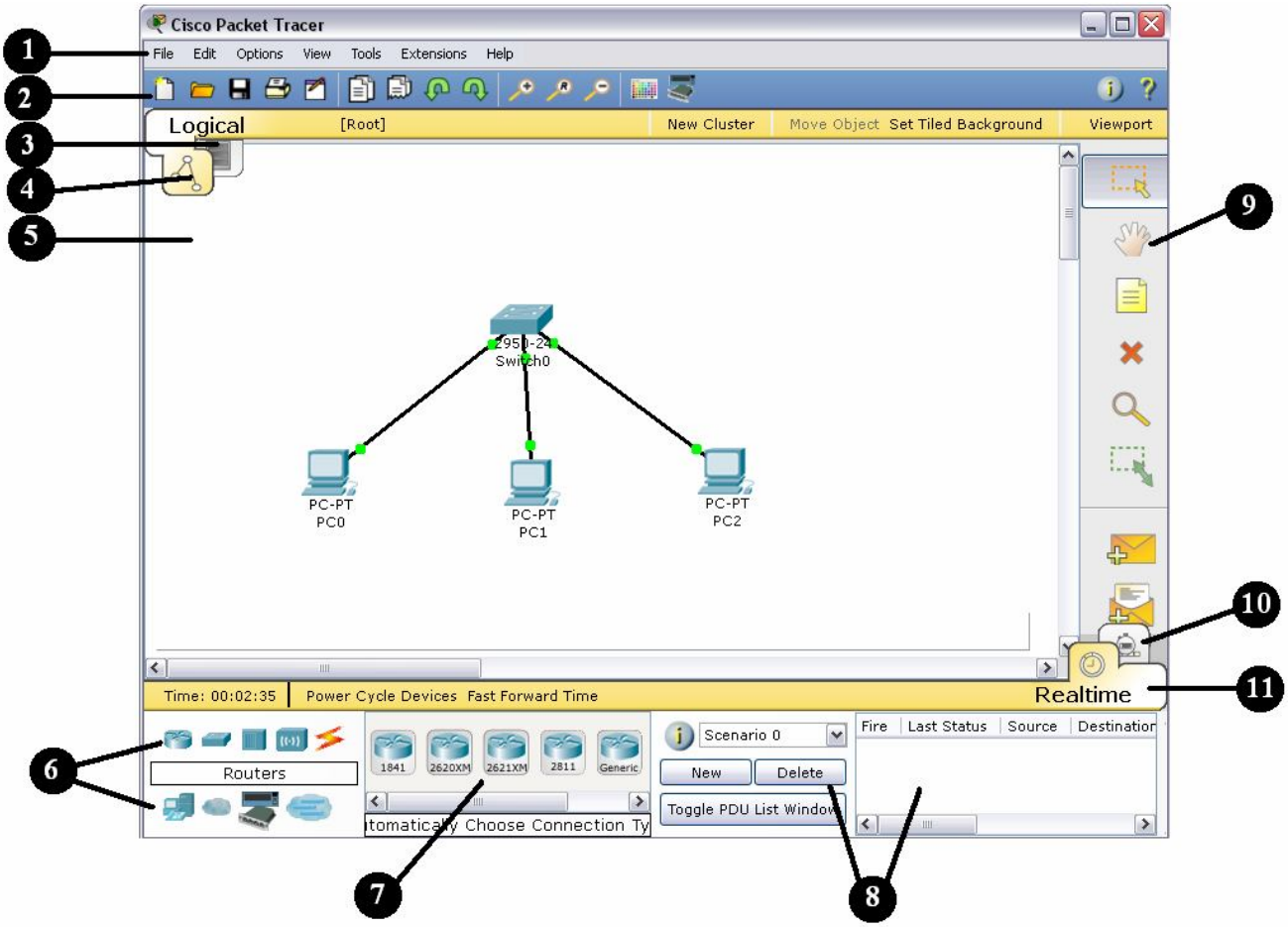


Рисунок Д.1 – Інтерфейс програми Packet Tracer

Робоча область вікна програми складається з наступних елементів:

1. **Menu Bar** – головне меню програми. Дозволяє детально налаштувати роботу програми. Панель містить меню File, Edit, Options, View, Tools, Extensions, Help.

2. **Menu Tool Bar** – піктографічне меню, містить графічні зображення ярликів для доступу к командам меню File, Edit, View і Tools, а також кнопку Network Information.

3. **Logical/Physical Workspace and Navigator Bar -** панель, яка надає можливість перемикати робочу область: фізичну чи логічну, а також дозволяє пересуватися між рівнями кластера.

4. **Logical Workspace and Navigator Bar -** режим побудови логічної топології мережі.

5. **Workspace –** область, в якій відбувається створення мережі, проводяться спостереження за симуляцією і проглядається різна інформація і статистика.

6. **Network Component Box** – це область, в якій вибираються устаткування і зв'язки для розміщення їх на робочому просторі. Вона містить області Device – Type Selection і Device-Specific Selection. Область Device –Type Selection містить доступні типи пристроїв і зв'язків, а область Device-Specific Selection змінюється в залежності від обраного пристрою.

7. **Device-Specific Selection** – область використовується для вибору конкретних устаткувань і з'єднань, необхідних для побудови в робочому просторі мережі. Вибір класу пристрою, яке буде елементом фізичної або логічної топології.

8. **User Created Packet Window** – вікно керує пакетами, які були створені в мережі під час симуляції сценарію.

9. **Common Tools Bar -** панель піктограм, яка забезпечує доступ до найбільш використовуваних інструментів програми: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU і Add Complex PDU.

10. **Simulation Bar -** пакетний аналізатор, містить кнопки Play Control і перемикач Event List.

11. **Realtime Bar** – панель для роботи в режимі реального часу, містить кнопки, що відносяться до Power Cycle Devices.

Для створення топології необхідно вибрати устаткування з панелі Network Component, а далі з панелі Device–Type Selection вибрати тип обраного устаткування. Після цього потрібно натиснути ліву кнопку миші в полі робочої області програми (Workspace). Також можна витягнути пристрій прямо з області Device–Type Selection, але при цьому буде обрана модель пристрою за замовчанням.

Для швидкого створення декількох екземплярів одного і того ж пристрою потрібно натиснути кнопку Ctrl і разом з нею натиснути на пристрій, який вже

знаходиться в області Workspace. Після цього можна декілька разів натискати на робочій області для додавання копій пристрою.

В Packet Tracer представлені наступні типи устаткування:

– маршрутизатори;
– комутатори (в тому числі і мости);
– хаби і повторювачі;
– ПК, сервери, принтери, IP – телефони;
– бездротові пристрої: точки доступу і бездротовий маршрутизатор;
– інші пристрої – хмара, DSL – модем і кабельний модем.

Додамо необхідні елементи в робочу область програми так, як показано на рис.Д.2.

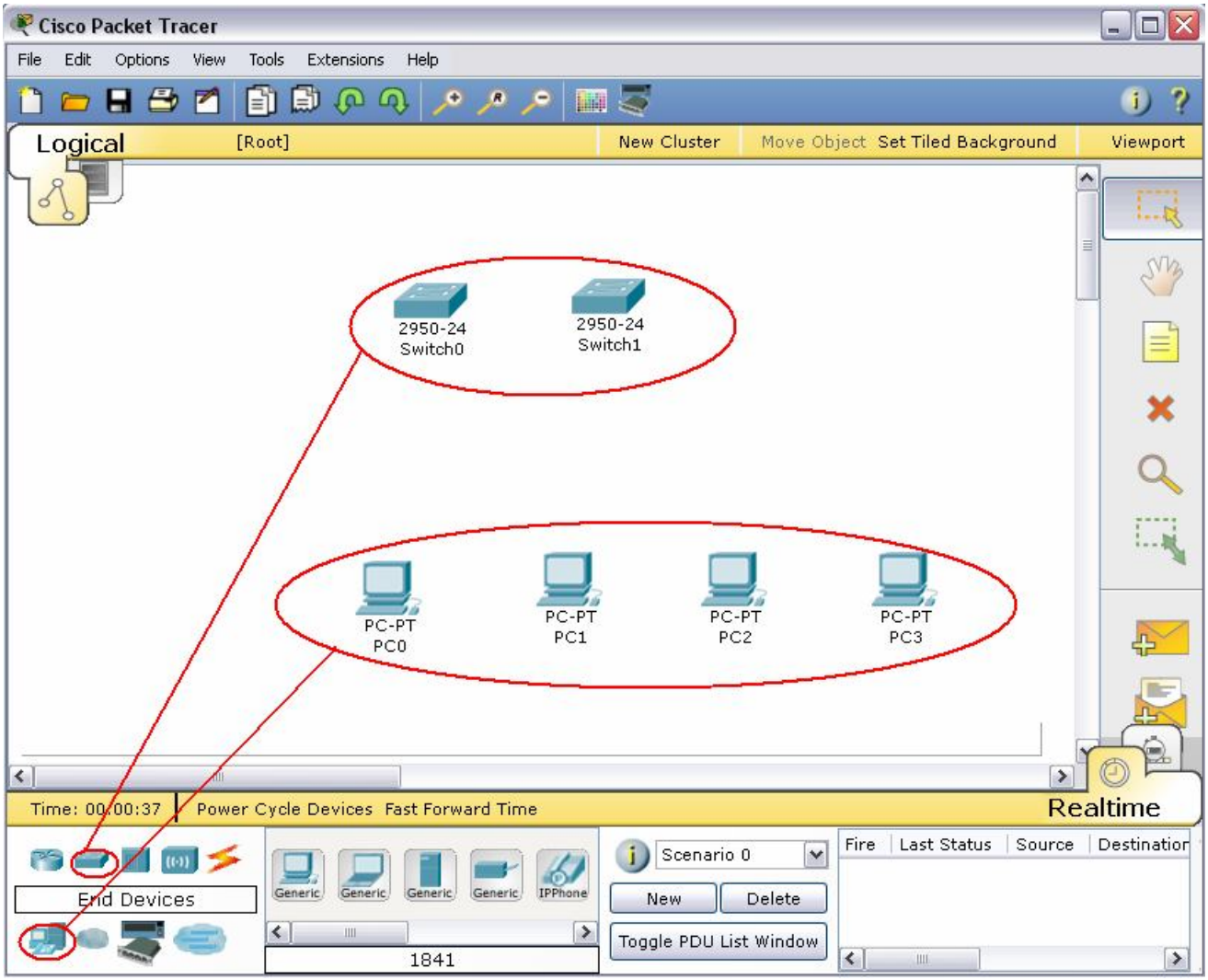


Рисунок Д.2 – Додавання елементів мережі

При додаванні кожного елемента користувач має можливість дати йому ім’я і установити параметри. Для цього необхідно натиснути на потрібний елемент

лівою кнопкою миші (ЛКМ) і в діалоговому вікні устаткування перейти до вкладки **Config**.

Діалогове вікно властивостей кожного елемента має дві вкладки:

– Phisical – містить графічний інтерфейс устаткування і дозволяє симулювати роботу з ним на фізичному рівні.

– Config – містить всі необхідні параметри для настройки устаткування і має зручний для цього інтерфейс.

Також в залежності від устаткування, властивості можуть мати додаткову вкладку для керування роботою обраного елемента: Desktop (якщо обране кінцеве устаткування) або CLI (якщо обраний маршрутизатор) і т.п.

Для видалення устаткувань використовується кнопка Delete (Del).

Додані елементи треба зв'язати за допомогою з'єднувальних зв'язків. Для цього необхідно вибрати вкладку Connections з панелі Network Component Box. Стануть доступними всі можливі типи з'єднань між устаткуваннями. Далі вибирається відповідний тип кабелю. Вказівник миші зміниться на курсор "connection" (має вигляд рознімання). Слід натиснути на першому пристрої і вибрати відповідний інтерфейс, к якому треба виконати з'єднання, а далі натиснути на другий пристрій, виконавши ту ж операцію. Можна також з'єднати за допомогою **Automatically Choose Connection Type**  (автоматично з'єднує елементи в мережі). Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів які мають індикатор).

Рисунок Д.3 – Типи кабелю, що підтримуються в Packet Tracer

Packet Tracer підтримує широкий діапазон мережевих з'єднань. Вони описані в табл.Д.1. Кожний тип кабелю може бути з'єднаний лише з певними типами інтерфейсів.

Таблиця Д.1 – Типи кабелю в Packet Tracer

Тип кабелю	Опис
 Console	Консольне з'єднання може бути виконане між ПК і маршрутизаторами або комутаторами. Для цього повинні виконуватися деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох

Тип кабелю	Опис
	сторін повинна бути однаковою, 7 біт даних (або 8 біт) для обох сторін, однаковий контроль парності, 1 або 2 стопових біта (але вони не обов'язково повинні бути однаковими), а потік даних може бути будь-яким для обох сторін.
 Copper Straight - through	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet). Використовується для з'єднання типу ПК-комутатор, маршрутизатор-комутатор).
 Copper Cross - over	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв. Використовується для з'єднання типу ПК-ПК, комутатор-комутатор, маршрутизатор-маршрутизатор, маршрутизатор-ПК).
 Fiber	Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт/с або 1000 Мбіт/с).
 Phone	З'єднання через телефонну лінію може бути здійснено тільки між пристроями, які мають модемні порти.
 Coaxial	Коаксіальне середовище використовується для з'єднання між коаксіальними портами, такими як кабельний модем, з'єднаний з хмарою Packet Tracer.
  Serial DCE and DTE	З'єднання через послідовні порти, часто використовуються для зв'язку WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на боці DCE – устаткування. Синхронізація DTE виконується за вибором. Сторону DCE можна визначити по маленькому малюнку «годинника» поряд з портом. При виборі типа з'єднання Serial DCE, перший пристрій, до якого застосовується з'єднання, становиться DCE – устаткуванням, а другий – автоматично стане стороною DTE. Можливе і зворотне розташування сторін, якщо обраний тип з'єднання Serial DTE.

Найбільш часто будемо використовувати два типи кабелю: прямий (Copper Straight-through) і перехресний кабель (Copper Cross – over). Щоб визначити тип кабелю RJ-45, треба положити два кінця кабелю разом, щоб побачити різнокольорові дроти, як це показано на рис. Д.4. На кінці кожного є вісім різнокольорових смужок або контактів. Якщо порядок слідкування кольорових контактів співпадає, то такий кабель називається прямим (рис.Д.5).

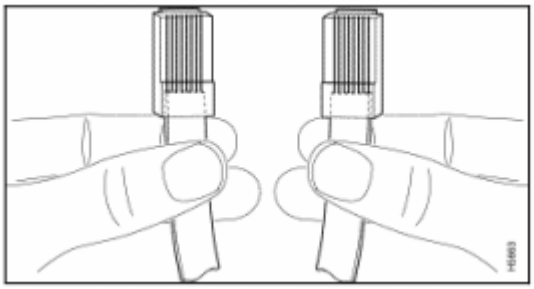
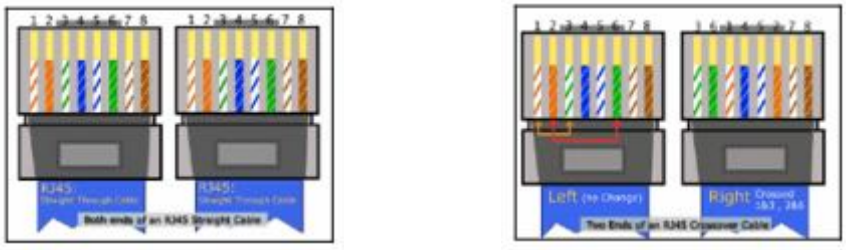


Рисунок Д.4 – Визначення типу кабелю RJ-45

Для того, щоб визначити який кабель слід використати для з'єднання, розділимо всі устаткування на два типа. Тип 1: мережеві адаптери комп'ютерів (LAN або Ethernet), WAN – порт маршрутизатора, рознімання Ethernet різних устаткувань (телевізори, тюнери та інш.). Тип 2: LAN- порти маршрутизаторів, LAN- порти ADSL модемів, всі порти концентраторів і комутаторів. При з'єднанні між собою двох пристроїв одного типу (наприклад, комп'ютер – комп'ютер або комутатор – комутатор) потрібен перехресний кабель, а при з'єднанні між собою двох пристроїв різного типу – прямий кабель (наприклад, комп'ютер – концентратор або комп'ютер – комутатор).



а) прямий кабель б) перехресний кабель

Рисунок Д.5 – Вигляд прямого та перехресного кабелю

Після створення мережі її треба зберегти, вибравши пункт меню File->Save або іконку Save на панелі Main Tool Bar. Файл з збереженою топологією має розширення *.pkt.

Packet Tracer надає можливість симулювати роботу с інтерфейсом командного рядка (ІКР) операційної системи IOS, встановленої на всіх комутаторах і маршрутизаторах компанії Cisco.

Підключившись до устаткування, можна працювати з ним так, як за консоллю реального пристрою. Стимулятор забезпечує підтримку практично усіх команд, що доступні на реальних пристроях.

Підключення до ІКР комутаторів або маршрутизаторів можна провести, клацнувши на необхідний пристрій і переключившись в вікно властивостей до вкладки CLI.

Для симуляції роботи командної строки на кінцевому устаткуванні (комп'ютері) необхідно во властивостях вибрати вкладку Desktop, а далі натиснути на ярлик Command Prompt.

Робота з файлами в Packet Tracer

Програма Packet Tracer дозволяє користувачеві зберігати конфігурацію деяких пристроїв, таких як маршрутизатори або комутатори в текстових файлах. Для цього необхідно перейти до властивостей даного пристрою і у вкладці Config натиснути на кнопку "Export…" для експорта конфігурації Startup Config або Running Config. Відкриється діалогове вікно для збереження необхідної конфігурації в файл, який буде мати розширення *.txt. Текст файлу з конфігурацією пристрою running-config.txt (ім'я за замовчуванням) представляється аналогічним до тексту інформації, отриманому при використанні команди show running в IOS пристроях.

Слід відмітити, що конфігурація кожного устаткування зберігається в окремому текстовому файлі. Користувач також має можливість змінювати конфігурацію в збереженому файлі вручну за допомогою довільного текстового редактору. Для надання устаткуванню збережених або відредагованих налаштувань треба в вкладці Config натиснути кнопку "Load…" для завантаження необхідної конфігурації Startup Config або кнопку "Merge…" для завантаження конфігурації Running Config.

МЕТОДИЧНІ ВКАЗІВКИ

до виконання контрольної роботи
з дисципліни “ Комп’ютерні мережі”

для студентів IV курсу заочної форми навчання.
Напрям підготовки – комп’ютерні науки, спеціальність
7.080.401 “Інформаційні управляючі системи та технології”.

Укладач: доц. Кузніченко С.Д.

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