**Міністерство освіти і науки, молоді та спорту України**
**Чернівецький національний університет**
**імені Юрія Федьковича**

# МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

*Навчальний посібник*

**Чернівці**
**Чернівецький національний університет**
**2012**

**УДК 004.7 (075.8)**
**ББК 32.973.2я73**
**М 52**

Друкується за ухвалою редакційно-видавничої ради
Чернівецького національного університету
імені Юрія Федьковича

**Рецензенти:**

***Бучковський І. А.***, *кандидат технічних наук, доцент кафедри кореляційної оптики інженерно-технічного факультету;*

***Шпатар П. М.***, *кандидат технічних наук, доцент кафедри радіотехніки та інформаційної безпеки фізичного факультету*

М 52 Мережні інформаційні технології : навчальний посібник / укл. Танасюк Ю.В. – Чернівці : ЧНУ, 2012. – 132 с.

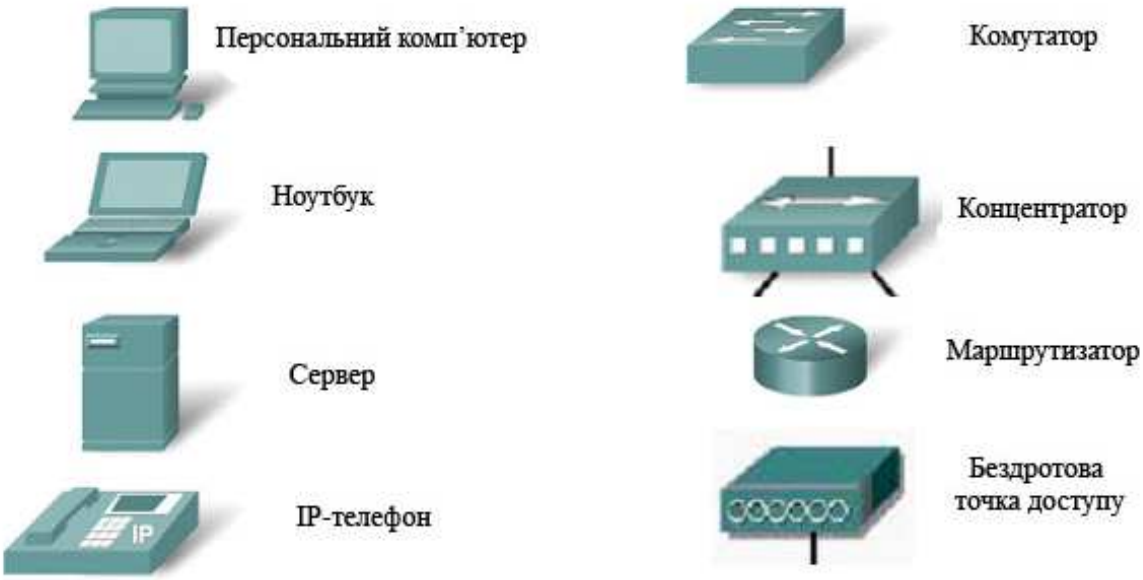
Запропоноване видання має на меті вивчення базових технологій побудови локальних і глобальних корпоративних мереж, ознайомлення з алгоритмами маршрутизації та способами їх реалізації на практиці, механізмами створення віртуальних локальних мереж, впровадження необхідних засобів безпеки у мережі та набуття практичних навичок, необхідних для планування, налаштування й обслуговування сучасних конвергентних мереж передачі даних.

Для студентів вищих навчальних закладів спеціальності 7.05010201 «Комп'ютерні системи та мережі», слухачів інших напрямів підготовки, які вивчають дисципліни „Комп'ютерні мережі" та «Мережні інформаційні технології».

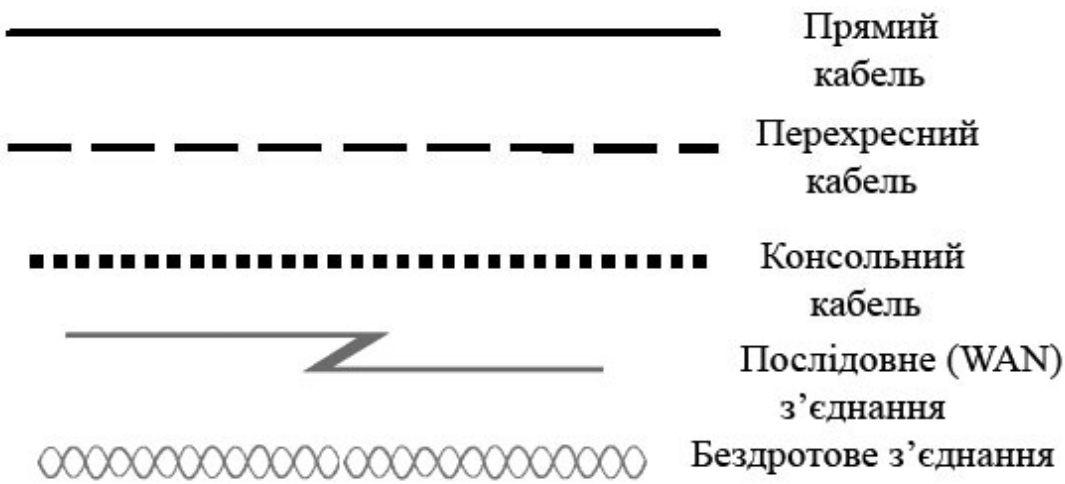
**ББК 32.973.2я73**

# ЗМІСТ

## Графічні позначення елементів мереж передачі даних




## Позначення середовищ передачі даних



# І. КОМПОНЕНТИ ТА РЕЖИМИ РОБОТИ МАРШРУТИЗАТОРА

Маршрутизатор – мережний пристрій, який, подібно до комп'ютера, має такі базові компоненти, як процесор, пам'ять, системну шину та різні вхідні/вихідні інтерфейси. Ці компоненти забезпечують виконання специфічних функцій маршрутизатора.

Як ПК вимагає наявності ОС для запуску різних програм, так і маршрутизатор використовує IOS (Internetwork Operating System) для запуску конфігураційних файлів, які містять основні налаштування маршрутизатора, інструкції та параметри для контролю вхідного та вихідного трафіків. Використовуючи протоколи маршрутизації, маршрутизатори приймають рішення про перенаправлення даних по мережі.

### *Внутрішні компоненти маршрутизатора*

Розглянемо типи пам'яті, які використовуються в маршрутизаторі.

**RAM (Random Access Memory, оперативна пам'ять)** виконує такі функції:

- зберігає таблиці маршрутизації;
- зберігає ARP-кеш;
- зберігає керовану таблицю комутації;
- при необхідності забезпечує буферизацію пакетів;
- управляє чергами пакетів;
- забезпечує зберігання тимчасового конфігураційного файла при роботі маршрутизатора.

При вимкненні маршрутизатора RAM втрачає свій вміст.

**NVRAM (Non-volatile RAM, енергонезалежна пам'ять)** зберігає завантажувальний конфігураційний файл;

При вимкненні маршрутизатора NVRAM зберігає свій вміст.

**Флеш-пам'ять (Flash memory, флеш пам'ять)** забезпечує виконання таких функцій:

- зберігає образ операційної система (IOS image);
- дозволяє оновити програмне забезпечення без заміни мікросхем процесора;
- може зберігати кілька версій IOS одночасно.

Флеш зберігає свій вміст при вимкненні маршрутизатора.

**ROM (Read-Only Memory, постійний запам’ятовуючий пристрій)**:

- управляє інструкціями для початкової самодіагностики апаратних частин маршрутизатора (power-on self test, POST);
- зберігає завантажувальну програму та базові функції операційної системи.

Для проведення оновлення ця пам’ять вимагає заміни апаратних компонент.

### *Інтерфейси*

Інтерфейси (порти) маршрутизатора призначені для його налаштування, управління, під’єднання до мережі та передачі даних. Зокрема, розрізняють **локальні (Ethernet)** інтерфейси для під’єднання окремих локальних мереж та **послідовні (serial)** інтерфейси для під’єднання маршрутизатора до глобальної мережі. Крім зазначених типів інтерфейсів існують також **управлінські** порти **(console та AUX)**, які не використовуються для передачі даних, а слугують для конфігурації параметрів маршрутизатора та моніторингу його роботи. На рис. 1.1 зображено задню панель маршрутизатора з позначенням її основних компонентів.

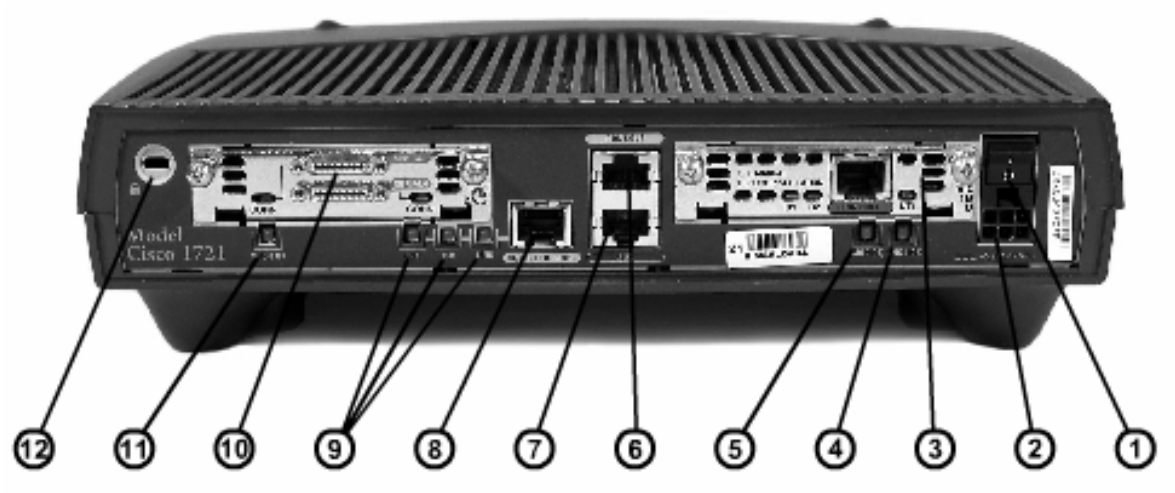



Рис. 1.1. *Елементи задньої панелі маршрутизатора Cisco 1721*

Призначення елементів маршрутизатора (рис. 6.1):

1. Перемикач ввімкнення/вимкнення.
2. Перемикач напруги 120/220 В.
3. Слот модуля WIC 1 (WAN Interface Card).
4. Індикатор стану WIC1.

5. Індикатор роботи апаратного забезпечення VPN.
6. Консольний порт.
7. AUX (auxiliary) порт (допоміжний).
8. 10/100 Mbps Ethernet порт.
9. Індикатори роботи порту Ethernet.
10. Послідовні (serial) порти.
11. Індикатор стану послідовних портів.
12. Сокет для ключа (за його допомогою можна підвищити фізичну безпеку пристрою).

Окрім назв, порти маршрутизаторів Cisco мають кольорове маркування (табл. 1.1).

Таблиця 1.1

Характеристики інтерфейсів маршрутизатора

| **Порт** | **Тип порту** | **Колір** | **З другого боку з'єднання** | **Тип кабелю** |
|---|---|---|---|---|
| Ethernet | RJ-45 | жовтий | Концентратор/ комутатор (робоча станція) | Прямий (перехресний) |
| Console | 8-піновий | блакитний | COM-порт комп'ютера | Консольний (rollover) |
| AUX | 8-піновий | чорний | модем | Консольний |
| Serial | Smart serial | синій | Маршрутизатор, комутатор, модем | V.35 |

***Під'єднання до глобальної мережі***

При налаштуванні глобального (WAN) з'єднання використовуються такі два типи пристроїв:

- **пристрій передачі даних** (Data Communications Equipment, DCE) – пристрій, який забезпечує синхронізацію для іншого пристрою. Зазвичай такий пристрій розташовується з боку провайдера і відповідає за передачу даних до глобальної мережі;
- **термінальний пристрій даних** (Data Circuit-Terminal Equipment, DTE) розташовується з боку користувача послугами глобальної мережі. Даний пристрій одержує сигнал синхронізації від пристрою DCE, відповідно до якого налаштовує власні параметри.

При утворенні безпосереднього з’єднання із сервіс-провайдером або із пристроєм передачі даних, таким як модуль обслуговування каналу та даних (channel service unit/data service unit, CSU/DSU), термінальним пристроєм даних (DTE) є маршрутизатор і використовується послідовний кабель DTE.

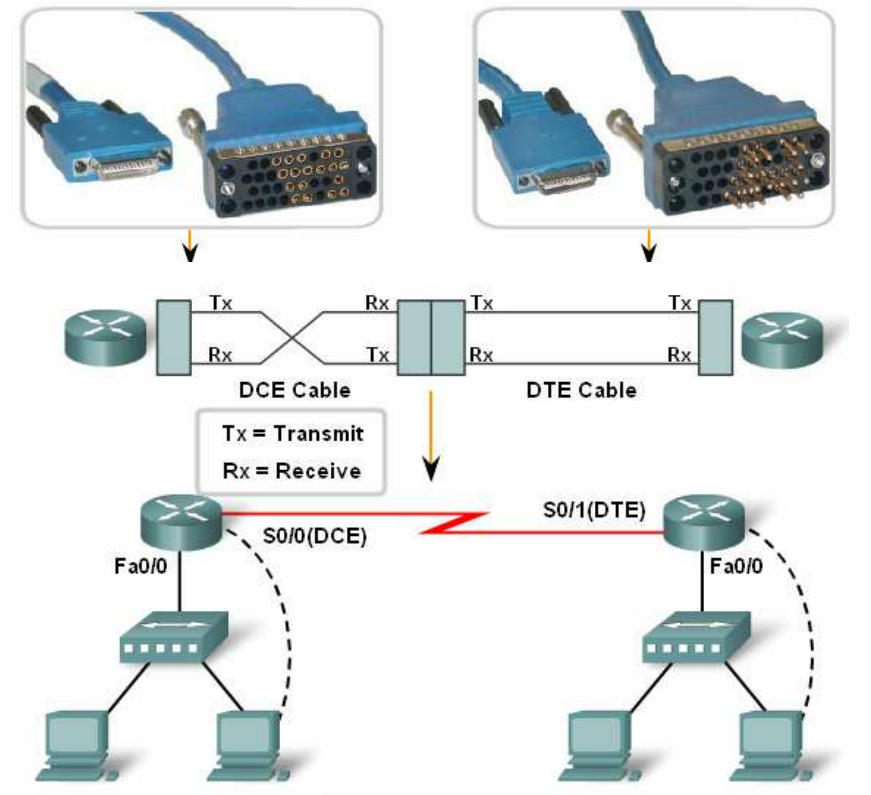



Рис. 1.2. *Послідовне WAN-з’єднання в лабораторних умовах*

Як показано на рис. 1.2, при утворенні WAN-з’єднання в лабораторних умовах два маршрутизатори з’єднують послідовним, т.зв. нуль-модемним кабелем. При цьому один із маршрутизаторів, до якого під’єднано DCE-кінець кабелю, задаватиме тактову частоту синхронізації і виступатиме пристроєм DCE, хоча за замовчуванням маршрутизатори належать до термінальних пристроїв (DTE).

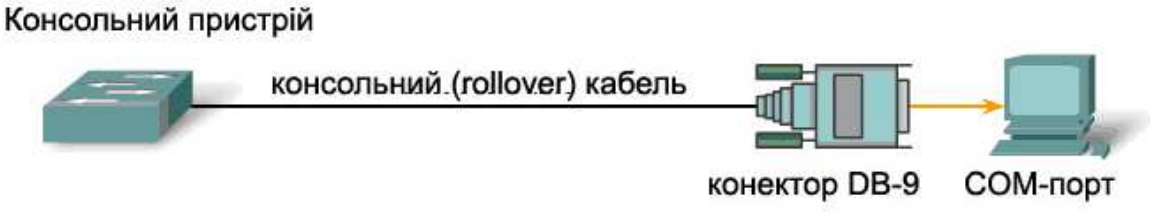



Рис. 1.3. *Утворення консольного з’єднання*

***Консольне з'єднання***

Перш ніж використовувати проміжний пристрій у мережі на ньому потрібно виконати налаштування необхідних мережних параметрів та протоколів. У лабораторних умовах доступ до конфігурації пристрою здійснюється через комп'ютер за допомогою консольного (rollover) кабелю. З одного боку даного кабелю встановлюється конектор RJ-45, який під'єднується до консольного порту мережного пристрою, з іншого боку – 9-піновий D-конектор, який під'єднується до послідовного (COM) порту RS-232 комп'ютера (рис. 1.3).

***Режими роботи***

Маршрутизатори Cisco можуть працювати в кількох режимах, кожен з яких дозволяє виконувати певні дії:

- **режим користувача (user EXEC mode)** – дозволяє виконувати лише обмежений набір команд для моніторингу роботи маршрутизатора. Його називають також режимом "тільки для перегляду" (view only). У цьому режимі відсутні будь-які команди, які можуть змінити конфігурацію маршрутизатора. У режимі користувача запрошення до введення має вигляд `"Router>"`;
- **привілейований режим (privileged mode)** – дозволяє виконувати всі команди перегляду, збереження, видалення налаштувань маршрутизатора. У цьому режимі запрошення до введення виглядає `"Router#"`.

*Для переходу із режиму користувача до привілейованого необхідно набрати команду* **`enable`**.

Для виклику допомоги в будь-якому режимі слід набрати `"?"`.

Для зміни будь-яких параметрів маршрутизатора необхідно ввійти у **режим глобальної конфігурації (global configuration mode)**. Для цього в привілейованому режимі слід набрати команду **`configure terminal`**, після чого запрошення до введення виглядатиме так: `"Router(config)#"`. В цьому режимі можна змінювати певні глобальні параметри, а саме:

- ім'я маршрутизатора: `Router(config)#`**`hostname`** *ім'я*;
- пароль на доступ до привілейованого режиму:

`Router(config)#`**`enable secret`** *пароль*

або

`Router(config)#`**`enable password`** *пароль* .

Цей пароль потрібно вводити щоразу при переході до привілейованого режиму після введення команди `enable`. Відмінність між цими двома

типами паролів полягає в тому, що при перегляді налаштувань маршрутизатора перший завжди відображатиметься в зашифрованому вигляді.

Існують також інші специфічні режими конфігурації окремих параметрів, до яких можна потрапити з режиму глобальної конфігурації, а саме:

- **режим конфігурації інтерфейсу `Router(config-if)#`:**

```
Router(config)#interface тип номер
Router(config-if)#ip address IP-адреса маска
Router(config-if)#description <опис інтерфейса>
Router(config-if)#no shutdown   ! відкриття інтерфейсу
Router(config-if)#exit          !вихід з цього режиму
```

Наприклад:

```
Router(config)#interface fa 0/0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#description Network Laboratory
Router(config-if)#no shutdown
Router(config-if)#exit
```

При конфігуруванні послідовних інтерфейсів слід пам'ятати про те, що один із маршрутизаторів обов'язково повинен бути налаштований як DCE-пристрій. На його **serial** інтерфейсі серед інших параметрів слід задати тактову частоту командою:

```
Router(config-if)# clock rate 64000
```

**- режим конфігурації лінії – `Router(config-line)#`:**

Конфігурація ліній включає в себе насамперед налаштування паролів на доступ до консолі:

```
Router(config)#line con 0
Router(config-line)#password пароль
Router(config-line)#login
Router(config-line)#exit
```

та до термінальних ліній (обмеження звернень за протоколом Telnet):

```
Router(config)#line vty 0 4
Router(config-line)# password пароль
Router(config-line)#login
Router(config-line)#exit
```

- **режим конфігурації протоколів маршрутизації – `Router(config-router)#`:**

```
Router(config)# router протокол маршрутизації
Router(config-router)# network IP-адреса_ мережі
```

Для повернення з певного режиму конфігурації до глобального режиму конфігурації виконують команду **`exit`**.

Для перегляду виконаних налаштувань, а також різноманітних параметрів конфігурації в привілейованому режимі використовується команда **`show`** із відповідними ключами, яка відображає такі дані:

- **`show interfaces`** – статистику для інтерфейсів маршрутизатора;
- **`show controllers serial`** – інформацію про контролер послідовного інтерфейсу;
- **`show clock`** – час та дату;
- **`show hosts`** – таблицю DNS-імен та IP-адрес;
- **`show users`** – дані усіх користувачів, під'єднаних до маршрутизатора;
- **`show history`** – історію уведених команд;
- **`show flash`** – інформацію про флеш-пам'ять та файли, які там зберігаються;
- **`show version`** – інформацію про маршрутизатор, його апаратне та програмне забезпечення (рис. 1.4);

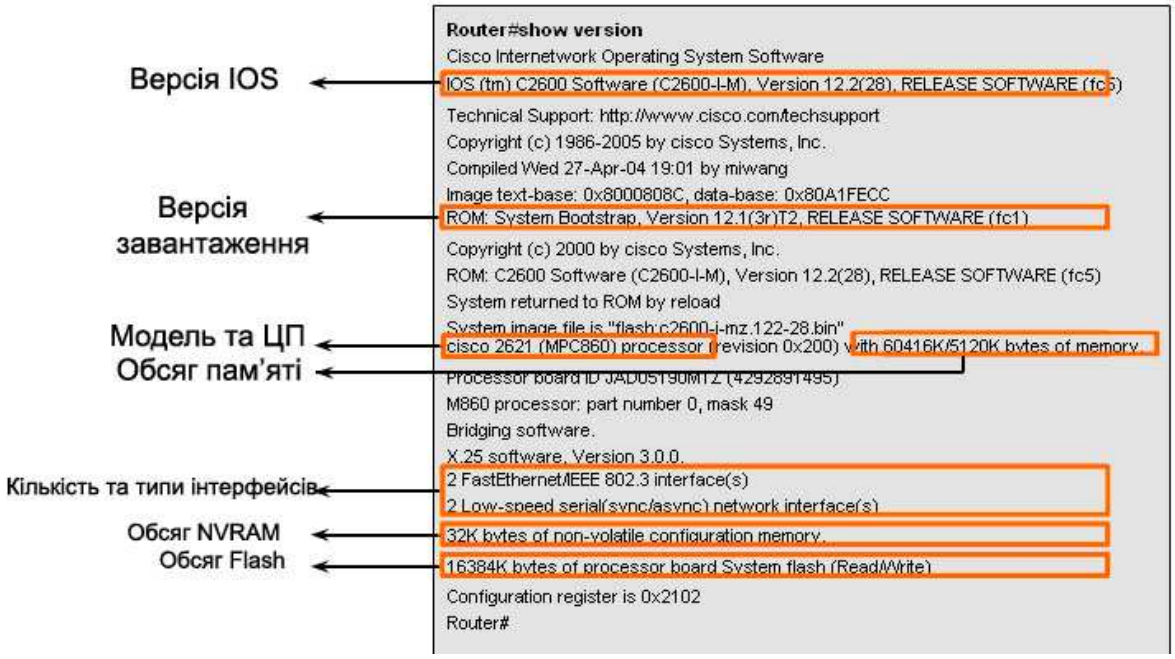



Рис. 1.4. *Перегляд результату виконання команди* `show version`

- **`show ARP`** – ARP-таблицю маршрутизатора;

- **`show ip protocols`** – параметри налаштування протоколу маршрутизації;
- **`show ip route`** – таблицю маршрутизації;
- **`show startup-configuration`** – конфігураційний файл запуску, який знаходиться у NVRAM;
- **`show running-configuration`** – поточну конфігурацію, яка знаходиться у RAM.

Усі налаштування, які виконуються на маршрутизаторі, зберігаються в оперативній пам'яті, яка втрачає свій зміст після ввімкнення живлення. Для збереження внесених змін слід скопіювати поточний конфігураційний файл (**`running-configuration`**) у конфігураційний файл запуску (**`startup-configuration`**), який зберігається постійно й використовується для завантаження після вимкнення:

```
Router#copy running-config startup-config
```

або скорочено

```
Router#copy run start.
```

Для перевірки збереження внесених змін можна перезавантажити маршрутизатор

```
Router#reload.
```

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета**: *ознайомлення зі способами підключення маршрутизатора, режимами роботи та можливостями, які вони надають.*

Конфігурація базових параметрів маршрутизатора включає в себе такі налаштування:

- ім'я маршрутизатора;
- пароль на доступ до привілейованого режиму;
- пароль на доступ до консолі;
- пароль на доступ до термінальних ліній;
- параметри інтерфейсів маршрутизатора.

Після цього необхідно здійснити перевірку налаштувань, створити конфігураційний файл запуску та в разі потреби зберегти або видалити налаштування.

На рис. 1.5 наведено схему мережі для проведення налаштувань, а в табл. 1.2 подано параметри налаштування.

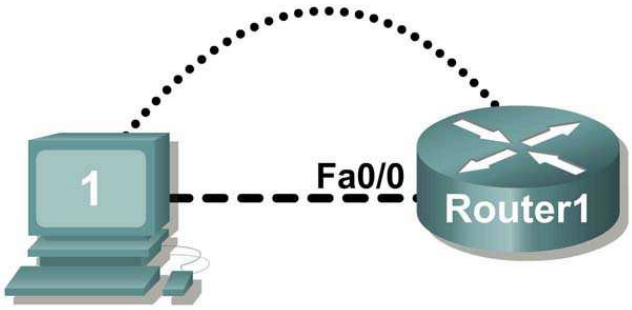



Рис. 1.5. *Схема з'єднання пристроїв*

**1. Фізичне з'єднання пристроїв**

Під'єднайте один кінець консольного (rollover) кабелю до консольного порту маршрутизатора, а інший з адаптером DB-9 або DB-25 – до послідовного порту комп'ютера COM 1. Перехресний (crossover) кабель використайте для з'єднання інтерфейсу мережної карти комп'ютера з інтерфейсом Fa0/0 маршрутизатора. Переконайтеся в тому, що на всі мережні та кінцеві пристрої подається живлення.

Таблиця 1.2

Параметри налаштування маршрутизатора

| **Параметр** | **Значення** |
|---|---|
| Ім'я маршрутизатора | Router1 |
| Пароль на привілейований режим | cisco |
| Пароль на консоль | class |
| Пароль на термінальні лінії | class |
| IP-адреса та маска інтерфейсу fa 0/0 | 10.0.0.100/24 |

**2. Запуск та налаштування параметрів програми HyperTerminal для утворення консольного з'єднання з маршрутизатором Cisco**

**2.1. Запуск програми HyperTerminal**

Здійсніть перехід **Start** (Пуск) **>** **Programs** (Програми)> **Accessories** (Стандартні) **>** **Communications** (Зв'язок)> **HyperTerminal**

**2.2. Налаштування HyperTerminal**

У діалоговому вікні опису з'єднання, що з'явилося, введіть довільну назву сеансу зв'язку в полі **Name** (Назва) та натисніть **OK**.


Рис. 1.6. *Вибір порту з'єднання*

Далі з'являтиметься вікно, екранна форма якого зображена на рис. 1.6. У єдиному активному полі **Connect using** (З'єднання з) оберіть назву послідовного порту комп'ютера, до якого під'єднано консольний кабель маршрутизатора. У лабораторних умовах, як і в зображеному прикладі, оберіть COM 1 та натисніть **OK**.

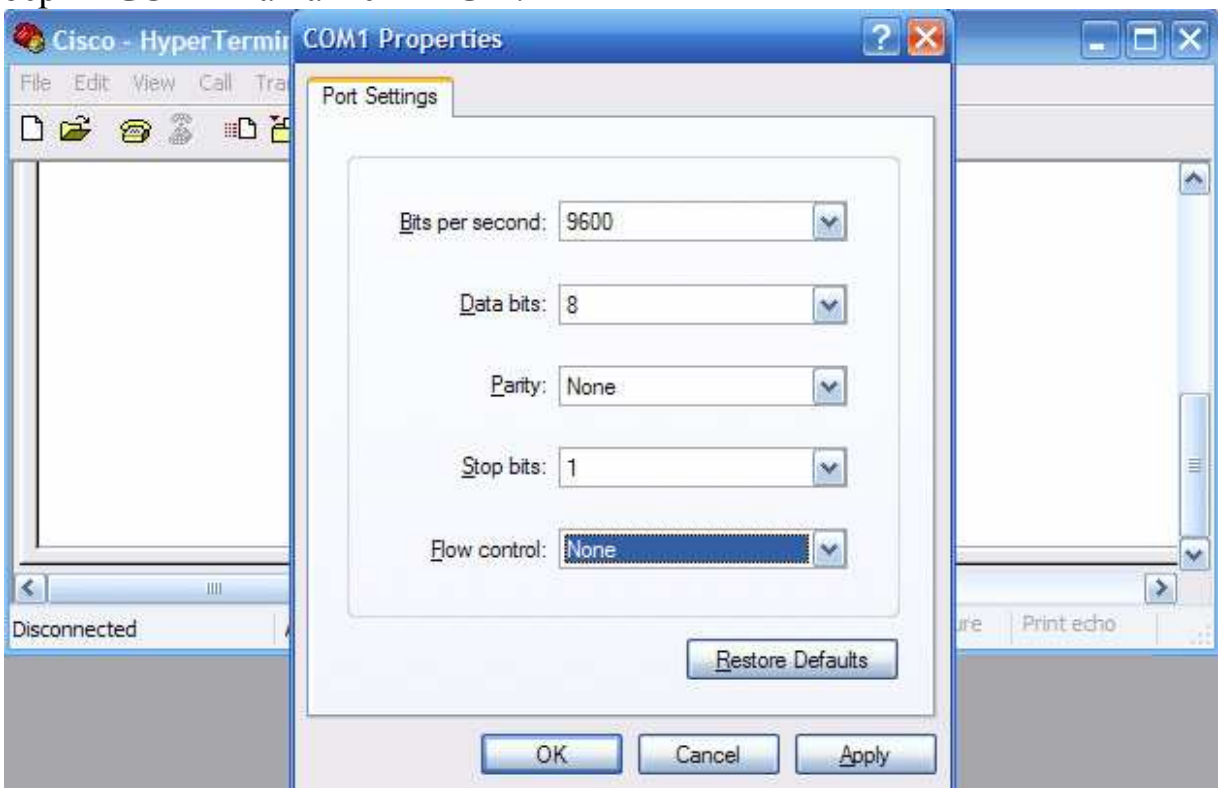



Рис. 1.7. *Налаштування параметрів порту з'єднання*

Наступним кроком є налаштування необхідних параметрів COM-порту, через який здійснюється консольне з'єднання. У вікні, зображеному на рис. 1.7, задайте такі параметри:

**Bits per second** (бітів за секунду) : 9600
**Data bits** (біти даних): 8
**Parity** (парність): None (Hi)
**Stop bits** (стопові біти): 1
**Flow control** (Контроль за потоком даних): None (Hi)

Натисніть **OK**.

Коли з'явиться вікно відкритого сеансу зв'язку через HyperTerminal, натисніть **Enter**. На екрані з'явиться відповідь маршрутизатора. Це означатиме, що консольне з'єднання налаштоване успішно. Якщо від маршрутизатора немає відповіді, перевірте спершу фізичні параметри підключення (живлення маршрутизатора, якість консольного кабелю, номер COM-порту комп'ютера), а потім параметри налаштування.

## 3. Налаштування параметрів маршрутизатора

### 3.1. Режими маршрутизатора

Коли на маршрутизаторі відсутні початкові налаштування, IOS запропонує користувачеві увійти в режим початкових налаштувань. На екрані з'явиться питання:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Оскільки при виконанні практичних завдань в подальшому цей режим налаштування маршрутизатора не використовується, слід ввести «**no**». Якщо випадково ввести «**yes**» й увійти в режим setup, цей процес можна припинити в будь-який момент, натиснувши комбінацію клавіш **CTRL+C**.

Після цього користувач опиняється в користувацькому режимі, про що свідчить позначка ">" біля імені маршрутизатора. Перейдіть до привілейованого режиму, набравши команду:

```
Router> enable
Router#
```

Використайте команду `show ?` для того, щоб переглянути всі можливі варіанти цієї команди в привілейованому режимі. Робоче поле програми HyperTerminal не може вмістити всі команди, а рядок " `-- more --` "

вказує на додаткову інформацію, яку ще можна переглянути. Для подальшого перегляду можна використати такі клавіші:

| | |
|---|---|
| **Пробіл** | Відобразити наступну сторінку |
| **Enter** | Відобразити наступний рядок |
| **Q або CTRL-C** | Вихід |

Використайте необхідну команду `show` для перегляду файлів конфігурації RAM і NVRAM маршрутизатора.

Для виходу з привілейованого режиму можна використати команди `disable` або `exit`.

### 3.2. Налаштування імені маршрутизатора

Перейдіть до режиму глобальної конфігурації:

```
Router# configure terminal
Router(config)#
```

*Команди можна записувати скорочено, натискаючи для їх продовження клавішу* **TAB**.

Змініть ім’я маршрутизатора за власним бажанням, наприклад:

```
Router(config)# hostname Router1
Router1(config)#
```

### 3.3. Налаштування паролів на маршрутизаторі Cisco

Паролі регламентують доступу до привілейованого режиму, на вхід користувачів через консольний та допоміжний порти, а також через віртуальні термінальні лінії.

#### *3.3.1. Налаштування пароля на перехід до привілейованого режиму*

Пароль на вхід до привілейованого режиму найбільш важливий, адже він контролюватиме доступ до режиму конфігурації.

Як уже зазначалося, Cisco IOS підтримує дві команди, які контролюють доступ до привілейованого режиму: **enable password** і **enable secret**. Остання команда використовує для захисту введеного пароля надійний алгоритм шифрування MD5, тому цей пароль називають секретом, адже його не можна переглянути або відновити при вивченні вмісту конфігураційного файла.

Встановіть пароль **cisco** на привілейований режим.

```
Router1(config)# enable secret cisco
Router1(config)#
```

### *3.3.2. Налаштування пароля на консоль*

Якщо маршрутизатор знаходиться в незахищеному приміщенні, до якого мають доступ безліч користувачів, під'єднання до нього через консольний порт із метою перегляду, зміни або видалення конфігурації не вимагатиме надмірних зусиль зловмисника. Тому для захисту маршрутизатора від несанкціонованого втручання через консольний порт необхідно налаштувати пароль на консолі.

Згідно з таблицею 6.2 налаштуємо на консолі пароль **class**.

```
Router1(config)# line console 0
Router1(config-line)# password class
Router1(config-line)# login
```

### *3.3.3. Налаштування пароля на віртуальних термінальних лініях*

До пристрою з налаштованою IP-адресою і підключеного до мережі можна звернутися за протоколом **Telnet**, що дозволить віддаленому користувачеві переглядати та змінювати налаштування. Звернення відбувається по так званих віртуальних лініях і забезпечує доступ до пристрою одночасно кількох користувачів. Для обмеження доступу зловмисників та надання можливості звернення по протоколу Telnet авторизованим користувачам на маршрутизаторі необхідно встановлювати пароль доступу на віртуальні термінальні лінії. В нашому випадку налаштуємо пароль **class**. Усього є п'ять термінальних ліній із номерами від 0 до 4. Можна встановити на кожну лінію окремий пароль або використати однаковий пароль для всіх ліній, що ми і зробимо далі.

```
Router1(config-line)# line vty 0 4
Router1(config-line)# password class
uter1(config-line)# login
```

*Зауважимо: якщо паролі на термінальну лінію не встановлено, до маршрутизатора неможливо буде отримати доступ через* ***Telnet****.*

## 3.4. Налаштування локального інтерфейсу fa0/0 маршрутизатора*

Застосуйте для налаштування даного інтерфейсу такі команди:

```
Router1(config)# interface fa0/0
Router1(config-if)# description Connection to Host1
Router1(config-if)# ip address 10.0.0.100 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# end
```

** Зауважте, що для різних моделей маршрутизатора тип та номер інтерфейсу можуть відрізнятися. Переглянути відповідні назви можна за допомогою команди* `show ip interface brief`.

Після виконаних налаштувань на екрані повинно з'явитися повідомлення про те, що інтерфейс перейшов до активного стану, наприклад, таке:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Перейдіть до привілейованого режиму. Вийти з режиму глобальної конфігурації можна за допомогою команди **`exit`** або, натиснувши комбінацію клавіш **CTRL-Z**.

### 4. Перегляд налаштувань і перевірка з'єднання

#### 4.1. Перевірка налаштувань

Після проведений налаштувань необхідно переконатися в правильності введених параметрів і зберегти їх. За замовчуванням Cisco IOS усі зміни конфігурації зберігаються у оперативній пам'яті у файлі під назвою **running-configuration**.

Перегляньте поточні налаштування за допомогою команди:

```
Router1# show running-configuration
```

*В якому вигляді відображаються налаштовані паролі?*

Для перевірки стану саме інтерфейсів маршрутизатора виконайте команду:

```
Router1# show ip interface brief
```

*Запишіть назви інтерфейсів та їх стани після проведених налаштувань.*

#### 4.2. Збереження налаштувань

Оперативна пам'ять втрачає свій вміст після вимкнення живлення. Щоб виконані налаштування вступили в дію при наступному запуску маршрутизатора, їх необхідно скопіювати до файла **startup-configuration** у NVRAM. Це не відбувається автоматично, тому щоразу при внесенні змін до конфігурації маршрутизатора файл запуску необхідно оновлювати вручну. Для цього слід виконати команду:

```
Router1#copy running-config startup-config
```

або скорочено

```
Router1#copy run start
```

```
Destination filename [startup-config]? <ENTER>
Building configuration...
[OK]
```

*Яку команду слід виконати для перегляду збереженого файла запуску?*

Після успішного збереження параметрів налаштування, перезавантажте маршрутизатор:

```
Router1# reload
Proceed with reload? [confirm] <ENTER>
```

*Як переглянути чи застосувалися нові параметри конфігурації після перезавантаження?*

### 4.3. Налаштування параметрів комп'ютера

Слід налаштувати мережні параметри робочої станції для мережі з адресою 10.0.0.0/24. При визначенні параметрів налаштування зауважте:

- IP-адреса визначається за номером комп'ютера в лабораторії;
- Маска налаштовується як чотири значення, відокремлені крапками;
- IP-адреса шлюзу – це IP-адреса інтерфейсу маршрутизатора, до якого під'єднано робочу станцію.

Перевірте виконані налаштування комп'ютера за допомогою команди **`ipconfig`**.

### 4.4. Перевірка мережного з'єднання

Використайте команду **ping** як на комп'ютері, так і на маршрутизаторі для перевірки мережного зв'язку. Який результат виконання даних команд? Якщо виникають проблеми зі з'єднанням, зверніть увагу на такі запитання:

*Чи ввімкнено всі мережні пристрої?*

*Який тип кабелю повинен використовуватися для з'єднання комп'ютера і маршрутизатора?*

*Які мережні параметри налаштування комп'ютера?*

*Яка команда Cisco IOS використовується для перевірки стану інтерфейсів маршрутизатора?*

### 4.5. Видалення налаштувань

Після успішного виконання всіх пунктів практичного завдання слід видалити конфігурацію маршрутизатора. Для цього в привілейованому режимі задайте команду:

```
Router1# erase start
```

```
  Erasing the nvram filesystem will remove all
configuration files! Continue? [confirm] <ENTER>
  [OK] Erase of nvram: complete
```

***Контрольні запитання та завдання***

1. Які існують типи конфігураційних файлів маршрутизатора? Де вони зберігаються?
2. Назвіть типи портів маршрутизатора. Які параметри слід налаштувати для утворення з'єднання кожного типу?
3. В чому призначення консольного порту?
4. За допомогою команди **`show version`** визначте:

а) версію операційної системи Cisco IOS ;

б) модель маршрутизатора та тип процесора;

в) загальний обсяг оперативної пам'яті;

г) загальний обсяг енергонезалежної пам'яті;

д) обсяг флеш-пам'яті.

5. Яка команда дає повну інформацію про обсяг і вміст флеш-пам'яті. Застосуйте її для визначення назви файлу Cisco IOS та його розміру.
6. Які параметри слід налаштувати на під'єданих портах маршрутизатора для утворення успішного з'єднання?
7. Який статус повинні мати інтерфейси маршрутизатора для успішної передачі даних?
8. В якому режимі можна здійснювати найбільш повний перегляд характеристик та налаштувань маршрутизатора? Наведіть приклади таких команд. Які ще можливості надає цей режим?
9. Які існують способи захисту маршрутизатора і як їх можна реалізувати за допомогою команд Cisco IOS?
10. Як переглянути та зберегти поточні налаштування маршрутизатора?

# ІІ. ПРОЦЕДУРА ЗАВАНТАЖЕННЯ МАРШРУТИЗАТОРА. ВІДНОВЛЕННЯ ПАРОЛІВ

Операційна система, яка використовується на маршрутизаторах Cisco, відома як Міжмережна операційна система Cisco (Cisco Internetwork Operating System, IOS). Як і будь-яка комп'ютерна операційна система, Cisco IOS керує апаратними і програмними ресурсами маршрутизатора, включаючи розподіл пам'яті, управління процесами, безпеку та файлові системи. Система Cisco IOS – це багатозадачна операційна система, яка поєднує функції маршрутизації, комутації, міжмережного зв'язку та передачі даних.

Хоча на різних моделях маршрутизаторів може використовуватися одна операційна система, існує широкий вибір різних образів IOS, в залежності від моделі маршрутизатора та його функцій. Звичайно, чим більше можливостей передбачено в IOS, тим більший обсяг флеш та оперативної пам'яті потрібен для збереження та завантаження IOS.

При запуску маршрутизатора конфігураційний файл запуску, який зберігається в NVRAM, копіюється в RAM як файл поточної конфігурації. IOS виконує ці конфігураційні команди. Будь-які зміни налаштування зберігаються у файлі поточної конфігурації і миттєво виконуються операційною системою.

На рис. 2.1 схематично зображено етапи завантаження маршрутизатора та процеси, які його супроводжують.

Зокрема, весь процес запуску маршрутизатора можна розбити на такі стадії:

1. Виконання процедури POST.
2. Завантаження програми запуску.
3. Виявлення та завантаження програмного забезпечення Cisco IOS.
4. Встановлення місцезнаходження та завантаження конфігураційного файлу або перехід до режиму початкового налаштування маршрутизатора.

### *1. Виконання процедури POST*

Самотестування при запуску (Power-On Self Test, POST) – це звичайний процес, який виконується на кожному комп'ютері при ввімкненні живлення. Процедура POST використовується для перевірки стану апаратного забезпечення маршрутизатора. При ввімкненні маршрутизатора, спеціалізована програма, яка зберігається у ROM, виконує самотестування, протягом якого здійснюється діагностика таких

апаратних компонент маршрутизатора, як CPU, RAM і NVRAM. Після завершення перевірки, виконується програма запуску.

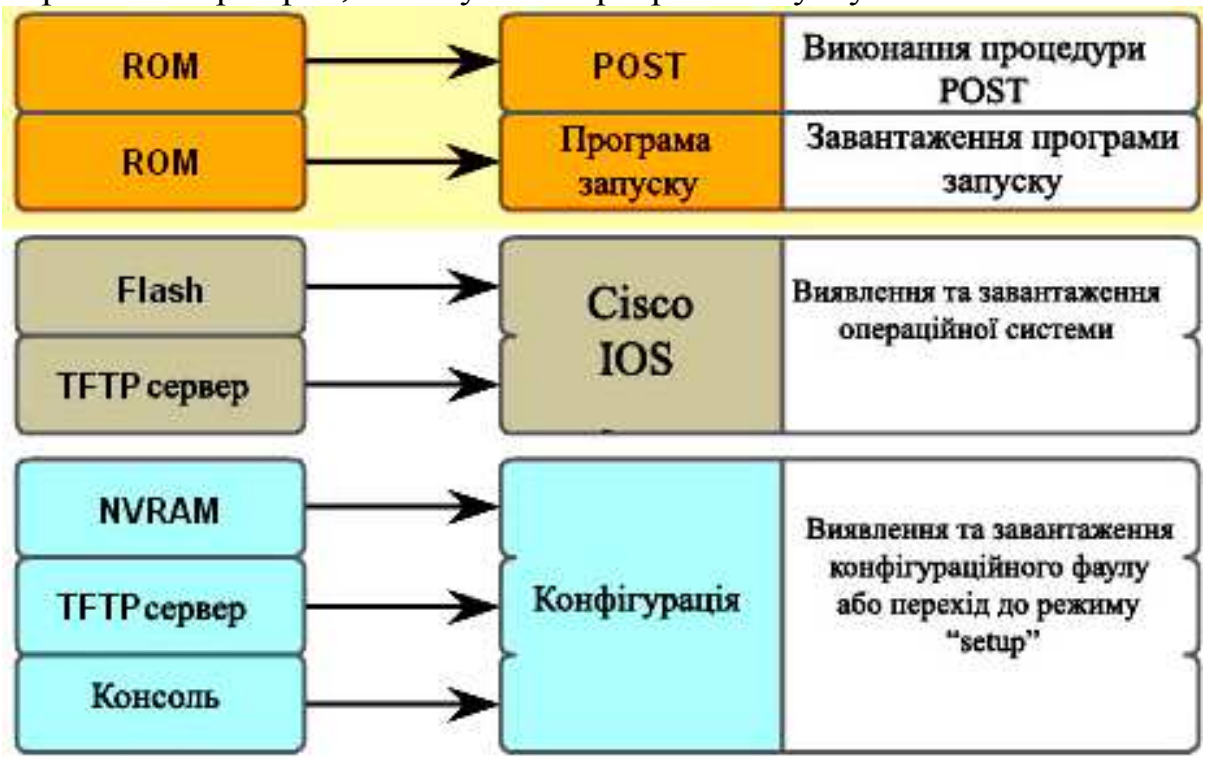



Рис. 2.1. *Етапи завантаження маршрутизатора*

***2. Завантаження програми запуску***

Після проведення процедури POST програма запуску завданням якої є виявлення місцезнаходження образа IOS, копіюється з ROM у оперативну пам'ять, звідки центральний процесор виконує інструкції запуску операційної системи.

***3. Виявлення та завантаження Cisco IOS***

Образ IOS звичайно зберігається у флеш-пам'яті, але його копії також можуть зберігатися на TFTP-сервері.

Якщо повну версію IOS не знайдено, резервна скорочена версія операційної системи копіюється з ROM у RAM. Дана версія IOS допомагає визначити проблему та завантажити повну версію операційної системи.

При завантаженні IOS розпаковується та вивантажується з флеш-пам'яті у RAM для подальшого виконання процесором.

На початку завантаження при розпаковці IOS на екрані з'являється кілька рядків решіток (#).

***4. Виявлення та завантаження конфігураційного файла***

Після завантаження операційної системи програма запуску виконує пошук конфігураційного файла запуску (**startup-config**) у NVRAM. Цей файл містить попередньо збережені налаштування таких параметрів маршрутизатора, серед яких:

- адреси інтерфейсів;
- інформація про маршрути;
- паролі.

Конфігураційний файл запуску з енергонезалежної пам'яті копіюється у файл поточної конфігурації (running-config) в оперативній пам'яті.

Якщо конфігураційний файл запуску не знайдено в NVRAM, маршрутизатор може намагатися відшукати його на TFTP-сервері. У разі виявлення активного з'єднання з іншим налаштованим маршрутизатором, маршрутизатор надсилає широкомовні повідомлення в пошуках конфігураційного файла. Це спричинятиме зупинку в роботі маршрутизатора на деякий час і супроводжується появою на екрані повідомлень, подібних до наведених нижче:

```
  %Error opening tftp://255.255.255.255/network-confg
(Timed out)
  %Error opening tftp://255.255.255.255/cisconet.cfg
(Timed out)
```

Якщо конфігураційний файл запуску знайдено, IOS завантажує його в оперативну пам'ять та послідовно виконує команди з файла.

При відсутності конфігураційного файла, маршрутизатор пропонує користувачеві перейти в режим налаштування (setup). Даний режим надає можливість визначити основні параметри маршрутизатора за допомогою підказок, проте в ньому неможливо виконати більш складні налаштування.

Коли режим setup не використовується, IOS створює за замовчуванням порожній файл running-config.

З міркувань безпеки на мережних пристроях налаштовують декілька типів паролів, аби запобігти неавторизованому доступу до налаштувань і параметрів пристроїв і мережі в цілому.

По-перше, щоб обмежити доступ до маршрутизатора при утворенні фізичного з'єднання між комп'ютером та маршрутизатором за допомогою консольного кабелю, використовують **пароль на консолі (console password)**, який при перегляді налаштувань відображається у відкритому вигляді. Пароль на консолі перешкоджає несанкціонованому під'єднанню до мережного пристрою й запитується першим, перед користувацьким режимом.

Паролі **enable password** і **enable secret** забезпечують аутентифікацію для доступу до привілейованого режиму, з якого легко потрапити до режиму глобальної конфігурації. Головна різниця між ними в тому, що перший **enable password** використовується у ранніх версіях Cisco IOS і відображається при перегляді налаштувань у відкритому вигляді. Кращий рівень захисту забезпечує пароль **enable secret**, до якого застосовується шифрування, отже, його неможливо переглянути і в разі втрати слід змінювати на новий.

Зауважимо: якщо на маршрутизаторі не налаштовано жодного з двох паролів **enable password** / **enable secret**, IOS перешкоджає доступ до привілейованого режиму при Telnet-з'єднанні у такий спосіб:

```
Router>enable
% No password set
Router>.
```

При відновленні пароля важливе значення конфігураційного регістру. Цей параметр подібний до налаштувань BIOS комп'ютера, який керує процесом завантаження. Окрім іншого, BIOS диктує ПК, з якого жорсткого диска здійснювати завантаження. На маршрутизаторі конфігураційний регістр відображається єдиною шістнадцятковою величиною і вказує, які етапи проходитиме маршрутизатор при ввімкненні. В залежності від потреб, значення конфігураційного регістра можна налаштовувати вручну, зокрема: при виконанні процедури відновлення паролів.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *набуття навичок у виконанні процедури відновлення та зміни паролів різних типів на маршрутизаторах Cisco серій 1700, 1800 та 2800.*

### 1. Утворення консольного з'єднання та перегляд поточного значення конфігураційного регістру

У привілейованому режимі введіть команду ***show version*** і запишіть значення конфігураційного регістру (configuration register).

```
R>#show version
<деякий вивід пропущено>
Configuration register is 0x2102
R1>
```

Значення конфігураційного регістру звичайно дорівнює 0x2102 або 0x102. Виконайте налаштування паролів різних типів. Збережіть конфігурацію. Перезавантажте маршрутизатор.

**3. Перехід до режиму ROMmon**

Протягом перших 30 секунд завантаження маршрутизатора натисніть комбінацію клавіш **Ctrl**+**Break** для переходу в режим ROMmon.

**4. Зміна стандартного значення конфігураційного регістру**

На екрані з'являється надпис **`rommon1>`**, після якого наберіть команду **`confreg 0x2142`**. Саме таке значення конфігураційного регістру використовується при відновленні паролів. Дана команда змінює значення конфігураційного регістру для того, щоб маршрутизатор при наступному перезавантаженні ігнорував початкові налаштування, що зберігаються в конфігураційному файлі **startup-config**, зокрема, не застосовував паролі, які були втрачені та перешкоджають переходу до системи налаштувань.

**5. Перезавантаження маршрутизатора**

Натисніть **Enter** і наберіть команду **`reset`** після **`rommon 2>`**. Маршрутизатор перезавантажується, проте ігнорує попередньо збережену конфігурацію.

Наберіть **`no`** у відповідь на пропозицію перейти в режим **setup**, або натисніть **Ctrl-C** аби припинити початкові налаштування..

**6. Доступ до збережених налаштувань**

Перейдіть у привілейований режим. Введіть команду **`copy startup-config running-config`** щоб скопіювати проігнорований конфігураційний файл із попередніми налаштуваннями з NVRAM в оперативну пам'ять.

**УВАГА! Не вводьте** `copy running-config startup-config`, **інакше всі попередні налаштування видаляться.**

**7. Перегляд і заміна паролів**

Перегляньте скопійовану поточну конфігурацію за допомогою команди **`show running-config`**. При виведенні можна побачити налаштування, серед яких є паролі (enable password, enable secret, vty, console) у зашифрованому або відкритому вигляді, які можна відновити або замінити на нові.

У режимі глобальної конфігурації замініть паролі на перехід у привілейований режим.

Наприклад:

```
R1(config)# enable secret cisco
```

**8. Зміна значення конфігураційного регістру**

Після внесення всіх необхідних змін налаштуйте стандартне значення конфігураційного регістру, яке ви одержали у п. 2:

```
R1(config)#config-register 0x2102
```

*Якщо не замінити значення конфігураційного регістру на стандартне, будь-які збережені зміни в конфігурації не будуть застосовуватися.*

Вийдіть з конфігураційного режиму. Збережіть внесені зміни до конфігураційного файла за допомогою команди `copy running-config startup-config`. Перезавантажте маршрутизатор і перевірте чи були застосовані нові параметри.

***Контрольні запитання та завдання***

1. Опишіть основні етапи завантаження маршрутизатора.
2. Які є способи захисту маршрутизатора від несанкціонованого під'єднання?
3. Назвіть типи паролів, передбачені для налаштування на маршрутизаторі? Яке їх призначення?
4. Яка команда дозволяє переглянути налаштовані паролі?
5. В чому полягає між паролями enable password і enable secret?
6. Що таке «конфігураційний регістр»? Яке його стандартне значення? Як його можна переглянути і змінити? Наведіть значення, які він може приймати та їх зміст.
7. Яке призначення команди `service password-encryption`?
8. Адміністратор виконав налаштування маршрутизатора і зберіг їх за допомогою команди `copy run start`. Після перезавантаження виявилося, що налаштування не збереглися. Назвіть одну з можливих причин такої поведінки маршрутизатора.
9. Як можна відновити невідомий або втрачений пароль на маршрутизаторі?
10. Як забезпечити авторизований доступ до маршрутизатора за протоколом Telnet?

# ІІІ. СТАТИЧНА МАРШРУТИЗАЦІЯ

Для того, щоб пакети просувалися по мережі, кінцеві та проміжні мережні пристрої повинні знати маршрут до мережі призначення. У цьому розділи ми порівняємо, як створюються та використовуються маршрути на робочих станціях з ОС Windows і маршрутизаторах Cisco.

### *З'єднання з віддаленими мережами*

Маршрутизатор, як випливає з його назви, приймає рішення щодо направлення будь-якого пакета, який надходить на його інтерфейси, тобто виконує *маршрутизацію* даних. Для направлення пакетів до цільової мережі маршрутизатор потребує визначення маршруту до цього пункту призначення, інакше пакети не можуть бути надіслані.

Для збереження інформації про маршрути використовується таблиця маршрутизації. Деякі маршрути додаються до таблиці автоматично на основі параметрів, налаштованих на мережному інтерфейсі. Налаштування IP-адреси та маски означатиме, що до пристрою безпосередньо підключена мережа, до якої вони належать, а маршрут до цієї мережі автоматично додається до таблиці маршрутизації. Для того щоб зв'язатися з віддаленими мережами, на кінцевому пристрої налаштовується адреса шлюзу, що володіє інформацією про маршрути, за якими слід надсилати трафік. У великих мережах *роль шлюзу відіграє маршрутизатор*.

Віддалена мережа може бути відокремлена від шлюзу кількома проміжними маршрутизаторами, які ще називають *стрибками*. Для кожного маршрутизатора на шляху до мережі призначення дороговказом служить адреса наступного стрибка, тобто інтерфейсу сусіднього маршрутизатора, з яким наявне безпосереднє з'єднання і до якого просувається пакет.

### *Характеристики маршрутів*

Основними характеристиками маршруту є *метрика* та *адміністративна відстань*.

***Метрика*** – це безрозмірна характеристика шляху, яка вказує на переваги того чи іншого шляху перед іншими. Метрика може бути досить простою (кількість проміжних пунктів до отримувача) або розраховуватися за складною формулою на основі багатьох показників (пропускна здатність каналу, його завантаженість, затримки і т.д.). Як правило, найоптимальнішим вважається шлях із мінімальною метрикою.

***Адміністративна відстань*** – це показник надійності джерела, яке повідомило про маршрут. Ця величина визначена стандартом протоколу маршрутизації. Чим менша адміністративна відстань, тим надійніший протокол.

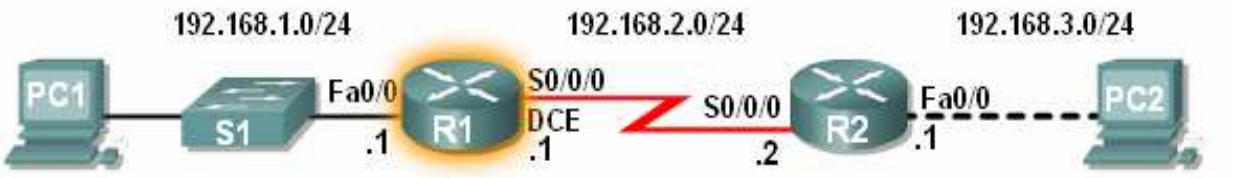



Рис. 3.1. *Топологія мережі для налаштувань маршрутизаторів*

Таблиця 3.1

Адресна схема мережі

| **Тип пристрою** | **Тип інтерфейсу** | **IP-адреса** | **Маска** |
|---|---|---|---|
| PC1 | NIC | 192.168.1.2 | 255.255.255.0 |
| R1 | Fa0/0 | 192.168.1.254 | 255.255.255.0 |
| R1 | S0/0/0 | 192.168.2.1 | 255.255.255.0 |
| R2 | S0/0/0 | 192.168.2.2 | 255.255.255.0 |
| R2 | Fa 0/0 | 192.168.3.254 | 255.255.255.0 |
| PC2 | NIC | 192.168.3.1 | 255.255.255.0 |

***Створення статичних маршрутів***

На маршрутизаторі відомості про маршрути відображаються набагато детальніше, ніж на комп'ютері. Це й не дивно, адже одна з основних функцій маршрутизатора полягає у спрямуванні трафіка між різними мережами, для чого потрібна саме така інформація.

Пакети направляються до мереж призначення за IP-адресами призначення. Для цього маршрутизатор повинен віднаходити в таблиці маршрутизації інформацію про маршрути до мережі отримувача.

Таблиця маршрутизації – це файл даних у RAM, який використовується для збереження інформації про безпосередньо під'єднані та віддалені мережі. Таблиця зберігає зв'язок між адресою відомої мережі та наступним стрибком (шлюзом), через який до неї можна дістатися. Окрім шлюзу, зазначається також назва та номер власного інтерфейсу маршрутизатора, який ще називають вихідним портом. Саме на цей інтерфейс перекомутовується пакет на шляху до пункту призначення.

*Безпосередньо під'єднана мережа* – це мережна ланка, яка підключена до одного з портів маршрутизатора. Після того, як інтерфейс маршрутизатора відкрито за допомогою команди **no shutdown**, налаштовано на ньому IP-адресу та мережну маску, інтерфейс стає вузлом цієї під'єднаної мережі. Мережна адреса та маска інтерфейсу разом з його типом і номером автоматично додаються до таблиці маршрутизації як безпосередньо під'єднана мережа (**directly connected network**).

*Віддалена мережа* – це мережа, яка не під'єднана безпосередньо до маршрутизатора. Інакше кажучи, до віддаленої мережі можна потрапити шляхом надсилання пакета до іншого (сусіднього) маршрутизатора. Віддалені мережі можуть додаватися до таблиці маршрутизації автоматично за допомогою динамічного протоколу маршрутизації або вручну шляхом налаштування статичних маршрутів.

На маршрутизаторі для перегляду вмісту таблиці маршрутизації використовується команда **show ip route**. Без додаткових налаштувань таблиця маршрутизації R1 (рис. 3.1) міститиме лише під'єднані мережі, для кожної з яких наводиться така інформація:

```
R1# show ip route
Codes: C – connected, S – static, I- IGRP, R – RIP, M – mobile,
B – BGP, D – EIGRP, EX – EIGRP external, O – OSPF, IA – SPF inter
area, N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type
2, E2 – OSPF external type 2, E – EGP, I – IS-IS, L1  IS-IS level-
1, L2 – ISIS level-2, ia – IS-IS inter area, P- periodic downloaded
static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, Serial 0/0/0
```

Тут C позначає джерело інформації про маршрут, зокрема, чи мережа безпосередньо під'єднана (**C**), статично налаштований маршрут (**S**) або динамічно повідомлений протоколом маршрутизації, таким як RIP, EIGRP, OSPF, (**R**, **D**, **O**, відповідно);

192.168.1.0/24 – мережна адреса та маска під'єднаної або віддаленої мережі. В даному прикладі обидва записи, 192.168.1./24 та 192.168.2.0/24, відображають інформацію про під'єднані мережі;

FastEthernet 0/0 – інформація в кінці запису, яка позначає вихідний інтерфейс і/або IP-адресу шлюзу, до якого слід перенаправити пакет на шляху до мережі призначення. У даному прикладі обидва інтерфейси,

FastEthernet 0/0 та Serial0/0/0, вихідні й належать до мереж, безпосередньо під'єднаних до маршрутизатора R1.

Для утворення зв'язку з віддаленими мережами, а отже, забезпечення функції маршрутизації пакетів, на маршрутизаторі часто використовують статичне налаштувати шляхів. Даний спосіб зручно використовувати в невеликих мережах, які не зазнають частих змін.

Для налаштування статичного маршруту використовується команда в режимі глобальної конфігурації:

`Router(config)#` **`ip route`** *IP-адреса_мережі_призначення маска IP-адреса_інтерфейсу_наступного стрибка| вихідний інтерфейс* `[`*адміністративна відстань*`].`

При налаштуванні статичного маршруту після команди **ip route** слід вказати IP-адресу та маску віддаленої мережі, до якої прокладається шлях. Далі зазначається або IP-адреса інтерфейсу сусіднього маршрутизатора, через який можна потрапити до мережі призначення, або тип та номер власного інтерфейсу маршрутизатора, на який переправляється пакет на шляху до отримувача. Необов'язковим параметром є адміністративна відстань, яка позначає рівень довіри до маршруту. Чим менша ця величина, тим більш оптимальним вважається маршрут. Для статичних маршрутів адміністративна відстань дорівнює одиниці, проте її можна змінити, вказавши значення в діапазоні від 0 до 255.

Для створення статичного маршруту на маршрутизаторі R1 до мережі 192.168.3.0/24 використовується одна з двох команд:

`R1(config)#` **`ip route 192.168.3.0 255.255.255.0 192.168.2.2`**

або

`R1(config)#` **`ip route 192.168.3.0 255.255.255.0 s 0/0/0`**

*Зауважимо: для утворення двостороннього зв'язку між усіма точками мережі, зображеної на рис. 7.1, на маршрутизаторі R2 також потрібно налаштувати статичний маршрут до мережі 192.168.1.0/24.*

Після створення маршрутів у різних напрямках до всіх існуючих мереж, можна переглянути таблицю маршрутизації:

`R1#` **`show ip route`**

```
Codes: C – connected, S – static, I- IGRP, R – RIP, M – mobile,
B – BGP, D – EIGRP, EX – EIGRP external, O – OSPF, IA – SPF inter
area, N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type
2, E2 – OSPF external type 2, E – EGP, I – IS-IS, L1  IS-IS level-
1, L2 – ISIS level-2, ia – IS-IS inter area, P- periodic downloaded
static route

Gateway of last resort is not set
```

```
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, Serial 0/0/0
S 192.168.3.0/24 [1/0] via 192.168.2.2
```

У цьому прикладі S позначає статично налаштований маршрут до мережі 192.168.3.0/24. Параметри у квадратних дужках – 1 та 0 – позначають, відповідно, адміністративну відстань та метрику для даного маршруту. Останній параметр, 192.168.2.2, позначає адресу інтерфейсу шлюзу, тобто сусіднього маршрутизатора, через який можна потрапити до мережі 192.168.3.0.

Перевірка з'єднання між віддаленими точками мережі здійснюється за допомогою команд **ping** і **traceroute** (скор. **trace**). Для зв'язку з іншими маршрутизаторами, крім IP-адрес інтерфейсів, можна використовувати умовні імена. Для цього необхідно на кожному вузлі створити таблицю хостів з іменами та адресами сусідніх шлюзів:

Router(config)#**ip host** *назва <перелік IP-адрес інтерфейсів маршрутизатора>*

Наприклад, створимо на маршрутизаторі R1 таблицю імен сусідніх маршрутизаторів:

R1(config)# **ip host R2 192.168.2.2 192.168.3.254**

Якщо як параметр команди **ping** використовується не IP-адреса конкретного інтерфейсу маршрутизатора, а його ім'я, звернення здійснюється послідовно за всіма адресами в порядку їхнього розташування в переліку.

Найбільш повний механізм тестування та засіб перевірки роботи прикладного рівня забезпечує протокол **Telnet**. Для з'єднання по даному протоколу з віддаленим маршрутизатором *у користувацькому режимі* використовують його IP-адресу та/або ім'я як самостійно, так і разом зі службовими словами **telnet** або **connect**. Наприклад, на маршрутизаторі Rome можливі такі варіанти утворення з'єднання з маршрутизатором на ім'я Paris із IP-адресою 115.105.10.1:

Rome> **connect** Paris

Rome> **telnet** Paris

Rome> Paris

Rome>**115.105.10.1**

Команди **disconnect** або **logout** використовуються для завершення сеансу з'єднання.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *налаштування основних параметрів маршрутизаторів, створення статичних маршрутів, перевірка з'єднання між усіма пристроями мережі.*

Схема мережі для налаштувань зображена на рис. 3.2. Параметри налаштувань подано в таблиці 3.2.

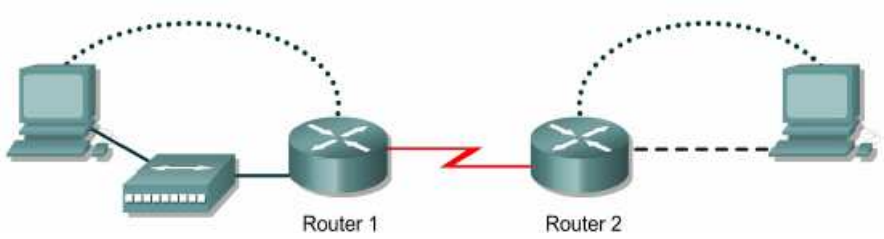



Рис. 3.2. *Топологія мережі для налаштування*

### 1. З'єднання пристрої за вказаною схемою

Зверніть увагу на типи з'єднувальних кабелів та інтерфейсів. Зокрема, кінець DCE нуль-модемного кабелю приєднайте до послідовного порту serial 0/0 маршрутизатора Router 1, а кінець DTE – до serial 0/1 Router 2.

Таблиця 3.2

Параметри налаштування

| **Позначення пристрою** | **Ім'я пристрою** | **Інтерфейс** | **IP-адреса/ маска** | **Паролі** |
|---|---|---|---|---|
| Router1 | Lviv | Fa0/0 | 192.168.14.1/24 | enable secret: **class** |
| | | S0/0 (DCE) | 192.168.15.1/24 | console, vty: **router** |
| Router 2 | Donetsk | S0/1 (DTE) | 192.168.15.2/24 | enable secret: **static** |
| | | Fa 0/0 | 192.168.16.1/24 | console, vty: **config** |
| PC1 | | NIC | 192.168.14.2/24 | - |
| PC2 | | NIC | 192.168.16.2/24 | - |

### 2. Налаштування параметрів маршрутизаторів (табл. 3.2)

Змініть імена маршрутизаторів, налаштуйте відповідні паролі на консольне з'єднання, привілейований режим та віртуальні термінальні лінії та параметри з'єднаних інтерфейсів обох маршрутизаторів.

Якщо налаштування проведені успішно, на екрані з'являтиметься повідомлення про те, що відповідний порт перейшов у відкритий стан.

**3. Збережіть конфігурацію.**

*Яка команда відображає поточну конфігурацію маршрутизатора?* Збережіть виконані налаштування та перевантажте маршрутизатори.

**4. Налаштування параметрів робочих станцій**

Запишіть параметри налаштування для кожної робочої станції:
*IP-адреса:*_____
*Маска:*_____
*IP-адреса шлюзу*_____

**5. Перевірка наявності зв'язку**

**5.1.** Використайте команду **ping** для перевірки наявності з'єднання між пристроями та інтерфейсами (табл. 3.3). Наведіть результати перевірки з'єднання для кожного випадку та поясніть їх.

Таблиця 3.3

| **Пункт 1** | **Пункт 2** | **IP-адреса призначення** | **Результат ping** |
|---|---|---|---|
| PC1 | FastEthernet0/0 (Router 1) | | |
| PC1 | Serial 0/0 (Router 1) | | |
| PC1 | PC2 | | |
| Router1 | Serial 0/1 (Router 2) | | |
| Router 1 | FastEthernet0/0 (Router 2) | | |
| Router 1 | PC1 | | |
| Router 1 | PC2 | | |
| Router 2 | Serial 0/0 (Router 1) | | |
| Router 2 | FastEthernet0/0 (Router 1) | | |
| Router 2 | PC2 | | |
| Router 2 | PC1 | | |
| PC2 | FastEthernet0/0 (Router 2) | | |
| PC2 | FastEthernet0/0 (Router 1) | | |
| PC2 | Serial 0/0 (Router 1) | | |
| PC2 | PC1 | | |

**5.2.** У разі відсутності зв’язку використайте команду **traceroute** для виявлення, на якій саме ділянці мережі втрачається з’єднання.

*Чим пояснюється відсутність з’єднання?*

**5.3.** Перегляньте стан інтерфейсів маршрутизатора, з якими відсутній зв’язок.

*Наведіть команди, які слід використати для перегляду загальної та детальної інформації про інтерфейси, та результати їх виконання.*

Для успішного функціонування всі з’єднані інтерфейси маршрутизаторів повинні знаходитися у відкритому стані «up».

*Чи виявила перевірка можливі причини відсутності з’єднання? Якщо так, то вкажіть які?*

**5.4.** Перегляньте мережі, з якими може з’єднуватися маршрутизатор.

*Яка команда використовується для перевірки таблиці маршрутизації?*

Для кожного маршрутизатора наведіть вміст таблиці маршрутизації.

*Про що свідчать отримані дані? Чи можуть вони пояснити відсутність з’єднання, що спостерігалася?*

**6. Налаштування статичних маршрутів**

Головною, але не єдиною причиною невдалого з’єднання між крайніми точками мережі є відсутність у маршрутизатора відомостей про мережі, які під’єднані до його сусідів. Для того, щоб прокласти шлях до віддалених мереж, слід на обох маршрутизаторах налаштувати статичні маршрути.

**6.1.** Для кожного маршрутизатора заповніть табл. 3.4, внісши туди відповідні параметри для налаштування статичних шляхів.

Таблиця 3.4

Параметри віддалених мереж

| **Вихідний маршрутизатор** | **IP-адреса мережі** | **Маска** | **Вихідний інтерфейс** | **IP-адреса шлюзу*** |
|---|---|---|---|---|
| | | | | |

**Для безпосередньо під’єднаних мереж адресу шлюзу вказувати не потрібно.*

**6.2.** Запишіть команди для налаштування статичних маршрутів на кожному маршрутизаторі. Запустіть їх на виконання.

**6.3.** Перегляньте таблиці маршрутизації на кожному шлюзі.

*Чи спостерігаються зміни в переліку відомих маршрутів? Наведіть вигляд таблиць маршрутів для кожного маршрутизатора.*

**7. Тестування параметрів з'єднання**

**7.1.** Повторно перевірте з'єднання між крайніми точками мережі в обох напрямках.

*Який результат тестування?*

**7.2.** *Яку команду слід використати для перегляду маршрутів робочих станцій?* Наведіть результат її виконання.

**7.3.** *Визначте та запишіть MAC-адреси, які відповідають налаштованим IP-адресам на інтерфейсах пристроїв у мережі. Яку команду слід для цього використати?*

**7.4.** Встановіть з'єднання за протоколом **telnet** з одним із маршрутизаторів.

*Які команди можна використати для встановлення та припинення з'єднання? Про що свідчить успішно налаштоване з'єднання за* **telnet***?*

**Після успішного виконання практичного завдання видаліть конфігурацію на обох маршрутизаторах та відновіть початкові параметри робочих станцій.**

***Контрольні запитання та завдання***

1. Наведіть основні характеристики маршрутизатора та вкажіть функції, які він виконує.
2. За якими показниками обирається оптимальний шлях передачі даних по мережі?
3. Які переваги та недоліки використання статичних маршрутів?
4. Наведіть команди налаштування статичних маршрутів для мережі, схема якої наведена на рис. 3.3.

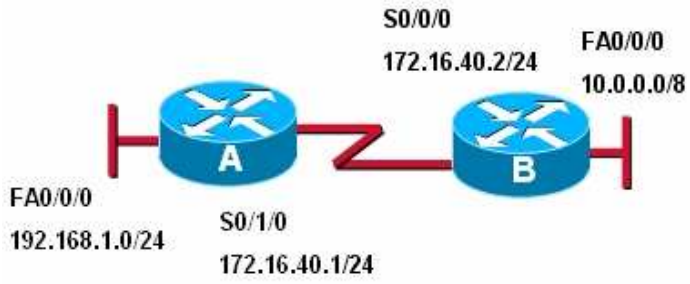



Рис. 3.3

5. Які існують способи перегляду активних маршрутів на робочій станції та маршрутизаторі?

# IV. ДИНАМІЧНА МАРШРУТИЗАЦІЯ. ПРОТОКОЛ RIP

При налаштуванні статичної маршрутизації адміністратор стикається з низкою проблем, зокрема значні затрати часу, велика ймовірність помилки й необхідність підтримки відповідності налаштувань. Динамічні протоколи маршрутизації найчастіше використовуються у великих мережах і дозволяють усунути недоліки статичних маршрутів.

***Протоколи маршрутизації***

Протоколи маршрутизації використовуються для динамічного поширення інформації про віддалені мережі між маршрутизаторами, визначення найкращого шляху до кожної мережі і автоматичного розміщення нової інформації про маршрути до таблиці маршрутизації. Для поширення інформації використовуються повідомлення-обновлення. Як правило вони розсилаються періодично. Отже, за будь-яких змін у топології мережі маршрутизатори динамічно одержують інформацію про нові мережі й можуть визначити альтернативні шляхи при втраті зв'язку на деякій ділянці з'єднання.

Розрізняють динамічні протоколи маршрутизації двох типів: дистанційно-векторні та стану каналу.

Протоколи першого типу рекламують відомі маршрути як вектор відстані та напрямку. Відстань визначається за допомогою метрики, такої як кількість проміжних вузлів, а напрямком є інтерфейс сусіднього маршрутизатора (шлюзу) або власний вихідний порт. Тому маршрутизатор «бачить» мережу з точки зору своїх сусідів. Дистанційно-векторні протоколи зазвичай використовують для визначення найкращого шляху алгоритм Беллмана–Форда. Для цих протоколів характерна поява петель маршрутизації.

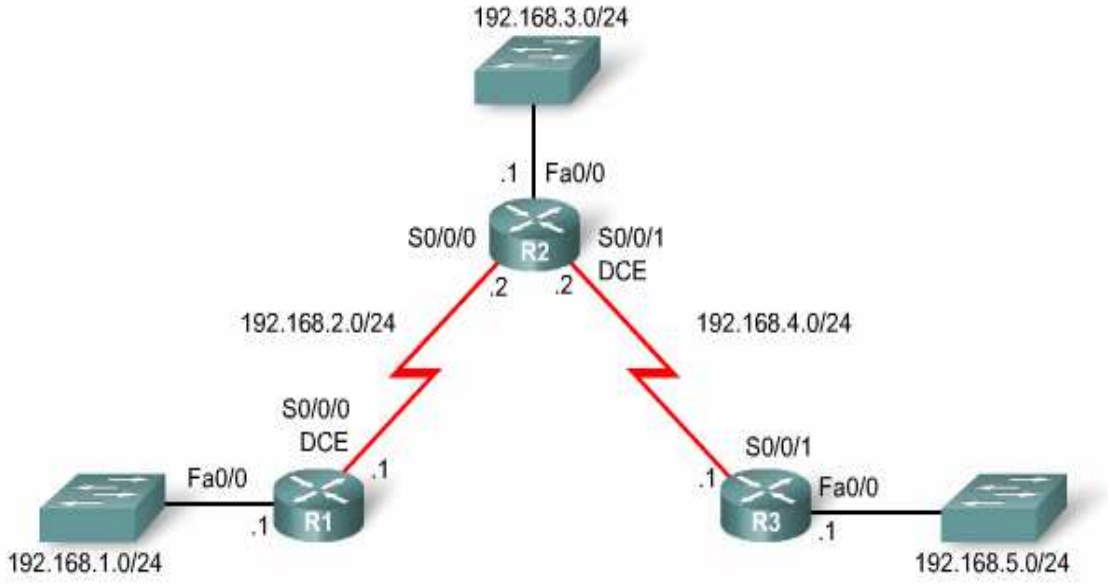
На відміну від дистанційно-векторних протоколів, маршрутизатор, на якому налаштований протокол маршрутизації стану каналу може створити «повну картину» або топологію всієї мережі на основі тієї інформації, яку він отримує від усіх маршрутизаторів у системі.

Зупинимося більш детально на дистанційно-векторних протоколах маршрутизації. Більшість протоколів цього типу потребують періодичної розсилки обновлень, які містять повні таблиці маршрутизації. Такий спосіб неефективний, оскільки обновлення не лише споживають пропускну здатність каналу передачі даних, але й ресурси маршрутизатора, зокрема його ЦП для обробки інформації, яка надходить.

***Протокол маршрутизації RIP***

Одним із найбільш поширених дистанційно-векторних протоколів для невеликих мереж є *Routing Information Protocol (RIP).* Він має такі характеристики:

- як метрика для визначення оптимального шляху використовується кількість проміжних вузлів;
- адміністративна відстань – 120;
- максимальна кількість пересилань –15;
- повідомлення-обновлення розсилаються кожні 30 секунд за широкомовною (255.255.255.255, RIP версії 1) або (груповою 224.0.0.9, RIP версії 2) адресами.




**R1**

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.1.0 | Fa 0/0 | 0 |
| 192.168.2.0 | S0/0/0 | 0 |
| | | |
| | | |
| | | |

**R2**

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.2.0 | S0/0/0 | 0 |
| 192.168.3.0 | Fa 0/0 | 0 |
| 192.168.4.0 | S0/0/1 | 0 |
| | | |
| | | |

**R3**

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.4.0 | S0/0/1 | 0 |
| 192.168.5.0 | Fa 0/0 | 0 |
| | | |
| | | |
| | | |

***а***

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.1.0 | Fa 0/0 | 0 |
| 192.168.2.0 | S0/0/0 | 0 |
| 192.168.3.0 | S0/0/0 | 1 |
| 192.168.4.0 | S0/0/0 | 1 |
| 192.168.5.0 | S0/0/0 | 2 |

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.2.0 | S0/0/0 | 0 |
| 192.168.3.0 | Fa 0/0 | 0 |
| 192.168.4.0 | S0/0/1 | 0 |
| 192.168.1.0 | S0/0/0 | 1 |
| 192.168.5.0 | S 0/0/1 | 1 |

| Мережа | Інтерфейс | М-ка |
|---|---|---|
| 192.168.4.0 | S0/0/1 | 0 |
| 192.168.5.0 | Fa 0/0 | 0 |
| 192.168.1.0 | S0/0/1 | 2 |
| 192.168.2.0 | S0/0/1 | 1 |
| 192.168.3.0 | S0/0/1 | 1 |

***б***

Рис. 4.1. *Приклад топології мереж і схематичний вигляд таблиць маршрутизації: а – після виконання базових налаштувань маршрутизаторів; б – при використанні протоколу маршрутизації RIP у даній системі*

При підключенні маршрутизатора до мережі й налаштуванні його базових параметрів, таких як IP-адреси інтерфейсів та протокол маршрутизації, маршрутизатор володіє інформацією лише про ті мережі, які до нього безпосередньо під'єднані. Вміст початкових таблиць маршрутизації схематично зображено на рис. 4.1, а. Проте, завдяки роботі протоколу RIP, після двох періодичних обновлень (тобто приблизно через 60 секунд) таблиці маршрутизації набувають вигляду, показаного на рис. 4.1,б.

***Налаштування роботи протоколу маршрутизації RIP***

До конфігурування будь-якого динамічного протоколу маршрутизації можна переходити після відповідних налаштувань IP-адрес на з'єднаних інтерфейсах.

Спочатку необхідно в режимі глобальної конфігурації вибрати протокол маршрутизації:

`Router(config)# router` *протокол_ маршрутизації*

та задати мережі, про які будуть розповсюджуватися повідомлення найближчим сусідам:

`Router(config-router)# network` *IP-адреса_під'єднаної мережі*

Зокрема, для маршрутизатора R1 на схемі мережі (рис. 4.1) налаштування протоколу RIP будуть такими:

```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

Команда **network** активує протокол RIP на всіх інтерфейсах, які належать цій мережі, тобто через них будуть надходити та розсилатимуться обновлення RIP, а інформація про ці мережі надходитиме до інших маршрутизаторів кожні 30 секунд.

*Подібні налаштування необхідно виконати на кожному маршрутизаторі в системі, вказавши відповідні під'єднані мережі:*

```
R2(config)#router rip
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0

R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
```

Після проведених налаштувань необхідно перейти до привілейованого режиму і зберегти поточну конфігурацію до NVRAM.

***Перевірка RIP -маршрутизації***

Команда **show ip route** використовується для перегляду всіх мереж топології, внесених до таблиці маршрутизації, на кожному маршрутизаторі.

Маршрути, які були визначені завдяки протоколу RIP, позначаються літерою **R**. Із запису можна одержати таку інформацію:

**R** *адреса_віддаленої_мережі/маска* [*адмін.відстань/метрика*] via *IP-адреса шлюзу час_існування_у_таблиці, локальний_інтерфейс*

```
R1#show ip route
Codes: C – connected, S – static, I- IGRP, R – RIP, M – mobile, B – BGP, D – EIGRP, EX – EIGRP external, O – OSPF, IA – SPF inter area, N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2, E2 – OSPF external type 2, E – EGP, I – IS-IS, L1  IS-IS level-1, L2 – ISIS level-2, ia – IS-IS inter area, P- periodic downloaded static route
Gateway of last resort is not set
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0/0
R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04,Serial0/0/0
R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04,Serial0/0/0
R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04,Serial0/0/0
R1#
```

Команда `show ip protocols` використовується для перегляду інформації про протокол та процеси маршрутизації і дозволяє перевірити більшість параметрів протоколу RIP, а саме:

- налаштований протокол маршрутизації;
- часові параметри протоколу;
- інтерфейси, які беруть участь у розсиланні та отриманні обновлень;
- IP-адреси мереж, які рекламує маршрутизатор;
- IP-адреси сусідніх маршрутизаторів, через які можна потрапити до відділених мереж;
- значення адміністративної відстані.

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
```

```
  Interface Send Recv Triggered RIP Key-chain
  FastEthernet0/0 1 2 1
  Serial0/0/0 1 2 1
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
  192.168.1.0
  192.168.2.0
  Passive Interface(s):
  Routing Information Sources:
  Gateway Distance Last Update
  192.168.2.2 120
  Distance: (default is 120)
  R1#
```

Результат виконання команди показав, що на маршрутизаторі R1 налаштовано протокол маршрутизації RIP, R1 надсилає й отримує обновлення через інтерфейси FastEthernet0/0 та Serial0/0/0, повідомляє про власні мережі 192.168.1.0 та 192.168.2.0 і має одне джерело інформації про маршрути (`Gateway Distance Last Update 192.168.2.2 120`), тобто інтерфейс S0/0/0 машрутизатора R2, а 120 свідчить про те, що інформація отримана від джерела, на якому також налаштовано протокол RIP).

Для того, щоб переглянути процес відправлення/отримання обновлень у реальному часі, використовується команда **`debug ip rip`.** Результат виконання команди може з’явитися не одразу, адже RIP-повідомлення надходять кожні 30 секунд.

```
  R1#debug ip rip
  R1#RIP: received v1 update from 192.168.2.2 on Serial0/0/0
  192.168.3.0 in 1 hops
  192.168.4.0 in 1 hops
  192.168.5.0 in 2 hops
  RIP: sending v1 update to 255.255.255.255 via
FastEthernet0/0 (192.168.1.1)
  RIP: build update entries
  network 192.168.2.0 metric 1
  network 192.168.3.0 metric 2
  network 192.168.4.0 metric 2
  network 192.168.5.0 metric 3
  RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
(192.168.2.1)
  RIP: build update entries
  network 192.168.1.0 metric 1
```

Зверніть увагу на те, що надсилання всіх повідомлень-обновлень виконується за широкомовною адресою 255.255.255.255.

Вивід команди **debug** показав, що R1 отримує обновлення від R2. Це обновлення містить мережі, які не під'єднані до маршрутизатора R1. Незважаючи на те, що інтерфейс FastEthernet0/0 не під'єднано до іншого маршрутизатора, він належить до мережі 192.168.1.0, налаштованої для роботи протоколу RIP, R1 створює обновлення і надсилає його через цей інтерфейс. Дане обновлення містить усі мережі, відомі для R1, окрім тієї, до якої належить інтерфейс Fa 0/0. При формуванні обновлення метрики відомих мереж збільшуються на одиницю.

Надсилання обновлень через локальний інтерфейс неефективно витрачає смугу пропускання та ресурси всіх пристроїв у даній локальній мережі. Крім того, широкомовна розсилка небезпечна, оскільки обновлення, які надходять у відкритому вигляді, можуть бути перехоплені програмою-сніфером. Це дозволить зловмиснику дізнатися інформацію про мережі та їх розташування в системі, а також модифікувати вміст обновлення та розповсюдити спотворену інформацію до маршрутизаторів, пошкоджуючи таблиці маршрутизації сусідів і метрики маршрутів, з метою перехоплення трафіка.

Для того, щоб уникнути зазначених проблем та ризиків, на перший погляд, можна було б не долучати відомості про локальну мережу, зокрема 10.1.0.0, до команди **network**, при налаштуванні протоколу RIP. Проте, в цьому випадку, інформація про цю мережу не повідомлялася б сусіднім шлюзам і не було б доступу до локальних мереж. Тому, аби заборонити надсилання обновлень через локальний інтерфейс, долучивши мережу, до якої він належить, до таблиці маршрутів і обновлень, використовується команда:

R1(config-router)# **passive-interface** *назва_інтерфейсу номер інтерфейсу*.

У режимі налаштування протоколу маршрутизації використовуйте команду в такий спосіб:

R1(config-router)#**passive-interface fastethernet 0/0**

І, нарешті, в останньому виводі команди `debug ip rip` R1 створює обновлення для сусіднього маршрутизатора R2. Завдяки правилу розщеплення обріїв, згідно з яким інформація про мережі може поширюватися лише в одному напрямку від джерела інформації, R1 долучає до обновлення інформацію про власну мережу 192.168.1.0.

Припинити процес відстеження роботи протоколу RIP у реальному часі можна за допомогою команди:

```
R1#undebug all
All possible debugging has been turned off
```

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета**: *організація з'єднання між усіма точками системи за допомогою налаштування динамічного протоколу маршрутизації RIP; перегляд конфігурації та роботи протоколу маршрутизації RIP, перевірка досяжності всіх вузлів мережі.*


Рис. 4.2. *Топологія мережі для налаштування протоколу маршрутизації RIP*

Таблиця 4.1

Параметри налаштування

| **Позначення пристрою** | **Ім'я пристрою** | **Інтерфейс** | **IP-адреса/маска** |
|---|---|---|---|
| Router1 | Moscow | Fa0/0 | 192.168.14.1/24 |
| | | S0/0/0 (DCE) | 192.168.15.1/24 |
| Router 2 | Kyiv | S0/0/0 (DTE) | 192.168.15.2/24 |
| | | Fa 0/0 | 192.168.16.1/24 |
| PC1 | | NIC | 192.168.14.2/24 |
| PC2 | | NIC | 192.168.16.2/24 |

**1. З'єднайте пристрої за наведеною схемою (рис. 4.2).**

**2. Налаштуйте параметри робочих станцій.**

**3. Налаштуйте параметри інтерфейсів обох маршрутизаторів.** Після налаштувань перегляньте стан інтерфейсів. *Яка команда для цього використовується?* Запустіть команду на виконання і збережіть її результат. При правильному з'єднанні та конфігурації задіяні інтерфейси повинні знаходитися у відкритому стані. Якщо ні, виявіть та усуньте причини.

**4. Перевірте з'єднання між усіма пристроями в мережі.** *Які проблеми виникли і чому? Перегляньте і збережіть вміст початкових таблиць маршрутизації для R1 і R2.*

**5. Налаштуйте роботу динамічного протоколу маршрутизації RIP у системі.**

**5.1. Наведіть адреси під'єднаних мереж для кожного маршрутизатора:**

R1:_____

R2:_____

**5.2. На кожному маршрутизаторі налаштуйте протокол маршрутизації RIP і вкажіть мережі, інформацію про які необхідно поширити по мережі.**

**6. Перевірте виконані налаштування маршрутизації RIP.**

**6.1. Перегляньте таблиці маршрутизації.** Порівняйте отримані дані з початковими таблицями маршрутизації.

*Для кожного маршрутизатора вкажіть у табл. 4.2 IP-адресу мережі, яка з'явилася, її метрику, адресу шлюз та власний інтерфейс, через який можна потрапити до віддаленої мережі.*

Якщо не всі з наявних мереж відображаються в таблиці маршрутизації, перевірте правильність налаштувань протоколу RIP, стан інтерфейсів і з'єднань.

Таблиця 4.2

| **Вихідний маршрутизатор** | **IP-адреса мережі** | **Метрика** | **Вихідний інтерфейс** | **IP-адреса шлюзу*** |
|---|---|---|---|---|
| R1 | | | | |
| R2 | | | | |

**6.2. Для перегляду інформації про процес маршрутизації використайте команду show ip protocols.**

Виконайте дану команду на маршрутизаторі та визначте параметри:

| | |
|---|---|
| Час надсилання періодичних обновлень | |
| Час до наступного обновлення | |
| Час, протягом якого маршрут є недійсним | |
| Час видалення маршруту з таблиці маршрутизації | |
| Інтерфейси, через які надходять обовлення | |
| Версія протоколу RIP для обновлень, які розсилаються надходять | |
| Адреса шлюзу | |
| Адміністративна відстань | |

**6.3. Перегляньте процес формування та розповсюдження обновлень протоколом RIP у реальному часі.** Наведіть результат виконання у звіті.

Припиніть перегляд у реальному часі.

***Контрольні запитання та завдання***

1. Назвіть основні характеристики дистанційно-векторних протоколів маршрутизації. Наведіть протоколи, що належать до цього класу.
2. Опишіть механізм обміну інформацією про маршрути, який використовується протоколом маршрутизації RIP.
3. Поясніть чому при налаштуванні протоколу RIP у команді **network** не вводять маски підмереж, а у таблиці маршрутизації відображаються класові маски?
4. За якими показниками у протоколі RIP обирається найкращий маршрут? Чи завжди такий маршрут можна вважати найкращим?
5. Як можна дізнатися, коли було отримано останнє обновлення від сусіда і коли очікувати наступний?
6. Яку проблему дозволяє розв’язати команда **passive-interface**? Як її використовують?
7. Виконання якої команди наведено на рис. 4.3? Які висновки про топологію мережі можна зробити з даного прикладу?

```
<output omitted>
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:012, Serial0/0/1
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:024, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
<output omitted>
```

Рис. 4.3

8. Що таке петлі маршрутизації? У результаті чого вони виникають і як можна запобігти їх виникненню?
9. Яка характеристика відображає рівень довіри до джерела інформації про маршрути? За допомогою яких команд її можна переглянути?
10. Окресліть переваги та недоліки протоколу маршрутизації RIP.

# V. ПРОТОКОЛ МАРШРУТИЗАЦІЇ СТАНУ КАНАЛУ OSPF

Якщо б у реальному житті для пошуку шляху використовувалися протоколи маршрутизації, то дистанційно-векторні протоколи використовували б для цього поради перехожих та дорожні знаки, які б давали приблизну інформацію лише про пункт призначення та напрямок руху. Натомість протоколи маршрутизації стану каналу дозволяли б використовувати карту, на якій можна було б побачити всі можливі шляхи та вибрати з них найбільш оптимальний.

Протокол маршрутизації OSPF(Open Shortest Path First) – це протокол стану каналу, який базується на відкритих стандартах і використовує у своїй роботі алгоритм пошуку найкоротшого шляху.

Якщо дистанційно-векторні протоколи маршрутизацій при визначенні оптимального шляху покладаються на інформацію, отриману від безпосередньо під'єднаних маршрутизаторів, то протоколи маршрутизації стану каналу збирають повну інформацію про існуючі мережі від усіх маршрутизаторів у межах автономної системи і кожен самостійно визначає найкращий шлях до кожної з існуючих мереж. Завдяки такому принципу роботи, протокол OSPF характеризується такими функціями:

- швидко реагує на зміни в мережі;
- обновлення надсилаються за груповою адресою лише в разі виникнення змін у топології;
- періодично розсилає повідомлення про стан каналу зв'язку;
- використовує механізм привітань для перевірки досяжності сусідніх маршрутизаторів;
- найкоротший шлях визначається за допомогою алгоритму SPF (Shortest Path First), який також називають Dijkstra за прізвищем засновника;
- маршрути характеризуються вартістю, яка складається з суми вартостей усіх з'єднань на шляху;
- використовує аутентифікацію в процесі обміну повідомленнями.

### *Інформація про стан каналу*

OSPF є ієрархічним протоколом маршрутизації з оголошенням стану про канал з'єднання (link-state). Він був спроектований як протокол роботи всередині автономної системи AS (Autonomous System), що являє собою групу маршрутизаторів і мереж, об'єднаних за ієрархічним принципом, які знаходяться під єдиним керуванням і спільно використовують загальну стратегію маршрутизації (рис. 5.1). Як транспортний протокол для маршрутизації в межах AS OSPF використовує IP-протокол.

Обмін інформацією про маршрути в одній AS протокол OSPF здійснює за допомогою обміну повідомленнями про стани каналу з'єднань між маршрутизаторами й мережами області (link-state advertisement – LSA). Ці

повідомлення передаються між об’єктами мережі, що знаходяться в межах автономної системи.

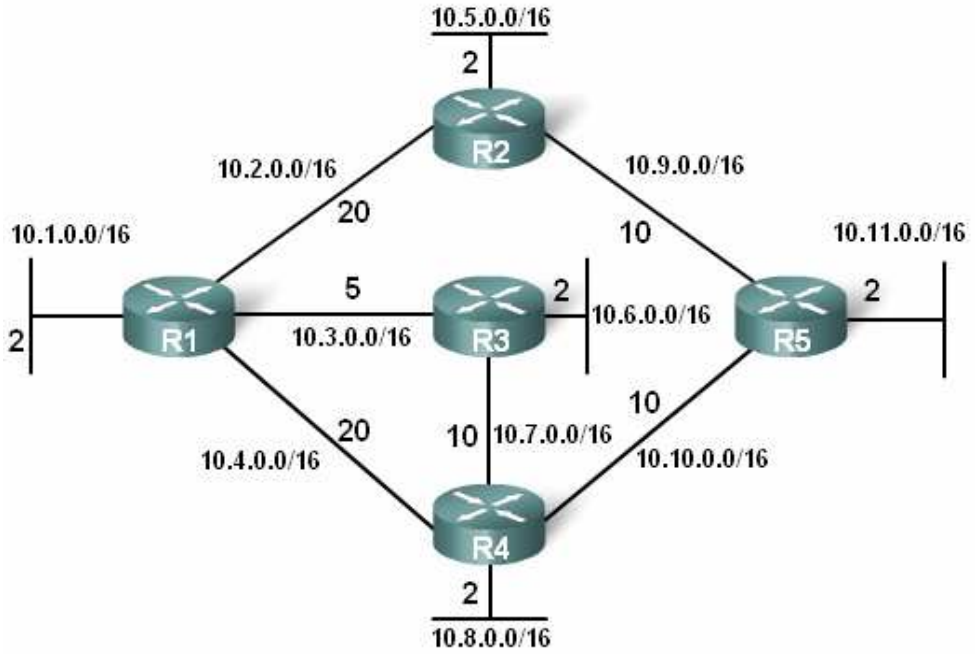



Рис. 5.1. *Приклад автономної системи, в якій використовується протокол маршрутизації OSPF. Кожен канал зв’язку характеризується вартістю*

У LSA-повідомлення протоколу OSPF включає таку інформацію:

- IP-адресу та мережну маску інтерфейсу;
- тип мережі з’єднання, зокрема Ethernet (широкомовна) або Serial (точка-точка);
- вартість з’єднання;
- ідентифікатори сусідніх маршрутизаторів з іншого боку з’єднання.

Маршрутизатор обробляє повідомлення про стан каналу й поширює його до всіх інших маршрутизаторі. Таким чином, після нетривалого процесу обміну інформацією на кожному маршрутизаторі формується топологічна база даних усіх існуючих з’єднань (табл. 5.1).

Таблиця 5.1

Схематичне подання топологічної бази даних АС (рис. 5.1)

| **R1** | **R2** | **R3** | **R4** | **R5** |
|---|---|---|---|---|
| R2/20 | R1/20 | R1/5 | R1/5 | R2/10 |
| R3/5 | R5/10 | R4/10 | R3/10 | R4/10 |
| R4/20 | | | R5/10 | |

На основі отриманої інформації про стан маршрутів, маршрутизатори розраховують найкоротший шлях до кожного сегмента мережі,

використовуючи алгоритм SPF. Причому розрахунок оптимального маршруту здійснюється динамічно відповідно до змін топології мережі. Найкращі маршрути заносяться до таблиці маршрутизації.

Так, для маршрутизатора R1 (рис. 5.1), :таблиця маршрутів матиме схематичний вигляд, наведений в табл.5.2.

Таблиця 5.2.

Таблиця маршрутів для маршрутизатора R1 (рис. 5.1)

| Мережа призначення | Найкоротший шлях | Вартість |
|---|---|---|
| R2 (10.5.0.0/16) | R1-R2 | 22 |
| R3 (10.6.0.0/16) | R1-R3 | 7 |
| R4 (10.8.0.0/16) | R1-R3-R4 | 17 |
| R5 (10.11.0.0/16) | R1-R3-R4-R5 | 27 |

Вартість маршруту OSPF визначається за сумою вартостей усіх з’єднань на шляху від даного маршрутизатора до мережі призначення.

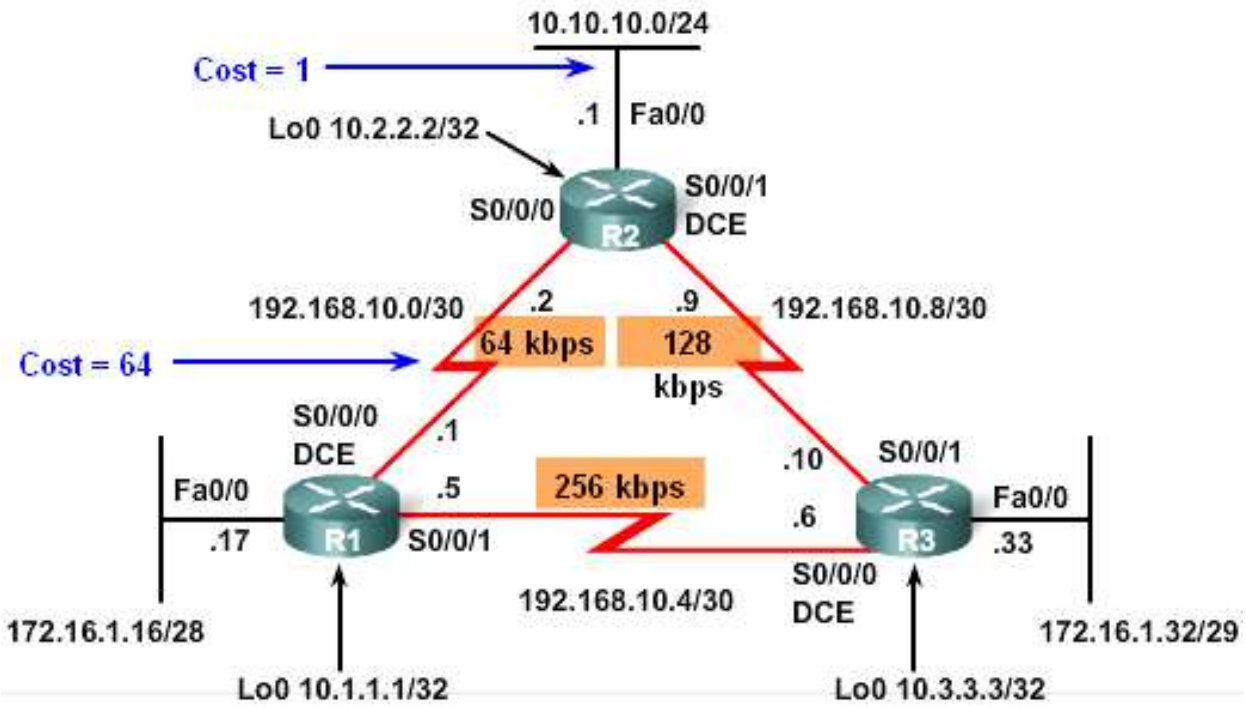



Рис. 5.2. *Топологія мережі з позначеннями вартості маршрутів*

Вартість з’єднання залежить від пропускної знатності інтерфейсу і визначається, як показано в табл. 5.3. Переглянути пропускну здатність інтерфейсу можна за допомогою команди **`show interface`** *назва номер*.

Наприклад, переглянемо фрагмент таблиці маршрутизації для R1, зображеного на рис. 5. 2:

```
R1# show ip route
Codes: C – connected, S – static, I- IGRP, R – RIP, M – mobile,
B – BGP, D – EIGRP, EX – EIGRP external, O – OSPF
<some output omitted>
O 10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:54,Serial0/0/0
```

Таблиця 5.3

Вартість з’єднання для інтерфейсів різних типів

| **Тип інтерфейсу** | **Вартість з’єднання $10^8$/(пропускна_здатність, біт/с)** |
|---|---|
| FastEthernet (100 Мбіт/с) | 1 |
| Ethernet (10 Мбіт/с) | 10 |
| E1 (2.05 Мбіт/с) | 48 |
| T1 (1.54 Мбіт/с) | 64 |
| 256 кбіт/с | 390 |
| 128 кбіт/с | 781 |
| 64 кбіт/с | 1562 |
| 56 кбіт/с | 1785 |

Сумарна вартість шляху від маршрутизатора R1 до мережі 10.10.10.0/24 маршрутизатора R2 дорівнює 65 (рис. 5.2): оскільки мережа 10.10.10.0/24 під’єднана до інтерфейсу FastEthernet, її вартість на R2 дорівнює 1, до якої R1 додає вартість послідовного з’єднання T1 (64) між маршрутизаторами R1 і R2.

***Налаштування OSPF***

OSPF активується в режимі глобальної конфігурації за допомогою команди **`router ospf`** *id-процесу*. Номер процесу – це число в діапазоні від 1 до 65535, яке обирається адміністратором і має локальне значення, тобто не повинно збігатися для всіх маршрутизаторів у АС, аби вони могли з’єднуватися між собою.

```
R1(config)#router ospf 1
R1(config-router)#
```

Далі, як і при налаштуванні дистанційно-векторних протоколів маршрутизації, використовується команда **`network`**, яка виконує звичні функції:

Будь-який інтерфейс маршрутизатора, який належить мережі, адреса якої зазначена в цій команді, буде брати участь у надсиланні й отриманні

OSPF-пакетів, а інформацію про саму мережу (або підмережу) буде долучено до повідомлень-обновлень.

Формат команди в режимі конфігурації маршрутизатора такий:

`Router(config-router)#`**`network`** *адреса_мережі шаблон_маски* **`area`** *номер_області*

У даній команді використовується комбінація мережної адреси і шаблона маски. Комбінація цих двох показників визначає діапазон інтерфейсів, на яких активується процес OSPF.

Шаблон маски – це інвертована мережна маска. Наприклад, для інтерфейсу FastEthernet 0/0 маршрутизатора R1 172.16.1.16 з мережною маскою /28 або 255.255.255.240, обернений шаблон маски можна визначити в такий спосіб:

```
  255.255.255.255
-
  255.255.255.240 (Віднімаємо мережну маску)
  ----------------
    0.  0.   0.  15  (Шаблон маски)
```

Номер області (або АС) визначає групу маршрутизаторів, які будуть обмінюватися інформацією про стани каналів та маршруту. Тому номер області для всіх маршрутизаторів у системі повинен бути однаковий. У наших налаштуваннях номер області буде однаковий і дорівнюватиме 0.

***Визначення ID маршрутизатора***

Кожен маршрутизатор у OSPF-системі має свій ідентифікатор, який визначається за трьома критеріями в такій послідовності:

1. Використовується IP-адреса, яка налаштовується за допомогою команди **`router-id`**.

Синтаксис команди:

`Router(config)#`**`router ospf`** *id-процесу*

`Router(config-router)#`**`router-id`** *IP-адреса*

2. Якщо **`router-id`** не налаштовано, маршрутизатор вирізняється за найвищою IP-адресою інтерфейсу **`loopback`**.

Адреса зворотної петлі (loopback) – це віртуальний інтерфейс, який переходить у відкритий стан одразу після налаштування. Команди для налаштування:

```
Router(config)#interface loopback номер
Router(config-if)#ip address IP-адреса мережна_маска
```

У загальному, налаштування подібні до конфігурації фізичного інтерфейсу, проте не потрібно використовувати команду no shutdown і як мережна маска використовується 255.255.255.255, що позначає мережу, яка складається з одного хоста. Перевагою інтерфейсу зворотної петлі є те, що він ніколи не відмовить фізично, а отже, забезпечить стабільність процесу OSPF.

3. Якщо два попередні параметри відсутні, як ідентифікатор маршрутизатора обирається найвища активна IP-адреса, серед налаштованих на фізичних інтерфейсів.

*Погляньте на схему і визначте ідентифікатор для кожного маршрутизатора.*

Для перевірки ID маршрутизатора використовується команда **`show ip protocols`**.

***Особливості роботи протоколу OSPF у широкомовній мережі***

Для поширення інформації маршрутизатори, на яких активовано протокол OSPF, намагаються встановити суміжність між собою. Спосіб, у який це відбувається, залежить і від типу мережі. Зокрема, інтерфейси, які беруть участь у OSPF-процесі, найчастіше належать до двох типів мереж:

1. Широкомовна багаторазового доступу (Ethernet): кілька маршрутизаторів може бути під'єднано до одного мережного сегмента і з кожним із них потрібно установити суміжність. Якщо кількість під'єднаних маршрутизаторів дорівнює n, необхідно утворити n*(n-1)/2 суміжностей.
2. Точка-точка (послідовне WAN-з'єднання, HDLC, PPP): два безпосередньо з'єднані маршрутизатори.

З метою зменшення надлишкових повідомлень, які генеруються при утворенні суміжностей, у широкомовних мережах обирають головний маршрутизатор (**Designated Router, DR**), який стає суміжним з усіма іншими маршрутизаторами сегмента. DR надсилає інформацію про стан каналу до інших маршрутизаторів за груповою адресою 224.0.0.5 і отримує від них інформацією за іншою груповою адресою 224.0.0.6. DR обирається всіма учасниками процесу маршрутизації і ним стає маршрутизатор з найвищим ідентифікатором. Оскільки визначений маршрутизатор є головною точкою ураження мережі, також обирається його замісник –

запасний визначений маршрутизатор (**Backup Designated Router, BDR**), маршрутизатор з другим найбільшим ID.

*Погляньте на рис. 5.3 і визначте, які ролі виконуватимуть маршрутизатори в цій системі.*

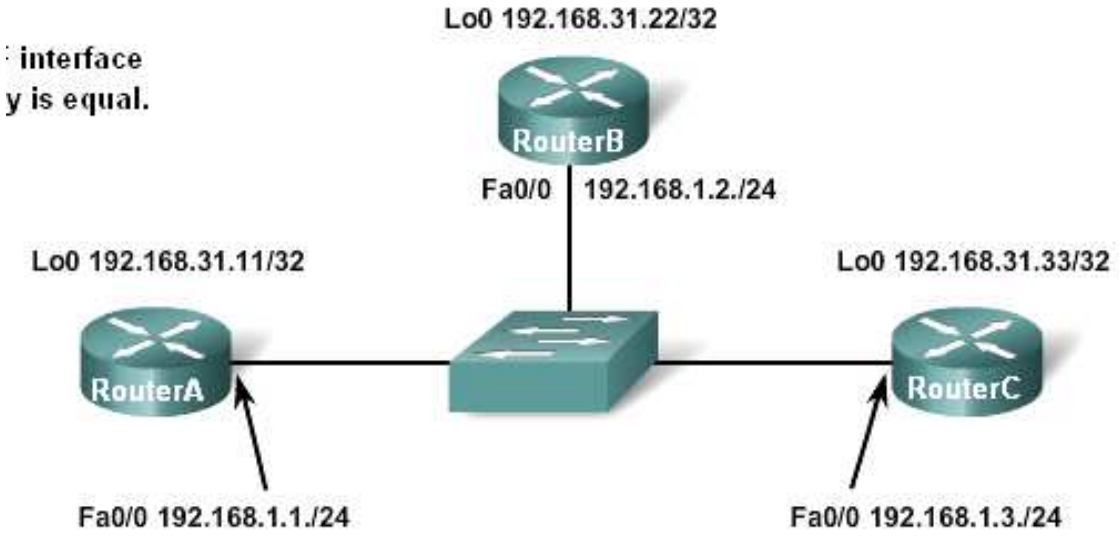



Рис. 5.3. *Приклад широкомовної мережі з багаторазовим доступом*

Переглянути результати виборів головного і запасного маршрутизаторів на широкомовному сегментів можна за допомогою команди **`show ip ospf interface fastethernet`** *номер*.

Через те, що визначений маршрутизатор є центральною точкою широкомовної мережі й відповідає за обробку та надсилання повідомлень, цей маршрутизатор повинен володіти потужним ЦП і достатнім обсягом пам’яті для виконання своїх функцій. Часто можна за допомогою налаштувань визначити маршрутизатори, які найкраще виконуватимуть ролі DR і BDR завдяки своїм апаратним характеристикам. Для цього потрібно змінити пріоритет маршрутизатора, використавши в режимі конфігурації інтерфейсу команду **`ip ospf priority interface`**.

```
Router(config-if)#ip ospf priority {0 - 255}
```

За замовчуванням, пріоритет OSPF інтерфейсів маршрутизатора однаковий і дорівнює 1. Отже, ідентифікатор маршрутизатора визначає обрання DR і BDR. Проте, якщо збільшити значення пріоритету, перемогу одержить маршрутизатор з найвищим пріоритетом.

***Перевірка роботи протоколу OSPF***

Для перевірки роботи протоколу OSPF використовуються такі команди:

- **`show ip ospf neighbor`**;
- **`show ip protocols`**;
- **`show ip ospf`**;
- **`show ip ospf interface`**.

Команду **`show ip ospf neighbor`** використовують для перевірки стану «сусідських взаємин» між OSPF-маршрутизаторами. Для кожного безпосередньо під'єднаного маршрутизатора можна переглянути таку інформацію:

- ID маршрутизатора;
- OSPF пріоритет з'єднувального інтерфейсу;
- стан інтерфейсу стосовно роботи протоколу OSPF. Стан FULL означає, що маршрутизатор і його сусіди мають однакові бази даних про стан каналів;
- час Dead Time – інтервал, протягом якого маршрутизатор очікує на отримання привітання від сусіднього маршрутизатора, перш ніж оголосити його недосяжним;
- адреса – IP-адреса сусіднього безпосередньо з'єднаного інтерфейсу.
- інтерфейс – порт, через який даний маршрутизатор встановив суміжність із сусідом.

Команда **`show ip protocols`** дозволяє переглянути необхідну інформацію про налаштування протоколу OSPF, зокрема ID OSPF-процесу, ID маршрутизатора, мережі, які рекламує маршрутизатор, сусідів, від яких надходять обновлення, адміністративну відстань для OSPF.

За допомогою команди **`show ip ospf`** також можна переглянути ідентифікатори OSPF-процесу та маршрутизатора. Крім того, ця команда відображає інформацію про АС, а також час останнього обчислення найкоротшого шляху за алгоритмом SPF.

Швидко одержати інформацію про інтервали вітання та відсутності відгуку можна використовуючи команду **`show ip ospf interface`**, після якої слід вказати назву та номер інтерфейсу. Для того щоб встановити суміжність, Hello- і Dead-інтервали на з'єднаних маршрутизаторах повинні збігатися. За замовчуванням вони становлять 10 с і 40 с відповідно. У разі відсутності зв'язку між двома сусідніми маршрутизаторами слід використовувати дану команду для перевірки ідентичності таймерів.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *налаштування протоколу OSPF для заданої топології в AC area 0, перегляді параметрів його роботи та перевірка досяжність усіх пристроїв системи.*

На рис. 5.4 наведено схему з'єднання пристроїв, а в таблиці 5.4 – параметри налаштування.

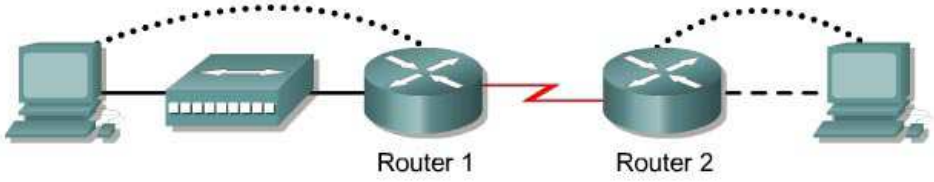



Рис. 5.4. *Тестова топологія та параметри для налаштування протоколу OSPF*

Таблиця 5.4

Параметри налаштування протоколу OSPF (рис. 5.4)

| **Позначення** | **Ім'я** | **Адреса інтерфейсу FastEthernet** | **Адреса інтерфейсу Serial** | **Тип інтерфейсу Serial** |
|---|---|---|---|---|
| Router 1 | Berlin | 192.168.1.129 /26 | 192.168.15.1 /30 | DCE |
| Router 2 | Rome | 192.168.0.1 /24 | 192.168.15.2 /30 | DTE |

### 1. Базові налаштування маршрутизаторів

З'єднайте пристрої за вказаною схемою (рис. 5.4). На маршрутизаторах у режимі глобальної конфігурації налаштуйте імена та параметри інтерфейсів згідно з таблицею 5.4.

### 2. Налаштування параметрів робочих станцій

Параметри для налаштування робочої станції:

а) під'єднаної до маршрутизатора Rome:
IP-адреса: 192.168.0.2
Мережна маска: _____
IP-адреса шлюза: _____

б) під'єднаної до маршрутизатора Berlin:
IP-адреса: 192.168.1.130
Мережна маска:_____
IP-адреса шлюза: _____

*Мережну маску та IP-адресу шлюзу визначіть самостійно на основі конфігураційних параметрів маршрутизаторів (табл. 5.4).*

**3. Перевірка налаштувань маршрутизаторів**

У привілейованому режимі:

а) перевірте поточну конфігурацію;

б) перегляньте коротку інформацію про інтерфейси; *наведіть результат перевірки; вкажіть, у якому стані знаходяться під'єднані інтерфейси;*

в) перевірте наявність зв'язку між усіма точками мережі в обох напрямках; *зазначте, який результат перевірки і чим він пояснюється;*

г) перегляньте і збережіть таблиці маршрутів для обох маршрутизаторів.

**4. Налаштування протоколу маршрутизації OSPF на маршрутизаторах**

Налаштуйте процес маршрутизації OSPF на маршрутизаторах, використавши при цьому номер процесу 1 та номер області 0.

Зауважимо, що для успішного обміну даними, на маршрутизаторах встановлюється однаковий номер АС (**area 0**), а в команді **network** окрім звичної IP-адреси мережі, яка братиме участь в OSPF-процесі маршрутизації (для кожної мережі – окрема команда **`network`**), слід вказати шаблон маски.

*Для кожного маршрутизатора вкажіть адреси мереж, і відповідні їм шаблони масок, які будуть налаштовані в команді* ***`network`***.

**5. Після виконання налаштувань на всіх маршрутизаторах у системі, перегляньте та збережіть їх таблиці маршрутизації.**

*Як у таблиці маршрутизації позначаються маршрути OSPF?*

*Яка адміністративна відстань та метрика для OSPF-маршрутів?*

*Яка пропускна здатність послідовних інтерфейсів? Чи узгоджується величина метрики з відповідним розрахунковим параметром?*

*Визначте та запишіть ідентифікатори кожного маршрутизатора.*

*Перегляньте і збережіть таблиці сусідів.*

**6. Перевірте досяжність між крайніми точками мережі.**

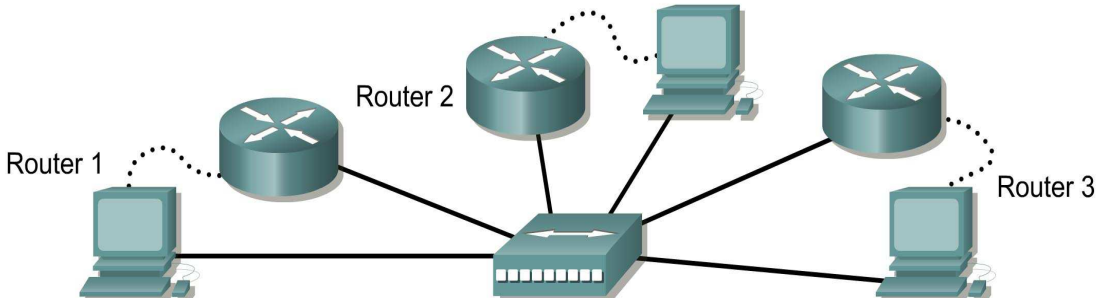
***Контрольні запитання та завдання***

1. Порівняйте основні характеристики протоколів маршрутизації: дистанційно-векторних і стану каналу.

2. Які параметри необхідно налаштувати для успішного OSPF-процесу маршрутизації?

3. Що таке loopback-інтерфейс? Яке його призначення?

4. На рис. 5.5 зображено схему з'єднання та параметри маршрутизаторів.




*Параметри інтерфейсів маршрутизаторів*

| Позначення марш-ра | Адреса /маска інтерфейсу FastEthernet | Адреса /маска інтерфейсу loopback |
|---|---|---|
| Router 1 | 192.168.1.30./24 | 192.168.31.11/32 |
| Router2 | 192.168.1.2 /24 | 192.168.31.22/32 |
| Router3 | 192.168.1.1/24 | 192.168.31.33/32 |

Рис. 5.5

На основі наведених даних визначте, який маршрутизатор займатиме визначну позицію (DR). Що станеться в разі його відмови?

5. Які характеристики з'єднання враховуються протоколом OSPF при обчисленні метрики?

6. Визначте шаблон маски для мережі 172.16.32.128/26.

7. Що таке ідентифікатор маршрутизатора і як він використовується протоколом OSPF?

8. Для трьох маршрутизаторів у широкомовній системі налаштовано такі параметри:

**R1: Priority:** 1, **Loopback: Fa 0/0:**172.16.8.8, **S 0/0/0:**200.0.0.10
**R2: Priority:** 1, **Loopback: Fa 0/0:**172.16.8.2, **S 0/0/0:**203.0.0.3
**R3: Priority:** 2, **Loopback: Fa 0/0:**172.16.8.1, **S 0/0/0:**202.0.0.2

Визначте ID для кожного маршрутизатора і роль, яку він виконуватиме.

# VI. СПИСКИ УПРАВЛІННЯ ДОСТУПОМ

Списки управління доступом (*Access Control List, ACL*) – це набір інструкцій, які застосовуються до інтерфейсу маршрутизатора і вказують, які пакети слід приймати, а які відкидати. Рішення про це може базуватися на таких критеріях, як адреса відправника, адреса одержувача, номер порту та протокол.

***Фільтрація даних***

Для кожного протоколу, який використовується на інтерфейсі маршрутизатора, може бути створений список управління доступом, який регулюватиме проходження потоку даних для цього протоколу. В деяких протоколах списки управління доступом називаються *фільтрами.* Наприклад, якщо інтерфейс маршрутизатора сконфігурований для протоколів IP, AppleTalk і IPX, необхідно буде визначити три списки керування доступом.

Список керування доступом являє собою набір директив, які визначають:

а) як організований вхід на інтерфейси;

б) як проходить передача інформації через маршрутизатор;

в) як організовані вихідні інтерфейси маршрутизатора.

Директиви списків виконуються поступово. Якщо умова директиви виконана, то пакету буде дозволено або відмовлено в доступі.

Якщо пакет відповідає умові першої директиви і йому відмовлено в доступі, він відкидається і переміщається в бітову корзину (bit bucket). Його відповідність наступним умовам не перевіряється.

Якщо пакет не відповідає умові першої директиви, то він перевіряється на відповідність другій директиві зі списку. Якщо параметри пакета відповідають наступній умові, яка являє собою директиву надання доступу, то йому дозволяється відправка на інтерфейс одержувача. Другий пакет не відповідає умовам першої директиви, але задовольняє умови наступного і йому також дається дозвіл на відправку.

Щойно умова виконана, над пакетом виконуються дії, передбачені директивою (відкинути або пропустити), а твердження, які стоять нижче по списку, не перевіряються. Тому при створенні списку управління доступом важливий порядок розташування директив.

Розрізняють три основні типи списків управління доступом:

- стандартні;
- розширені;
- іменовані.

У стандартних списках управління доступом параметром пакета, який перевіряється, є адреса відправника (або мережі відправника).

В розширених ACL рішення про подальшу долю пакета може базуватися на таких його параметрах, як адреса відправника і отримувача, мережний або транспортний протокол, за яким виконується з'єднання, номер порту або назва протоколу прикладного рівня, дані від якого передаються в пакеті.

Кожен список управління доступом характеризується своїм індивідуальним номером з певного діапазону, який визначає тип списку та протокол, для якого він використовується (табл.. 6.1). Зокрема, номери в діапазоні від 1 до 99 зарезервовані для стандартного ACL IP-протоколу, а від 100 до 199 – для розширених списків. У версіях Cisco IOS або 11.2 і вище для позначення списку управління доступом замість номера дозволено також використовувати ім'я. Тому іменовані списки можуть бути як стандартними, так і розширеними і позначаються не номерами, а змістовними назвами.

Таблиця 6.1

Протоколи та їх допустимі діапазони номерів списків управління доступом

| **Протокол** | **Діапазон змін номерів списків управління доступом** |
|---|---|
| Стандартний IP | 1 – 99 |
| Розширений IP | 100 – 199 |
| Apple Talk | 600 – 699 |
| IPX | 800 – 899 |
| Розширений IPX | 900 – 899 |
| IPX Service Advertising Protocol | 1000 - 1099 |

***Стандартні списки управління доступом***

Створення ACL відбувається у звичайному процесі установки глобальної конфігурації маршрутизатора.

Для фільтрації потоку даних за допомогою списків управління доступом необхідно виконати дві основні дії. Перша – створення списку, друга – застосування списку до конкретного інтерфейсу.

На першому етапі визначається список, використовуючи команду:

`Router(config)#` **`access-list`** *номер_списку* {**`permit`**|**`deny`**} *IP-адреса шаблон_маски*

Глобальна директива **`access-list`** визначає список управління доступом. Команда **`permit`** або **`deny`** в директиві вказує Cisco IOS дію над пакетами, які задовольняють задану умову.

На другому етапі ACL прив’язується до певного інтерфейсу, на якому буде виконуватися перевірка. Для застосування списку до одного з інтерфейсів, слід потрапити в режим його налаштування:

`Router(config) #`**`interface`** *назва номер*

і використати команду **`access-group`** у форматі:

`Router(config-if)#` *протокол* **`access-group`** *номер_списку* **`in|out`**

Використовуйте команди для видалення списку управління доступом у цілому:

**`no access-list`** *номер_списку*

з інтерфейсу:

**`no ip access-group`** *номер_списку*

***Шаблон маски***

Шаблон маски – це 32-бітова величина, яка розділена на чотири октета, кожен з яких складається з 8 бітів. Біт 0 шаблона маски означає, що цей біт повинен перевірятись, якщо ж біт дорівнює 1, це означає, що умова для нього перевірятися не буде (рис. 6.1).


Рис. 6.1. *Використання шаблону маски для обрання одного або кількох IP-адрес для виконання перевірки на дозвіл доступу або відмову в доступі*

Шаблон маски використовується для виокремлення або групування однієї або кількох адрес, які перевіряються на відповідність умовам дозволу або блокування.

Хоча шаблон маски списків управління доступом і маска підмережі є 32-бітовими величинами, функції, які вони виконують, суттєво відрізняються.

Нулі й одиниці в масці підмережі визначають біти, які позначають номер мережі, підмережі (одиниці), а які – частину хостів (нулі).

Тоді як у шаблоні маски нулі та одиниці вказують списку управління доступом, значення яких бітів в IP-адресі, що перевіряються, повинні збігатися зі значенням бітів IP-адреси, заданої в умові перевірки, а які неважливі. На рис. 6.1 показано процес застосування шаблону маски.

Припустимо, що необхідно перевірити IP-адресу для підмережі 172.30.16.0, доступ якій може надаватися або блокуватися. Ця адреса належить до класу B, тобто перші два октети позначають номер мережі, а третій октет призначений для номера підмережі. Шаблон маски – 0.0.0.255. Якщо потрібно дозволити доступ всім пакетам з номерами підмережі від 172.30.16.0 до 172.30.31.0, то слід використати шаблон маски, яка показана на рис. 6.2.

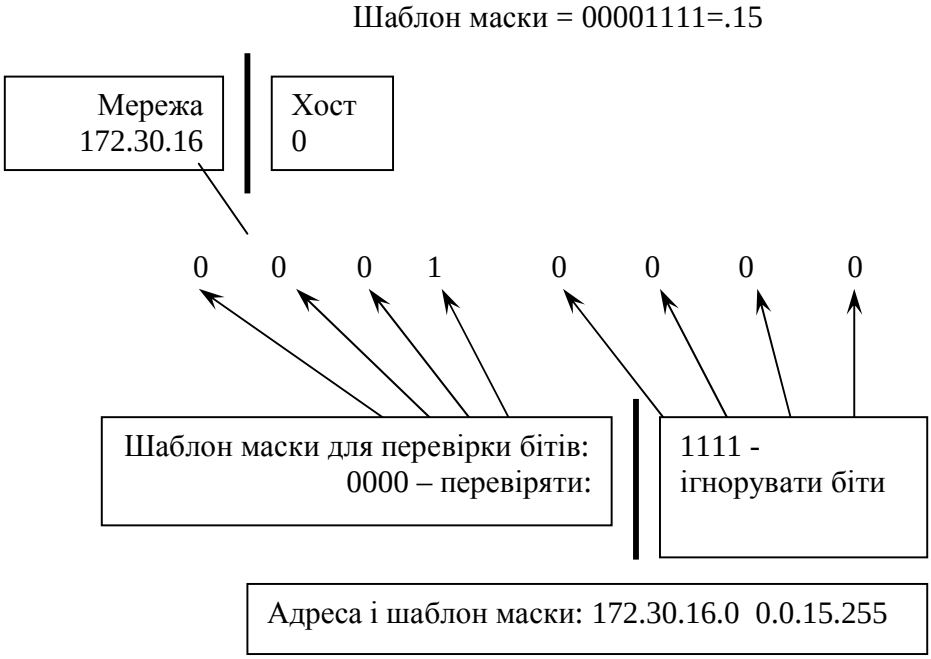



Рис. 6.2. *Адреса 172.30.16.0 з шаблоном маски 0.0.15.255 відповідає мережам з номерами від 172.30.16.0 до 172.30.31.0*

Спочатку з використанням нульових бітів шаблону маски перевіряються перші два октети (172.30), тобто відповідними будуть вважатися IP-адреси, які починаються з цих значень.

Оскільки адреси окремих хостів при перевірці неважливі, шаблон маски не враховує останній октет, а використовує в останньому октеті шаблону маски всі двійкові нулі.

У третьому октеті шаблон маски дорівнює 15 (00001111), а IP-адреса – 16 (00001000). Перші чотири нулі шаблону маски вказують маршрутизатору на необхідність перевірки перших чотирьох бітів IP-адреси (0001). Оскільки останні чотири біти не беруться до уваги, всі числа в інтервалі від 16 (00010000) до 31 (00011111) будуть задовольняти умову перевірки, бо всі вони починаються з 0001. У наведеному прикладі адреса 172.30.16.0/20 з маскою 0.0.15.255 відповідає адресам з номерами від 172.30.16.0 до 172.30.31.0. Інші підмережі не задовольняють умови маски.

Інколи замість шаблону маски можна використовувати ключові слова. Наприклад, якщо потрібно відкрити доступ для всіх номерів одержувачів, можна вказати IP-адресу 0.0.0.0 для зазначення того, що список управління доступом не повинен враховувати значення адрес (пропускати їх без перевірки), а для всіх бітів шаблону маски адрес встановити значення 1 (255.255.255.255). Для задання операційній системі Cisco цієї умови можна замість набору на клавіатурі 0.0.0.0 255.255.255.255 використовувати ключове слово **any**.

Наприклад, замість використання команди

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

можна ввести

```
Router (config) #access-list 1 permit any
```

Якщо необхідно керувати доступом конкретного хоста, кожен біт в адресі якого повинен підлягати перевірці, для створення директиви списку управління доступом потрібно повністю ввести його IP-адресу (наприклад, 172.30.16.29), а потім вказати, що список повинен перевірити всі біти адреси, тобто шаблон маски повинен складатися тільки з нулів (0.0.0.0). Цю ж умову можна записати з використанням ключового слова **host**:

```
Router (config) # access-list 1 permit 172.30.16.29 0.0.0.0
```

можна записати

```
Router (config) # access-list 1 permit host 172.30.16.29
```

Далі розглянемо налаштування стандартних списків управління доступом на прикладі мережі, зображеної на рис. 6.3.

*Приклад 6.1.* Дозволити передачу даних до сервера лише з мережі 172.16.0.0. Передача всіх інших даних заблокована.

Налаштування умови списку:

```
Router (config) #access-list 1 permit 172.16.0.0 0.0.255.255
```

Зауважимо, що згідно із цією умовою всім іншим вузлам буде відмовлено в доступі, оскільки в кінці стандартного списку за замовчуванням стоїть команда **deny any**.

Призначення створеного списку на інтерфейс:

```
Router (config) #interface ethernet 1
Router (config-if) #ip access-group 1 out
```

*Стандартні списки управління доступом завжди розміщуються якомога ближче до отримувача.*

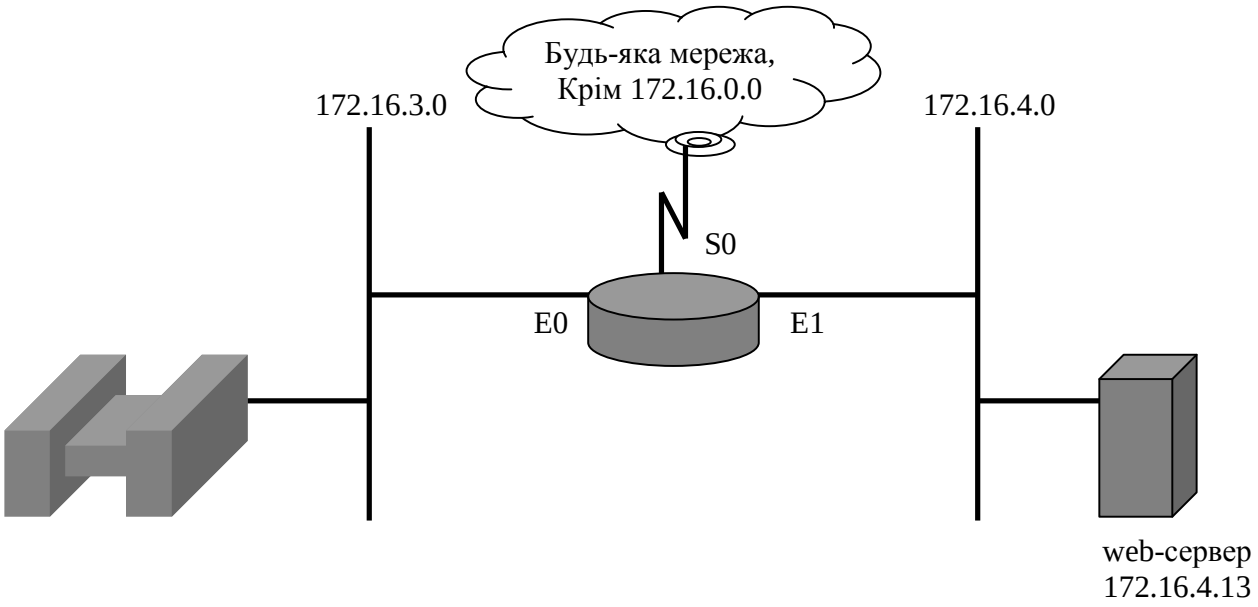



Рис. 6.3

*Приклад 6.2.* Відмовимо в доступі до мережі 172.16.3.0 web-серверу з мережною адресою 172.16.4.13 і дозволимо передачу даних від усіх інших хостів.

Перевірку вихідних пакетів потрібно виконувати на локальному інтерфейсі E0, з яким і буде пов’язано список за допомогою команди **ip access-group**, що створює групу списку на вихідному інтерфейсі.

При налаштування стандартного списку управління доступом потрібно заборонити доступ конкретному хосту з адресою 172.16.4.13, а всі інші пакети пропускати через Ethernet 0 в мережу 172.16.3.0. Перша команда у списку відмовляє в передачі вказаному хосту, використовуючи директиву **deny**. Шаблон маска 0.0.0.0 (замість якого можна використати слово **host**) вказує на необхідність перевірки всіх бітів IP-адреси.

Відмова в доступі конкретному хосту:

```
Router(config) #access-list 2 deny 172.16.4.13 0.0.0.0
```

У другій команді access-list комбінація 0.0.0.0 255.255.255.255 задає шаблон маски, яка пропускає пакети від будь-якого джерела. Вона також може бути записана з використанням ключового слова **any**.

```
Router (config) #access-list 2 permit 0.0.0.0 255.255.255.255
```

Призначення на інтерфейс:

```
Router (config-if) # interface ethernet 0
Router (config-if) # ip access-group 2 out
```

***Розширені списки управління доступом***

Розширені списки управління доступом (extended access control list, extended ACL) використовуються частіше за стандартні, оскільки вони забезпечують більші можливості контролю. Рекомендуються, наприклад, використовувати їх у тих випадках, коли потрібно дозволити передачу даних у World Wide Web і заблокувати протоколи FTP (File Transfer Protocol) або Telnet для використання їх мережами, які не належать компанії. Розширені списки перевіряють як адресу джерела, так і адресу одержувача. Вони можуть також перевіряти конкретні протоколи, номери портів та інші параметри. Це надає їм більшої гнучкості при створенні умов перевірки.

Формат команди access-list по створенню розширених списків має такий вигляд:

Router(config)# **access-list** *номер_списку* {**permit** | **deny**} *протокол IP-адреса_джерела шаблон_маски_джерела IP-адреса_отримувача шаблон_маски_отримувача* [*оператор операнд*], де

*номер_списку* вказує список, використовуються номери від 100 до 199.

**permit|deny** вказує на те, чи дозволяє дана позиція доступ до вказаної адреси.

*протокол*, зазначає тип застосованого протоколу, наприклад IP, TCP, UDP або ICMP.

*оператор* позначає типові операції порівняння lt (<), gt (>), eq (=), neq (<>) (менше ніж, більше ніж, рівне, не рівне) і номер порту.

*операнд* – це номер порту або скорочена назва протоколу, якому він відповідає (табл. 6.2).

Найбільш поширені зарезервовані номери портів, які використовуються для ідентифікації даних від різних протоколів прикладного рівня, й протоколи транспортного рівня, які забезпечують їх доставку, подані в табл. 6.2.

Таблиця 6.2

Зарезервовані номери портів

| **Десяткове число** | **Ключове слово** | **Описання** | **Протокол** |
|---|---|---|---|
| 20 | FTP-data | FTP (дані) | TCP |
| 21 | FTP | FTP | TCP |
| 23 | Telnet | Термінальне з’єднання | TCP |
| 25 | SMTP | SMTP | TCP |
| 53 | DOMAIN | DNS | TCP/UDP |
| 69 | TFTP | TFTP | UDP |
| 80 | HTTP | WWW | TCP |

Команда **`ip access-group`** зв’язує створений розширений список з вихідним або вхідним інтерфейсом. Слід звернути увагу на те, що кожному порту, протоколу та напрямку може відповідати тільки один список. Команда має такий формат:

`Router(config)#` **`ip access-group`** *номер_списку* {**`in`**|**`out`**}, де

*номер_списку* вказує номер списку управління доступом, який буде логічно зв’язаний з цим інтерфейсом;

**`in | out`** обирає, до яких пакетів даного інтерфейсу буде застосовуватись умова – вхідних чи вихідних. Якщо жодного параметра не зазначено, за замовчуванням приймається значення out.

*Приклад 6.3.* Заблокуємо доступ за протоколом FTP користувачам мережі 172.16.3.0 на інтерфейсі E0 (рис. 6.3).

Створюємо розширений список доступу для блокування протоколу FTP на інтерфейсі E0.

Для цього використовуємо такі команди:

```
Router(config)# access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 20
Router(config)#access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 21
!Дозволяємо доступ усім іншим:
Router(config)#access-list 101 permit ip any any
```

Дозволяємо доступ усім іншим

Застосуємо створений список управління доступом на інтерфейс E 0для перевірки вхідних даних:

```
Router(config)#interface e 0
Router(config-if)#ip access-group 101 in
```

*Приклад 6.4.* Налаштуємо розширений список доступу, який дозволяє звернення користувачам мережі 172.16.4.0 за протоколом електронної пошти SMTP тільки на інтерфейсі E0 і блокує решта потоків даних (рис. 6.3).

```
Router(config)#access-list 101 permit tcp 172.16.4.0 0.0.0.255 any eq 25
```

(неявно в кінці списку відмовляє в доступі всім іншим)

```
(access-list 101 deny ip 0.0.0.0 255.255.255.255)
Router(config)#interface e 0
Router(config-if)#ip access-group 101 out
```

### *Іменовані списки управління доступом*

Іменовані списки надають можливість звернення до стандартних і розширених списків управління доступом з допомогою символьних імен (набору символів з букв і цифр) замість номерів (від 1 до 199). Іменовані списки дозволяють видаляти зі списків окремі умови без необхідності попереднього видалення і повторного конфігурування цілого списку. До іменованого списку можна додавати й нові умови, які розміщуватимуться в кінці списку.

Для створення іменованого списку необхідно виконати команду:

`Router(config)#`**`ip access-list {standard|extended}`** ім'я

Далі, в режимі конфігурації `Router(config{std-|ext-}nacl)#` в залежності від типу списку, можна задавати одну або кілька умов надання або блокування доступу. Після створення, іменований список управління доступом застосовують на інтерфейсі маршрутизатора.

***Особливості використання списків управління доступом***

Оскільки в стандартних списках управління доступом рішення базується на адресі відправника, списки цього типу розміщуються на інтерфейсі якомога ближче до отримувача. Інакше б усі пакети відправника, на адресі якого базується директива, або повністю відкидалися, або одержували повний доступ незалежно від напрямку передачі.

Розширені списки управління доступом розміщуються найбільш наближено до відправника, оскільки вони базуються на адресі як відправника, так і отримувача і забезпечують більш гнучкий механізм керування потоками даних на основі не лише адрес, а й протоколів.

При потраплянні на інтерфейс рух пакета розглядається ніби зсередини маршрутизатора. Це слід враховувати в команді `access-group` при визначенні напрямку, в якому перевіряються пакети (**in** або **out**).

Список, який перевіряє вхідні пакети, не буде застосовуватися для вихідних пакетів з тими самими параметрами. Для кожного напрямку потрібно створювати окремий набір директив.

У кінці будь-якого списку управління доступом за замовчуванням стоїть директива **`deny any.`**

Директиви у списку управління доступом потрібно розміщувати в порядку від конкретних до загальних.

До списку, який уже призначено на інтерфейс, не можна додавати нові умови перевірки. Для цього потрібно видалити список і створити новий, додавши необхідні директиви. Виняток – іменовані списки, у яких нові умови долучаються в кінці списку.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *навчитися налаштовувати та застосовувати стандартні списки управління доступом для блокування або надання доступу трафіка від визначеного відправника.*

### 1. Базові налаштування маршрутизатора

З'єднайте пристрої за схемою, наведеною на рис. 6.4. На маршрутизаторі налаштуйте на під'єднаному локальному інтерфейсі відповідну адресу та маску (табл. 6.3). Переведіть інтерфейс у відкритий стан.

### 2. Налаштування робочих станцій Ethernet-сегмента

Для цього спочатку знайдіть і запишіть адресу підмережі, до якої належать робочі станції. Після цього визначте адреси 10-го і 15-го хостів у цій мережі. Наведіть одержані параметри у звіті. Налаштуйте відповідні адреси разом з маскою підмережі на комп'ютерах. *Яка адреса шлюзу для цих робочих станцій?*

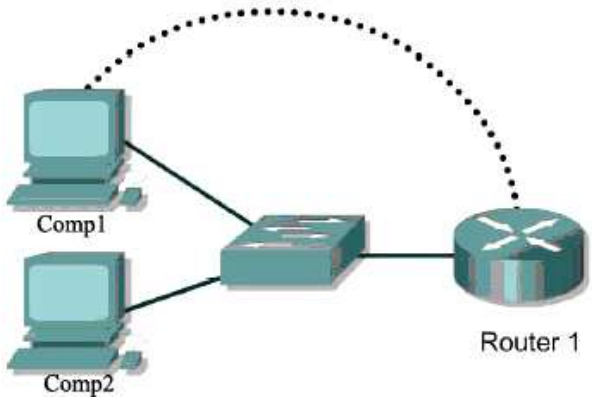



Рис. 6.4. *З'єднання пристроїв для налаштування стандартних списків управляння доступом*

Таблиця 6.3

Параметри налаштування

| **Позначення пристрою** | **Адреса інтерфейсу з'єднання** |
|---|---|
| Router 1 | 192.168.1.129 /26 |
| Comp1 | 10-та можлива адреса хоста |
| Comp2 | 15-та можлива адреса хоста |

### 3. Перевірка з'єднання

За допомогою команди **ping** протестуйте з'єднання між локальним інтерфейсом маршрутизатором і робочими станціями в обох напрямках. *Що показали результати перевірки?*

## 4. Налаштування стандартних списків управління доступом

**4.1.** Створіть стандартний список управління доступом з номером 1, який заборонить звернення до маршрутизатора робочої станції Comp1 (усім решта потрібно надати дозвіл).

*Запишіть умови списку управління доступом і налаштуйте його на маршрутизаторі.*

**4.2.** Призначте список на інтерфейс маршрутизатора. *Наведіть команду, яка виконує цю дію. В якому напрямку перевірятимуться пакети на відповідність умовам списку?*

**4.3.** Пропінгуйте маршрутизатор з хостів. *Який результат виконання команди ping і як його пояснити?*

**4.4.** Видаліть створений список. Перегляньте поточні налаштування аби переконатися в тому, що список більше не прив'язаний до локального інтерфейсу.

**4.5.** Створіть новий стандартний список управління доступом під номером 2, який заборонить звернення до маршрутизатора всіх користувачів локальної мережі.

*Запишіть умови списку управління доступом і налаштуйте його на маршрутизаторі. Який шаблон маски використовується?*

**4.6.** Призначте список на інтерфейс маршрутизатора. *Наведіть команду, яка виконує цю дію. В якому напрямку перевірятимуться пакети на відповідність умовам списку?*

**4.7.** Видаліть створений список управління доступом, попередньо зберігши його налаштування у звіті.

**4.8.** Створіть ще один список управління доступом, access-list 3, який би надавав дозвіл хостам із парними IP-адресами і не пропускав пакети від хостів з непарними номерами.

Для виконання цього завдання потрібно змінити шаблон маски. Для непарних номерів молодший біт четвертого октету дорівнює 1. Отже, його потрібно перевіряти при надходженні пакета. *Який вигляд при цьому матиме шаблон маски?*

Створіть команду налаштування за вказаною умовою і налаштуйте її на маршрутизаторі. *Чи потрібно додавати в кінці списку твердження* ***`permit any`***?

**4.9.** Застосуйте список доступу до відповідного інтерфейсу маршрутизатора.

**4.10.** Використайте команду ping для перевірки досяжності Ethernet-інтерфейсу маршрутизатора з кожної робочої станції. *Які результати тестування і чи досягнуто мету завдання 4.8*?

**5. Налаштування розширених списків управління доступом**

**5.1.** Видаліть створені списки управління доступом, попередньо зберігши команди налаштування у звіті.

**5.2.** Дозвольте доступ до маршрутизатора через web-браузер за протоколом http за допомогою команди в режимі глобальної конфігурації:

```
Router(config)#ip http server
```

**5.3.** Налаштуйте на маршрутизаторі пароль `enable secret` **connect** і пароль **acl** на віртуальних термінальних лініях.

**5.4.** Перевірте досяжність маршрутизатора, використавши з робочої станції команду ping з IP-адресою шлюзу (локального порту маршрутизатора). *Який результат виконання команди? Чи обидва вузли мають доступ до маршрутизатора? Якщо ні, перевірте чи всі списки управління доступом усунені.*

**5.5.** Зверніться за протоколом Telnet до маршрутизатора. *Яка команда для цього використовується? Чи успішний результат виконання команди? Які можливості надає користувачеві такий спосіб доступу до маршрутизатора?*

**5.6.** Зверніться до маршрутизатора з робочої станції через web-браузер, аби перевірити чи активована на маршрутизаторі функція web-серверу. *Який результат з'єднання? Чим відрізняється даний спосіб доступу від консольного режиму?*

**5.7.** Створіть розширений список управління доступом, який би заборонив вузлам мережі 192.168.1.129 /26 доступ до маршрутизатора за протоколами http і telnet. Призначте створений список до інтерфейсу. *Наведіть команди налаштування.*

**5.8.** *Як перевірити чи створений список вступив у дію? Які команди слід для цього використати? Який результат їх виконання?*

**5.9.** Використайте команду ping аби перевірити з'єднання з маршрутизатором. *Чи успішний результат виконання команди? Чи узгоджується він з результатами, отриманими в п. 5.9 та з виконаними налаштуваннями?*

**5.10.** Збережіть проведені налаштування та результати перевірок у текстовому документі для оформлення звіти.

**Видаліть створену конфігурацію на маршрутизаторі.**

***Контрольні запитання та завдання***

1. В чому призначення списків управління доступом і які їх типи?

2. Що таке шаблон маски? Як він визначається і для чого використовується?

3. Як у списках управління доступом задати умові для окремого хосту?

4. Що виконує створений розширений список управління доступом access-list 102 permit tcp 192.168.1.0 0.0.0.255 10.10.10.16 0.0.0.15 eq 80.

**5.** Створіть стандартний список управління доступом, який би дозволив доступ до мережі 10.1.1.0/30 лише користувачам сегмента 192.168.10.0/24 (рис. 6.5). Призначте створений список на відповідний інтерфейс.

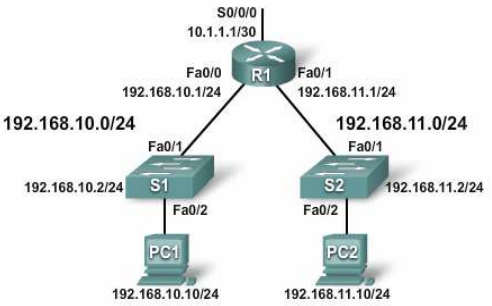



Рис. 6.5

6. Який шаблон маски слід використати для перевірки усіх хостів мережі з адресою 192.168.12.0/29:

а) 0.0.0.31; б) 0.0.0.30; в) 0.0.0.15; г) 0.0.0.8; д) 0.0.0.7; е) 0.0.0.3.

7. Які IP-адресу і шаблон маски слід було б вказати при створені списку управління доступом з п. 4.7, для надання доступу лише хостам з непарними номерами?

8. Створіть і застосуйте на інтерфейс список управління доступом, який би найбільш ефективно відсікав звернення за протоколом FTP до локальної мережі маршрутизатора R1 від користувачів сегмента 192.168.11.0/24 (рис. 6.6).

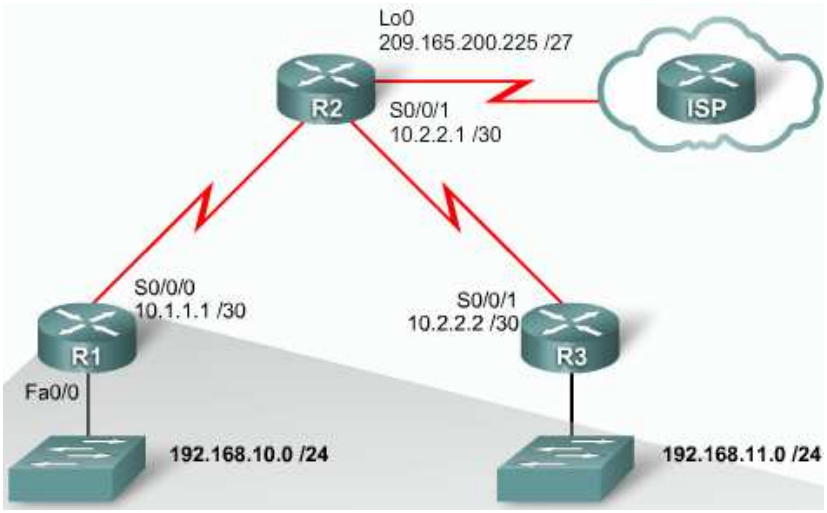



Рис. 6.6

# VII. ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ (VLAN)

За традиційною технологією Ethernet робочі станції об'єднуються в локальну мережу за допомогою багатопортових комутаторів 2-го рівня.

**Комутатор (switch)** – пристрій канального рівня, який об'єднує кінцеві пристрої в єдину локальну мережу та здійснює одночасний прийом і передачу даних на кожному зі своїх портів. Комутатор знижує перевантаженість мережі, зменшує мережний трафік та підвищує ефективну пропускну здатність мережі.

***Основи комутації***

У процесі роботи комутатора між приймачем і передавачем встановлюються *віртуальні зв'язки* – прямі виділені канали між портом, до якого під'єднаний відправник повідомлення та його отримувач. Процес встановлення таких зв'язків називають *мікросегментацією*. Самі зв'язки називаються віртуальними, оскільки вони встановлюються лише при потребі й на час передачі інформації, після чого одразу розриваються.

Згідно з алгоритмом роботи, комутатор на початку роботи мережі будує таблицю комутації, записуючи до неї MAC-адреси вузлів та власні номери портів, на які надійшла інформація (рис. 7.1). Далі на основі цієї таблиці він здійснює фільтрацію кадрів, тобто надсилає дані виключно адресату, якщо його MAC-адресу занесено до таблиці комутації. Інакше кадр розсилається на всі порти, окрім того, на який він надійшов.

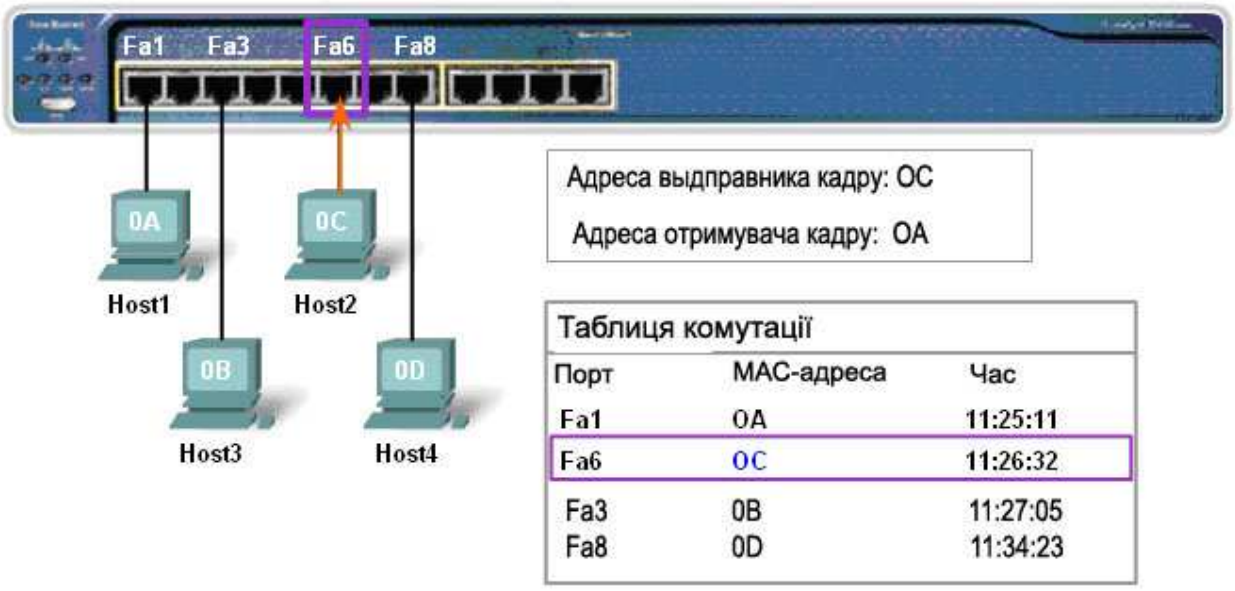



Рис. 7.1. *Схематичний вигляд таблиці комутації*

При використанні комутаторів у мережі не виникають колізії, оскільки *кожен порт комутатора з під'єднаним до нього вузлом є окремим фізичним сегментом.* Крім того, оскільки фільтрація кадрів здійснюється апаратно (на відміну від мостів, де для цього застосовуються програмні методи), комутатори забезпечують ще більшу швидкодію і як наслідок – більшу продуктивність роботи мережі.

Хоча комутатор дає можливість сегментувати велику мережу на менші домени колізій, він не створює бар'єри на шляху широкомовного трафіку.

***Віртуальні локальні мережі***

Проблема блокування небажаного трафіка розв'язувалася за допомогою побудови великої локальної мережі, яка складається з сегментів, об'єднаних за допомогою маршрутизаторів. Захисні властивості маршрутизатора пов'язані з тим, вони передають кадри з мережі в мережу тільки тоді, коли на цю необхідність явно вказує мережна адреса пакета, вкладеного в кадр канального протоколу. Усі кадри з широкомовними адресами не передаються маршрутизаторами за межі мережі, в якій вони виникли. Отже, виключаються всі ситуації, пов'язані з широкомовним штормом. Використання різноманітних фільтрів, які враховують інформацію третього і четвертого рівнів (IP-адреси, тип протоколу, зазначений у заголовку IP-пакета, номери портів TCP/UDP), перетворюють маршрутизатори в найпростіші брандмауери, що складають основу системи захисту багатьох мереж.

Проте комутатори внесли в рішення питання «об'єднання-роз'єднання» новий механізм – технологію віртуальних мереж *(Virtual LAN,* VLAN). З появою цієї технології відпала необхідність утворювати ізольовані сегменти фізичним шляхом — його замінив програмний спосіб, більш гнучкий і зручний.

*Віртуальною мережею (VLAN)* називається група вузлів мережі, потік даних якої, зокрема й широкомовний, на канальному рівні цілком ізольований від вузлів, які належать до інших віртуальних локальних мереж. Це означає, що передача кадрів між різними віртуальними сегментами на підставі адреси канального рівня неможлива, незалежно від типу адреси – унікальної, групової або широкомовної. Водночас усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки на той порт, який зв'язаний з адресою призначення кадру.

Віртуальні локальні мережі створюються програмно, а отже не вимагають заміни фізичної топології мережі чи доручення додаткового

обладнання (наприклад, маршрутизатора, який використовуються лише для передачі даних між різними VLAN). Завдяки цій технології, люди, які працюють в одному відділі не обов'язково повинні знаходитися в одному приміщенні для виконання своїх робочих обов'язків (рис. 7.2).

Розрізняють статичні й динамічна VLAN. До статичної VLAN долучають порти комутатора, незалежно від того, що до них під'єднано. Членство в динамічній VLAN досягається через MAC-адресу під'єднаного пристрою, незалежно від порту підключення.

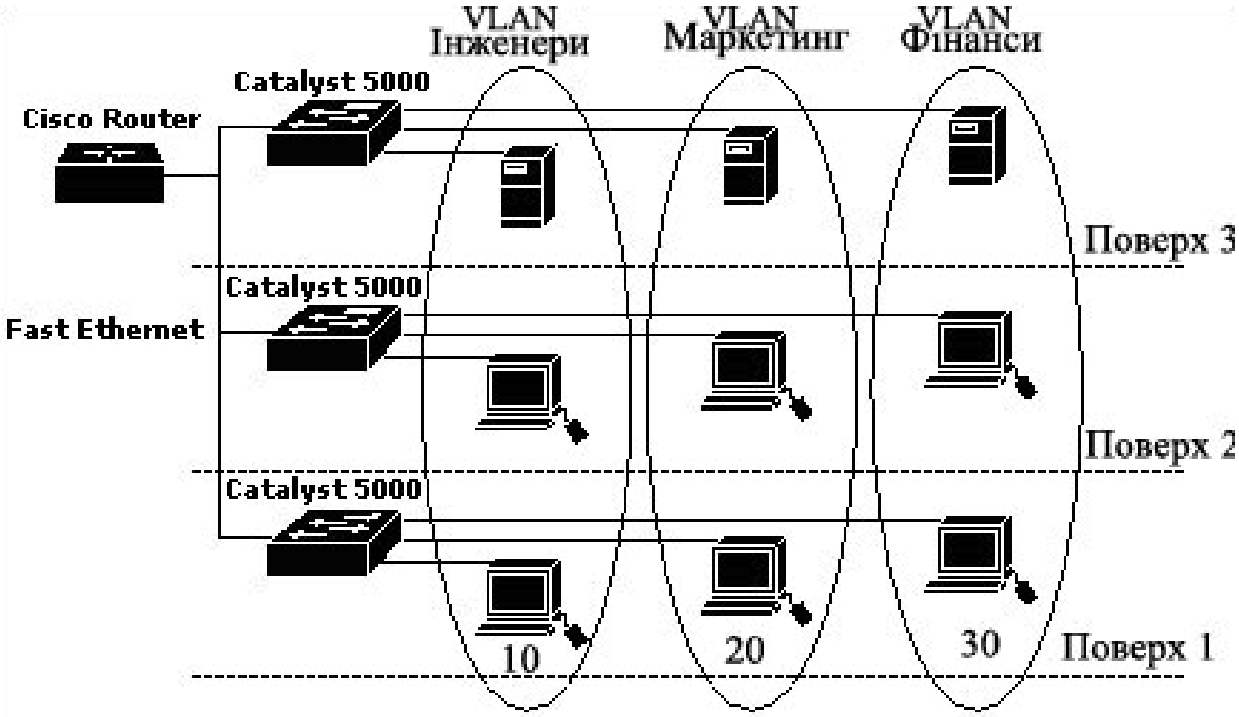



Рис. 7.2. *Використання віртуальних локальних мереж*

### *Особливості налаштування комутатора*

Комутатор за параметрами налаштування багато в чому подібний до звичайного ПК, адже на ньому потрібно налаштовувати IP-адресу, мережну маску та шлюз за замовчуванням. Ці параметри необхідні для здійснення віддаленого керування комутатором за допомогою TCP/IP. IP-адреса призначається віртуальному інтерфейсу, який за замовчуванням має назву VLAN 1. Цю віртуальну мережу називають управлінською. *Від початку всі порти комутатора належать одній VLAN – VLAN 1. Її неможливо видалити, але можна з метою безпеки змінити її номер.*


Рис. 7.3. *Топологія мережі для налаштування VLAN*

Для налаштування IP-адреси та мережної маски на управлінській VLAN комутатор, необхідно перейти в режим налаштування інтерфейсу. Це єдина віртуальна локальна мережа, до якої звертаються як до інтерфейсу мережного рівня.

Команди налаштування VLAN 1:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address IP-адреса маска
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Приклад налаштування:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.17.99.110 255.255.255.0
```

На комутаторі потрібно налаштувати IP-адресу шлюзу за замовчуванням (Default Gateway), до якого направляються IP-пакети, призначені назовні локальної мережі.

```
Switch(config)#ip default-gateway IP-адреса
```

На рис. 7.3 шлюзом є інтерфейс маршрутизатора f0/1 з адресою 172.17.99.1, до якого під’єднано комутатор S1.

Приклад налаштування адреси шлюзу за замовчуванням:

```
Switch(config)#ip default-gateway 1772.17.99.1
```

При налаштуванні нових VLAN для них потрібно вказати ID з визначеного діапазону та назву. Існує два діапазону номерів для VLAN:

- нормальний діапазон охоплює ID від 1 до 1001;
- розширений діапазон містить номери від 1006 до 4094.

Зарезервовані номери VLAN **-** 1, і від 1002 до 1005. Звичайно номери для нових віртуальних мереж обираються з нормального діапазону, при цьому деталі налаштування автоматично зберігаються до флеш-пам’яті до файла vlan.dat.

Створення статичних VLAN на комутаторі Cisco Catalyst можливе в режимі глобальної конфігурації у два різні способи:

1) у режимі налаштування бази даних віртуальних локальних мереж;
2) у режимі глобальної конфігурації комутатора.

Розглянемо приклади створення на комутаторі S1 нової VLAN з номером 20 і назвою Student (рис. 7.3).

За першим способом налаштування використовуються команди у форматі:

```
Switch# vlan database
Switch(vlan)# vlan номер name назва
Switch(vlan)#exit
```

Приклад налаштування:

```
Switch# vlan database
Switch(vlan)# vlan 20 name Student
Switch(vlan)#exit
```

Другий спосіб передбачає створення нової віртуальної локальної мережі безпосередньо в режимі глобальної конфігурації за допомогою команд:

```
Switch(config)# vlan номер
Switch(config-vlan)# name назва
Switch(config-vlan)#end
```

Приклад налаштування:

```
Switch(config)# vlan 20
Switch(config-vlan)# name Student
Switch(config-vlan)#end
```

Для перегляду повної інформації про базу даних VLAN, а отже, вмісту файла vlan.dat, у привілейованому режимі використовується команда **show vlan**, або **show vlan brief** для подання основних даних.

Після створення нових віртуальних локальних мереж потрібно призначити один або більше портів комутатора до VLAN. Такі порти називають статичними портами доступу (access ports). Один порт може належати лише одній VLAN.

Команди, які для цього використовуються:

```
Switch(config)# interface назва номер
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan номер
Switch(config-vlan)#end
```

Наприклад, долучимо до створеної VLAN 20 порт комутатора S1 fa 0/18, а разом із ним - під'єднаний комп'ютер PC1 (рис. 7.3).

```
S1(config)# interface fa 0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
```

`S1(config-vlan)#`**`end`**

Після проведених налаштувань VLAN і портів можна переглянути конфігурацію за допомогою команд:

- **`show vlan`** [**`brief`** | **`id`** *номер_vlan* | **`name`** *назва_vlan* | **`summery`**],

де квадратні дужки позначають, що параметр необов'язковий, а вертикальна риска – можливі варіанти.

**Параметри:**

**`brief`** відображає в одному рядку для кожної VLAN її назву, статус та порти.

**`id`** *номер_vlan* надає інформацію для VLAN з визначеним номером у діапазоні від 1 до 4094

**`name`** *назва_vlan* відображає інформацію про окрему VLAN з вказаною назвою. Ім'я VLAN може мати довжину від 1 до 32 символів ASCII.

**`summery`** виводить загальну інформацію про налаштовані віртуальні локальні мережі.

- **`show interfaces`** [*номер_порта* | **`vlan`** *номер_vlan* ] | **`switchport`**

**Параметри:**

**`vlan`** *номер_vlan* – відображає інформацію про управлінську VLAN

*номер_порта* **`switchport`** – відображає фізичні параметри порту, спосіб долучення та належність до VLAN

Для вилучення інтерфейсу з віртуальної локальної мережі використовується команда:

`Switch(config)#` **`interface`** *назва номер*

`Switch(config-if)#` **`no switchport access vlan`** номер

Для видалення цілої VLAN:

`Switch#` **`vlan database`**

`Switch(vlan)#` **`no vlan`** *номер*

Для видалення всієї бази VLAN:

`Switch#` **`delete flash:vlan.dat`**

***Магістральні лінії з'єднання***

Віртуальні локальні мережі логічно сегментують мережу й дозволяють підтримувати кілька IP-мереж або підмереж на одному комутаторі. Кінцеві пристрої в одній VLAN характеризуються однією адресою мережі та маскою. При цьому комп'ютери, які під'єднані до одного комутатора, але належать до різних VLAN, не зможуть з'єднуватися між собою. Взаємодія пристроїв у різних підмережах можлива лише за участі пристрою 3-го рівня (маршрутизатора).

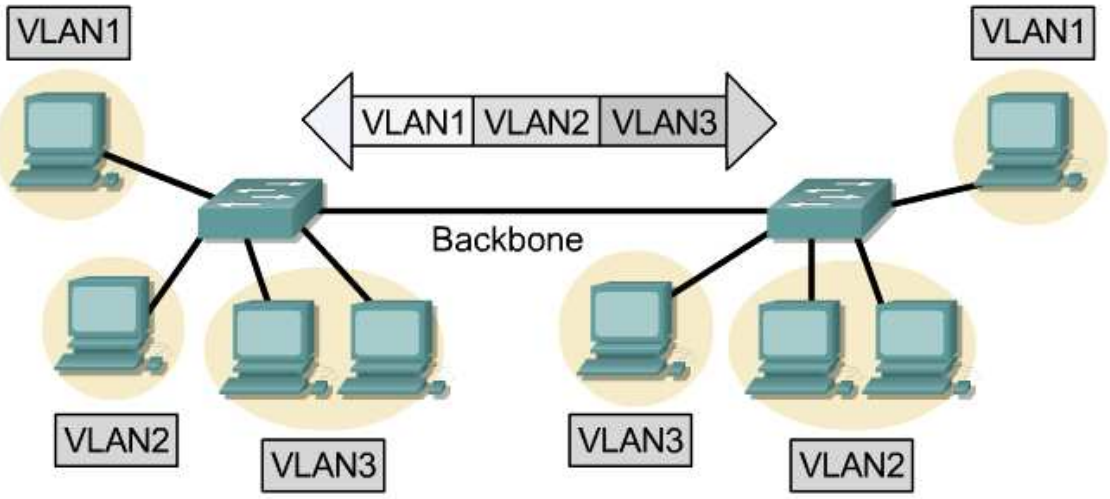



Рис. 7.4. *Передача даних від різних VLAN по одному каналу – магістралі*

**Магістраллю** (trunk, backbone) називається фізичне та логічне з'єднання між двома мережними пристроями, зокрема комутаторами, по якому здійснюється передача даних від різних VLAN (рис. 7.4). Призначення такого каналу – зекономити порти комутатора при встановленні зв'язку між двома пристроями, які працюють з VLAN.

**Магістральні протоколи** (trunking protocols) були спроектовані для того, щоб більш ефективно управляти передачею кадрів із різних VLAN по одному фізичному каналу.

На даний момент існує два механізми передачі кадрів магістральними каналами – фільтрація та ідентифікація кадрів.

Перш ніж передати кадр по магістральній лінії з'єднання, до його заголовку додають ідентифікатор VLAN, до якої він належить. Даний ідентифікатор обробляє кожен комутатором, перед тим як передати його до наступного комутатора, маршрутизатора, або робочої станції. При виході кадру з магістрального каналу кінцевий комутатор видаляє ідентифікатор і передає кадр до кінцевого вузла, якому він призначений. Ідентифікація кадрів була прийнята як стандартний механізм IEEE.

Існує дві найбільш поширені схеми забезпечення ідентифікації кадрів для Ethernet-сегментів:

- **802.1Q –** відкритий стандарт IEEE;
- **ISL (Inter-Switch Link protocol) –** протокол компанії Cisco.

Важливо розуміти, що магістральний канал не належить до жодної VLAN. Він призначений лише для перенесення інформації від інших VLAN між комутаторами та маршрутизаторами.

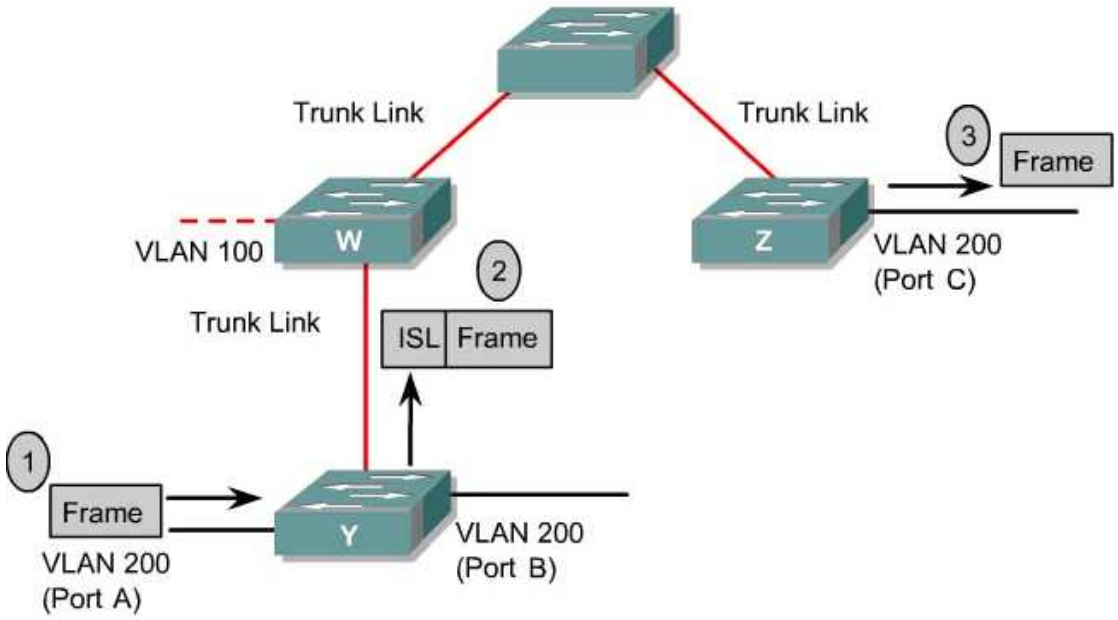



Рис. 7.5. *ISL-інкапсуляція*

ISL-протокол додає до Ethernet-кадрів спеціальний заголовок, який містить VLAN ID (рис. 7.5).

Головне, щоб з обох кінців магістрального з'єднання використовувався один і той самий спосіб ідентифікації (ISL або 802.1Q). Перший використовується на обладнанні фірми Cisco, тоді як стандарт IEEE підтримується багатьма виробниками мережного устаткування.

Для налаштувань магістрального порту використовуються команди:

```
Switch(config)# interface Fa номер
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport mode trunk encapsulation isl|dot1q
Switch(config-if)#exit,
```

де **dot1q** – позначення стандарту 802.1q. Для обох кінців магістрального з'єднання потрібно налаштувати однаковий спосіб ідентифікації.

***Маршрутизація між VLAN***

Для здійснення зв'язку між окремими VLAN слід використовувати маршрутизатор, як пристрій мережного рівня, до функцій якого належить з'єднання окремих мереж, у тому числі віртуальних.

Зазвичай, до кожного порту маршрутизатора можна під'єднати окрему мережу. У міру збільшення кількості VLAN, фізичний підхід призначення окремого інтерфейсу маршрутизатора на одну віртуальну локальну мережу стає неефективним (рис. 7.6). На комутаторі, що підтримує велику

кількість VLAN, потрібно налаштовувати один магістральний канал передачі даних, який під'єднується до єдиного порту маршрутизатора.

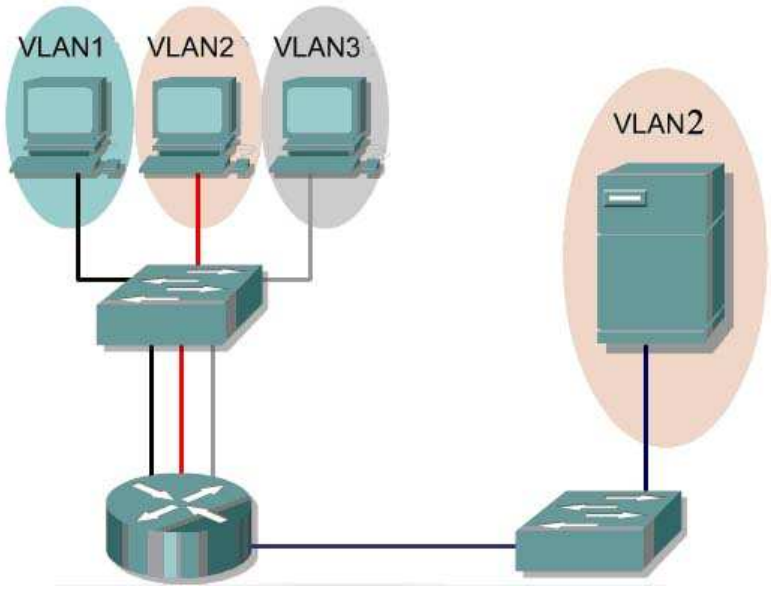



Рис. 7.6. *Маршрутизація між VLAN: фізичний підхід*

Для цього на основі фізичного порту маршрутизатора потрібно створити логічні підінтерфейси – по одному на кожну VLAN, як зображено на рис. 7.7. Головна перевага такого підходу – значне зменшення кількості використаних портів на комутаторі та маршрутизаторі. Це не лише економить витрати, але й зменшує обсяг необхідних налаштувань, а звільнені порти можна використати для подальшого розширення мережі.

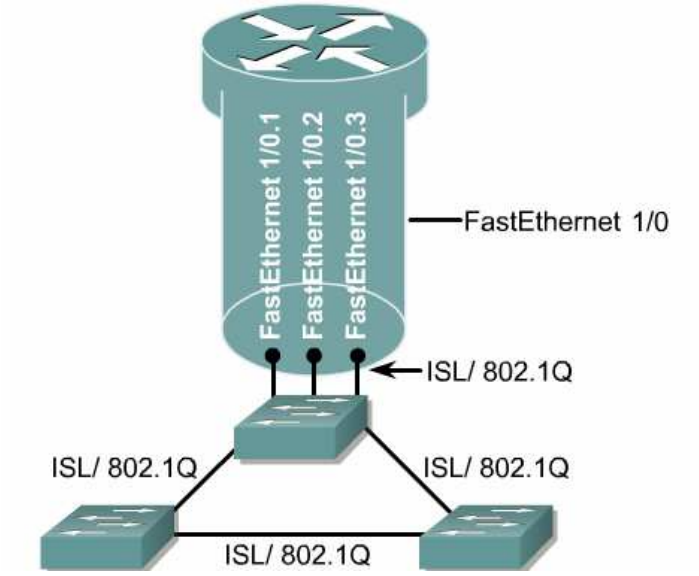



Рис. 7.7. *Маршрутизація між VLAN: логічний підхід*

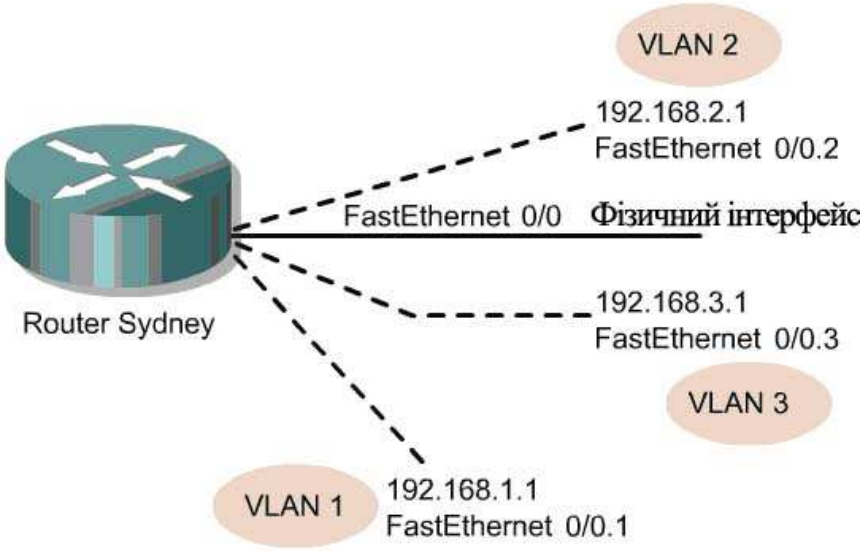



Рис. 7.8. *Створення підінтерфейсів*

Підінтерфейс – це логічний інтерфейс, створений на основі фізичного порту маршрутизатора, такого як Fast або Gigabit Ethernet. На одному фізичному інтерфейсі може існувати кілька логічних підінтерфейсів.

Щоб здійснювати передачу даних між різними VLAN, для кожної потрібно створити окремий підінтерфейс.

Кожен підінтерфейс підтримує одну VLAN і потребує окремої IP-адреси , яка належить тій самій мережі, що віртуальна локальна мережа.

Наприклад, якщо для користувачів VLAN 1 надано IP-адресу мережі 192.168.1.0, то пристрої, які їй належать, матимуть IP-адреси 192.168.1.2, 192.168.1.3, 192.1.1.4, в тому числі відповідний підінтерфейс Fa 0/0.1 **-** 192.168.1.1.

Аналогічно:

VLAN 2 – 192.168.2.0 , Fa 0/0.2 - 192.168.2.1;

VLAN 3 – 192.168.3.0, Fa 0/0.3- 192.168.3.1.

Для забезпечення маршрутизації між VLAN на з'єднаних маршрутизаторі та комутаторі слід виконати такі налаштування:

1. Порт комутатора, під'єднаний до маршрутизатор, налаштувати як магістральний і визначити тип інкапсуляції.
2. Створити під інтерфейси на порті маршрутизатора.

Для цього в режимі глобальної конфігурації використовується команда формату:

`Router(config)#` **`interface fa`** *номер_порту номер_підінтерфейсу*,

де номер порту – це фізичний інтерфейс, а номер підінтерфейсу позначає віртуальний інтерфейс.

3. Визначити спосіб інкапсуляції та приналежність до VLAN для підінтерфейсу.

Аби коректно обробляти дані, отримані від комутатора, маршрутизатор повинен підтримувати стандартизовані способи ідентифікації кадрів магістральної лінії з'єднання Тому для кожного підінтерфейсу слід налаштувати стандарт інкапсуляції VLAN за допомогою команди в режимі налаштування підінтерфейсу:

`Router(config-subif)# encapsulation dot1q` *номер-VLAN*,

де *номер_VLAN* **-** ідентифікатор віртуальної локальної мережі, для якої передаватимуться дані через створений підінтерфейс.

4. Призначити IP-адресу.

Як і для будь-якого фізичного інтерфейсу маршрутизатора, на підінтерфейсі слід налаштувати IP-адресу та маску:

`Router(config-subif)# ip address` *IP-адреса маска*

Зауважте, що для підінтерфейсів не потрібно задавати команду **no shutdown**. Для їх відкриття слід застосувати цю команду для всього фізичного інтерфейсу.

Для прикладу, зображеного на рис. 7.8, команди налаштування будуть такі:

```
Sydney(config)# interface Fa 0/0.1
Sydney(config-subif)# encapsulation dot1q 1
Sydney(config-subif)# ip address 192.168.1.1 255.255.255.0
Sydney(config-subif)#exit

Sydney(config)# interface Fa 0/0.2
Sydney(config-subif)# encapsulation dot1q 2
Sydney(config-subif)# ip address 192.168.2.1 255.255.255.0
Sydney(config-subif)#exit

Sydney(config)# interface Fa 0/0.3
Sydney(config-subif)# encapsulation dot1q 3
Sydney(config-subif)# ip address 192.168.3.1 255.255.255.0
Sydney(config-subif)#exit
```

Отже, VLAN є зручним програмним способом розмежування користувачів за функціями, які вони виконують, і створення захисних бар'єрів на шляху трафіка (в т.ч. широкомовного) з різних віртуальних локальних мереж.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *навчитися виконувати основні налаштування комутатора, визначати його апаратні параметри, створювати VLAN, налаштовувати лінії магістрального з'єднання та реалізовувати зв'язок між VLAN.*

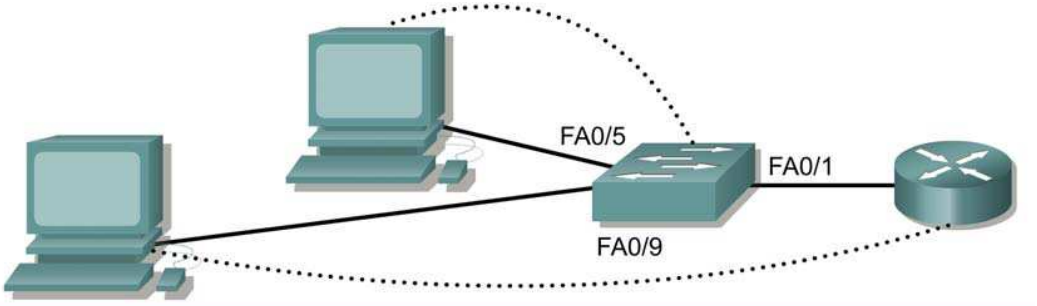



Рис. 7.9. *Схема мережі для налаштування VLAN*

Таблиця 7.1

Параметри налаштування комутатора

| **Параметри** | **Налаштування** |
|---|---|
| Назва комутатора | Switch_A |
| enable secret | pass |
| Пароль console, vty | cisco |
| Адреса VLAN 1 | 192.168.1.2 |
| Мережна маска | 255.255.255.0 |
| Параметри VLAN: | |
| VLAN 1 | Native |
| Порти, що належать до VLAN 1 | Fa0/1, Fa 0/4 |
| IP-адреса мережі | 192.168.1.0/24 |
| VLAN 10 | Study |
| Порти, що належать до VLAN 10 | Fa0/5, Fa 0/8 |
| IP-адреса мережі | 192.168.5.0/24 |
| VLAN 10 | Support |
| Порти, що належать до VLAN 20 | Fa0/9, Fa 0/12 |
| IP-адреса мережі | 192.168.7.0/24 |
| Робоча станція, під'єднана до Fa0/5 | 192.168.5.2/24 |
| Робоча станція, під'єднана до Fa0/9 | 192.168.7.2/24 |
| Підінтерфейс Fa 0/0.1 (VLAN 1) | 192.168.1.1/24 |
| Підінтерфейс Fa 0/0.2 (VLAN 10) | 192.168.5.1/24 |
| Підінтерфейс Fa 0/0.3 (VLAN 20) | 192.168.7.1/24 |

**1. Базові налаштування комутатора та робочих станцій**

За прикладом, наведеним нижче, налаштуйте назву комутатора, паролі (секретний, консольний, на звернення по віртуальних термінальних лініях (їх всього є 16) й управлінську VLAN 1 (табл. 7.1).

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch_A
Switch_A(config)#
Switch_A(config)#enable secret pass
Switch_A(config)#
Switch_A(config)#line con 0
Switch_A(config-line)#password cisco
Switch_A(config-line)#login
Switch_A(config-line)#line vty 0 15
Switch_A(config-line)#password cisco
Switch_A(config-line)#login
Switch_A(config-line)#exit
Switch_A(config-line)#interface vlan1
Switch_A(config)#ip address 192.168.1.2 255.255.255.0
Switch_A(config-if)#no shutdown
Switch_A(config-if)#exit
Switch_A(config)#end
```

*Перегляньте налаштування комутатора за допомогою команди:*

```
Switch_A#show interface vlan 1
```

*Яка MAC-адреса комутатора?*

**2. Перегляд параметрів комутатора**

Важливо знати версію операційної системи (IOS), адже різні версії забезпечують різні можливості комутатора, а також змінюють синтаксис команд. Задайте команду **`show version`** у привілейованому режимі.

*Яка версія операційної системи комутатора?*

**3. Перегляд інформації про VLAN**

Для перегляду інформації по віртуальні локальні мережі на комутаторі у привілейованому режимі задайте команду **`show vlan`**.

*Які VLAN уже існують і яке їх призначення?*

*Які порти належать до управлінської VLAN?*

*Скільки VLAN за замовчуванням встановлено на комутаторі?*

*У чому призначення VLAN 1003 і скільки портів до неї належить?*

**4. Створення нових віртуальних локальних мереж**

Створіть дві нові віртуальні локальні мережі, параметри яких наведено в табл. 7.1.

Наведіть команди по налаштуванню VLAN.

Перегляньте вміст бази даних віртуальних локальних мереж.

*Яка команда при цьому використовується? Чи з'явилися нові VLAN у переліку? Як одержати стислу інформацію про VLAN?*

Використавши налаштування VLAN на основі портів, у режимі налаштування інтерфейсу, призначте відповідні порти до створених VLAN.

*Наведіть команди, які при цьому використовуються.*

**5. Перегляд налаштувань**

Перегляньте інформацію про VLAN та інтерфейси, які їм належать, за допомогою команди **`show vlan.`**

*Які зміни відбулися в базі даних VLAN?*

*Які порти належать до VLAN 1, 10, 20 ?*

Одержіть інформацію про VLAN 10 за її номером, а про VLAN 20 – за назвою.

*Які команди при цьому використовуються?*

*Яку інформацію можна одержати в результаті виконання команд?*

За допомогою команди **ping** перевірте наявність зв'язку між комп'ютерами, які після проведених налаштувань належать до різних віртуальних локальних мереж. *Чи успішно виконалися команди? Поясніть одержані результати*.

*Збережіть результати налаштування для оформлення звіту та видаліть створену конфігурацію.*

**6. Налаштування магістрального з'єднання**

На комутаторі налаштуйте порт Fast Ethernet 0/1 як магістральний. Як спосіб інкапсуляції кадрів від різних VLAN оберіть 802.11q.

*Наведіть команди, які при цьому використовуються.*

**7. Налаштування маршрутизатора**

Активуйте порт маршрутизатора, до якого через магістральну лінію під'єднано комутатор, за допомогою команди **`no shutdown`**.

На базі даного фізичного інтерфейсу створіть три логічні інтерфейси, кожен для окремої VLAN. Параметри налаштувань наведені у табл. 7.1.

*Який тип інкапсуляції обрано для підінтерфейсів? Чим це зумовлено?*

Збережіть параметри маршрутизатора. Перегляньте вміст його таблиці маршрутизації.

*Про що свідчать записи таблиці маршрутів і чи потрібно додатково налаштовувати статичні маршрути між мережами?*

Перевірте з'єднання між пристроями в різних віртуальних локальних мережах. *Який результат перевірки з'єднання?*

Збережіть виконані налаштування та результати виконання команд до текстового файлу. Видаліть створену конфігурацію з комутатора і маршрутизатора.

***Контрольні запитання та завдання***

1. Що таке віртуальні локальні мережі? Чим вони відрізняються від звичайних локальних мереж. Яке їх призначення?
2. Які бувають VLAN? Переваги і недоліки їхнього використання.
3. Як реалізовано зв'язок між хостами, що належать одній VLAN, але під'єднані до різних комутаторів?
4. Які номери можна використовувати при створенні нових VLAN? Що таке зарезервовані номери?
5. Яке призначення управлінської VLAN і як вона налаштовується?
6. Що таке магістральний порт? Чим він відрізняється від порту доступу комутатора?
7. Наведіть приклад створення VLAN 10 і VLAN 20 з назвами Reseach і Marketing.
8. Порівняйте традиційні й віртуальні локальні мережі з точки зору обладнання, протоколів і використання.
9. Що потрібно для налаштування зв'язку між різними віртуальними локальними мережами?
10. Які стандарти визначені для магістральних ліній зв'язку?

# VIII. СТВОРЕННЯ ПІДМЕРЕЖ З МАСКАМИ ЗМІННОЇ ДОВЖИНИ (VLSM)

Кожному вузлу IP-мережі, наприклад комп'ютеру, маршрутизатору або навіть мережному принтеру, надається IP-адреса для ідентифікації цього пристрою при взаємодії з іншими вузлами по мережі.

Протокол IP версії 4 дозволяє використовувати $2^{32}$ (приблизно 4,3 мільярди) адрес, проте деякі великі блоки зарезервовані для спеціальних потреб і недоступні для публічного використання.

***Структура IP-адреси***

Завдяки структурі IP-адреси (рис. 8.1) та постійно зростаючій кількості користувачів мережі Інтернет кількість вільних IP-адрес різко зменшується. Насамперед це пов'язано з неефективним розподілом IP-адрес. Організації, які отримували адреси на початку 80-х, часто володіють більшою кількістю IP-адрес, ніж їм потрібно, оскільки від початку використовувався метод класової адресації, за яким кількість адрес хостів жорстко фіксувалася мережною маскою класу, до якого належить IP-адреса (табл. 8.1). Наприклад, крупним компаніям або навчальним закладам були надані адресні блоки класу A, які містили більше 16 мільйонів IPv4-адрес, більша частина з яких так і залишається досі невикористаною.

| **0** | | | **Клас A** |
|---|---|---|---|
| 0-127 (**M**) | **X** | **X** | **X** |
| 8 | 24 | | |
| мережа | хости | | |

| **1** | **0** | | **Клас B** |
|---|---|---|---|
| 128-191 (**M**) | **M** | **X** | **X** |
| 16 | | 16 | |
| мережа | | хости | |

| **1** | **1** | **0** | **Клас C** |
|---|---|---|---|
| 192-223 (**M**) | **M** | **M** | **X** |
| 24 | | | 8 |
| мережа | | | хости |

Рис. 8.1. *Класи IP-адрес*

Таблиця 8.1

Парамери IP-адрес різних класів

| Клас IP-адреси | Мережна маска | Кількість можливих мереж | Кількість хостів у мережі |
|---|---|---|---|
| **A** | 255.0.0.0/8 | 128 (2 адреси зарезервовано) | 16 777 214 |
| **B** | 255.255.0.0/16 | 16 348 | 65 534 |
| **C** | 255.255.255.0/24 | 2 097152 | 254 |

***Визначення мережних параметрів***

Нехай для заданої IP-адреси необхідно визначити мережну інформацію. Наприклад, дано:

| | |
|---|---|
| **IP-адреса комп'ютера** | 172.25.114.250 |
| **Мережна маска** | 255.255.0.0 (/16) |

**1. Переведення IP-адреси комп'ютера та мережної маски у двійкову систему числення**

| | | | | |
|---|---|---|---|---|
| | **172** | **25** | **114** | **250** |
| **IP-адреса** | 10101100 | 11001000 | 01110010 | 11111010 |
| **Мережна маска** | 11111111 | 11111111 | 00000000 | 00000000 |
| | **255** | **255** | **0** | **0** |

**2. Визначення адреси мережі**

**2.1.** Для визначення адреси мережі на основі IP-адреси вузла та маски слід застосували побітову операцію AND (логічне І) між IP-адресою та мережною маскою у двійковому форматі.

*Зауважте: 1 AND 1 дає 1; 0 AND будь-яке значення дає 0.*

**2.2.** Результат слід перевести в десятковий формат, відокремлюючи кожен октет (8 бітів) крапкою.

**2.3.** У даному прикладі комп'ютер належить мережі з адресою **172.25.0.0:**

| | | | | |
|---|---|---|---|---|
| | **172** | **25** | **114** | **250** |
| **IP-адреса** | 10101100 | 11001000 | 01110010 | 11111010 |
| **Мережна маска** | 11111111 | 11111111 | 00000000 | 00000000 |
| **Адреса мережі** | 10101100 | 11001000 | 00000000 | 00000000 |
| | **172** | **25** | **0** | **0** |

**3. Визначення широкомовної адреси для даної мережі**

Мережна маска відокремлює мережну частину адреси від частини хостів. Якщо у IP-адресі мережі на місцях бітів вузлів стоять двійкові (отже, й десяткові) нулі, тоді у широкомовній адресі на місцях бітів вузлів стоять усі одиниці. Повідомлення з широкомовною адресою призначення потрапляє до всіх кінцевих вузлів у цій мережі.

| | **172** | **25** | **0** | **0** |
|---|---|---|---|---|
| **Адреса мережі** | 10101100 | 11001000 | *00000000* | *00000000* |
| **Маска** | 11111111 | 11111111 | *00000000* | *00000000* |
| **Широкомовна адреса** | 10101100 | 11001000 | *11111111* | *11111111* |
| | **172** | **25** | **255** | **255** |

**4. Визначення кількості кінцевих вузлів у мережі**

Порахувавши кількість бітів, відведених під хости, можна визначити загальну кількість кінцевих пристроїв, яким можна призначати адреси в даній мережі.

**4.1.** Кількість бітів хостів: **16**.

**4.2.** Кожен біт може набувати лише два значення : **0** або **1**.

**4.3.** Отже, піднесемо кількість можливих значень біта (**2**) до степеня, який дорівнює загальній кількості бітів (**16**), і одержимо загальну кількість можливих адрес у мережі з адресою **172.25.0.0**:

$$\mathbf{2^{16} = 65536.}$$

**4.4.** Серед усіх можливих адрес дві не можуть використовуватися для налаштування на кінцевих пристроях. Зокрема, це адреси, в яких на місцях бітів хостів стоять усі нулі (адреса мережі, **172.25.0.0**) і всі одиниці (широкомовна адреса, **172.25.255.255**).

**4.5.** Тому загальна кількість допустимих адрес хостів визначається як:

$$\mathbf{65536 - 2 = 65534.}$$

Простір IP-адрес налічує близько 4.3 млрд. унікальних мережних адрес. Проте з них лише 3.7 млрд. можуть бути призначені для ідентифікації пристроїв у мережі. Через стрімку популярність всесвітньої мережі Інтернет, у січні 2007 більше 2.4 млрд. наявних IP-адрес було розподілено між користувачами мереж та Інтернет-провайдерами.

Коли деяка організація орендує IP-адресу мережі для своїх потреб, вона використовує цілу класову мережну адресу – або адресу класу B, що може налічувати 65534 адреси хостів або адресу класу C з 254 адрес вузлів, тоді як межа класу A може містити більше 16 млн. окремих мережних вузлів. Важко уявити організацію, мережа якої складається з такої кількості хостів. Більшість з адрес, які беруться в оренду, так і залишаються

невикористаними, і, при цьому, не можуть бути надані користувачам інших мереж. Не існує такого класу IP-адрес, який би відповідав потребам організацій і компаній середнього розміру.

Хоча приблизно 1.3 млрд. IP-адрес усе ще доступні для розподілу, деякі дослідження передбачають повне виснаження адресного простору до 2013 р.

***Засоби заощадження IP-адрес***

Серед засобів збереження вільного простору IP-адрес належать:

- безкласова адресація та використання масок змінної довжини для створення підмереж;
- приватні IP-адреси;
- технологія трансляції мережних адрес (Network address translation, NAT), яка дозволяє множині комп'ютерів звертатися назовні локальної мережі над однією публічною IP-адресою;
- впровадження нової версії протоколу IP – IP версії 6.

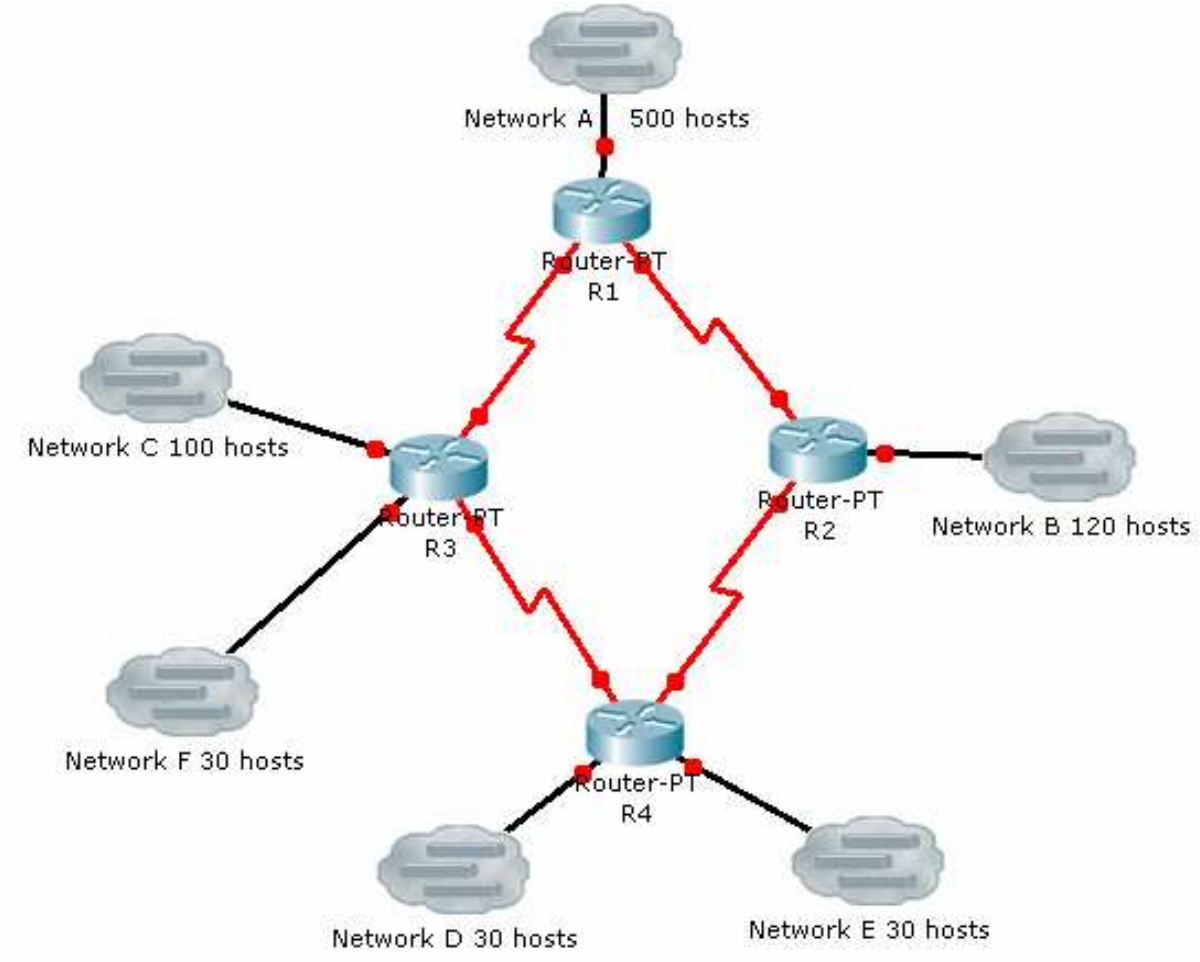



Рис. 8.2. *Топологія для створення підмереж*

### *Підмережі*

Перехід до безкласової адресації та створення підмереж дозволяє створити кілька логічних мереж на основі однієї мережної адреси.

Підмережі створюють завдяки використанню бітів хостів, найбільш наближених до мережної частини IP-адреси, як біти мережі. Таким чином, маска підмережі поширюється на позичені біти і більше не обмежується значеннями /8, /16 або /24. Границя між частиною мережі й вузлів стає більш гнучкою.

Чим більше бітів позичено у хостів, тим більше підмереж можна створити і тим менше вузлів кожна з них може містити. З кожним позиченим бітом подвоюється кількість можливих підмереж.

Для визначення кількості підмереж на основі позичених бітів необхідно піднести **2** (кількість можливих значень біта) до степеня, який дорівнює кількості позичених бітів.

Наприклад, маємо мережну адресу класу B 172.16.0.0/16 і топологію, зображену на рис. 8.2, яка складається з 10 локальних мереж, кожній з яких потрібно надати окрему адресу. Якщо протоколи маршрутизації підтримують лише класову адресацію, то, аби забезпечити адресами всі мережі, можна позичити 8 бітів у частини хостів для утворення підмереж з маскою 255.255.255.0/24 і кількістю допустимих вузлів у кожній – 254.

Таблиця 8.2

| Номер підмережі | Адреса підмережі | Початкова адреса хостів | Кінцева адреса хостів | Широкомовна адреса |
|---|---|---|---|---|
| 0 | 172.16.0.0 | 172.16.0.1 | 172.16.0.254 | 172.16.0.255 |
| 1 | 172.16.1.0 | 172.16.1.1 | 172.16.1.254 | 172.16.1.255 |
| 2 | 172.16.2.0 | 172.16.2.1 | 172.16.2.254 | 172.16.2.255 |
| … | … | … | … | … |
| 254 | 172.16.254.0 | 172.16.254.1 | 172.16.254.254 | 172.16.254.255 |

*Зауважте, що для утворення WAN-з'єднання потрібно лише дві IP-адреси, одна – для послідовного інтерфейсу кожного маршрутизатора.* Це означає, що 252 інші адреси залишаться невикористаними.

### *Створення підмереж з масками змінної довжини*

Технологія створення підмереж із масками змінної довжини (Variable Length Subnet Mask, VLSM) дозволяє на базі однієї IP-адреси створити кілька підмереж, довжина маска яких визначається відповідно до кількості вузлів у кожній підмережі.

Завдяки цій технології, компанії достатньо придбати або взяти в оренду одну мережну IP-адресу, на основі якої створюються мережі, розмір яких

більше не обмежується класовою мережною маскою, а визначається потребами організації. Мінімум IP-адрес залишаються невикористаними на випадок розширення організації зі збільшенням кількості вузлів та додаткових мереж.

Для застосування методу VLSM необхідно дотримуватися таких рекомендацій:

1. Спершу визначте загальну кількість хостів у всій корпоративній мережі, які потребують IP-адрес, з перспективою подальшого розширення. До них належать кінцеві вузли, сервери, проміжні пристрої, інтерфейси маршрутизаторів.

2. Далі, потрібно визначити кількість необхідних підмереж і розмір кожної з них.

3. Слід також врахувати кількість послідовних WAN-з'єднань між маршрутизаторами, кожне з яких належить окремій мережі і складається лише з двох хостів (з'єднаних інтерфейсів маршрутизаторів).

4. Починайте створення та розподіл з підмереж із найбільшою кількістю вузлів, поступово просуваючись до менш численних сегментів, закінчуючи WAN-з'єднаннями.

5. Ретельно задокументовуйте результати виконаного розподілу та призначення IP-адрес.

На рис. 8.2 топологія складається з 10 окремих мереж. Для забезпечення кожної з них адресою використаємо підмережування з масками змінної довжини. З'ясуємо, у якій степені двійка дає число більше, але найбільш наближене до потрібної кількості підмереж. Виявляється, що це $2^4$=16. Отже, позичимо в частини хостів 4 біти для утворення підмереж з маскою /20 (16+4) та визначимо їх адреси.

Таблиця 8.3

| Вихідна адреса мережі 172.16.0.0/16 | | | | | |
|---|---|---|---|---|---|
| Номер підмережі | 2 перші октети | Позичені біти для підмереж | Біти хостів 3-го октету | Біти хостів 4-го октету | Десятковий вигляд адрес підмереж |
| 0 | 172.16. | **0000** | 0000. | 00000000 | 172.16.0.0/20 |
| 1. | 172.16. | **0001** | 0000. | 00000000 | 172.16.16.0/20 |
| 2 | 172.16 | **0010** | 0000. | 00000000 | 172.16.32.0/20 |
| 3 | 172.16. | **0011** | 0000. | 00000000 | 172.16.48.0/20 |
| 4 | 172.16. | **0100** | 0000. | 00000000 | |
| 5 | 172.16. | **0101** | 0000. | 00000000 | |
| … | … | **…** | … | … | … |
| 15 | 172.16. | **1111** | 0000. | 00000000 | 172.16.240.0/20 |

Адреса підмережі визначається шляхом закодування номера підмережі на чотирьох позичених бітах з подальшим переведенням кожного байта отриманої адреси в десяткову форму. Значення перших двох октетів залишається незмінним, адже це номер мережі. Значення останніх 12 бітів – 0, оскільки це частина хостів. У кожній з отриманих підмереж може бути $2^{12}$-2=4096 хостів. При цьому найбільша кількість хостів у даній системі становить 500. Тому, для визначення адреси підмережі за кількістю наявних у ній кінцевих пристроїв, виконаємо подальше підмережування.

Для забезпечення адресами такої кількості хостів у підмережі А з'ясуємо, в якій степені 2 дає число більше, але найбільш наближене до 500. Це $2^9$-2=510. Степінь двійки (9) вказує, скільки бітів потрібно залишити під номери хостів. Решту старших бітів можна застосувати для утворення підпідмереж.

Отже, ще три біти можна позичити для утворення 8 ($2^3$) підмереж потрібного розміру. Для прикладу використаємо нульову підмережу з адресою 172.16.0.0/20 (табл. 8.3).

Таблиця 8.4

| Вихідна адреса мережі 172.16.0.0/20 | | | | | |
|---|---|---|---|---|---|
| Номер під-підмережі | Значення 2-х перших октетів | Біти вихідної підмережі | Біти для утворення підпідмереж | Біти хостів | Десятковий вигляд адрес підмереж |
| 0 | 172.16. | **0000** | *000* | 0.00000000 | 172.16.0.0/23 |
| 1. | 172.16. | **0000** | *001* | 0.00000000 | 172.16.2.0/23 |
| 2 | 172.16 | **0000** | *010* | 0.00000000 | 172.16.4.0/23 |
| 3 | 172.16. | **0000** | *011* | 0.00000000 | 172.16.6.0/23 |
| 4 | 172.16. | **0000** | *100* | 0.00000000 | 172.16.8.0/23 |
| 5 | 172.16. | **0000** | *101* | 0.00000000 | 172.16.10.0/23 |
| 6 | 172.16. | **0000** | *110* | 0.00000000 | 172.16.12.0/23 |
| 7 | 172.16. | **0000** | *111* | 0.00000000 | 172.16.14.0/23 |

Адресу нульової підмережі 172.16.0.0/23 призначимо сегменту А, який складається з 500 хостів. Оскільки мережа з такою адресою здатна підтримувати 510 пристроїв, є можливість невеликого доповнення для неї.

Далі у нашій системі наявні дві мережі В та С з приблизно однаковою кількістю хостів (120 та 100 відповідно). Для них вдамося до подальшого підмережування, використовуючи як базову адресу першої підмережі 172.16.2.0/23 з табл. 8.4. Якщо під номер комп'ютера залишити 7 бітів ($2^7$-2=126), то для менших 4 підмереж позичаємо ще 2 старших біти.

Таблиця 8.5

| Вихідна адреса мережі 172.16.2.0/23 | | | | | |
|---|---|---|---|---|---|
| Номер під-підмережі | Значення 2-х перших октетів | Біти вихідної підмережі | Біти для утворення підпідмереж | Біти хостів | Десятковий вигляд адрес підмереж |
| 0 | 172.16. | **0000001** | *0.0* | 0000000 | 172.16.2.0/25 |
| 1. | 172.16. | **0000001** | *0.1* | 0000000 | 172.16.2.128/25 |
| 2 | 172.16 | **0000001** | *1.0* | 0000000 | 172.16.3.0/25 |
| 3 | 172.16. | **0000001** | *1.1* | 0000000 | 172.16.3.128/25 |

Адреси 0 і 1 підмереж 172.16.2.0 /25 і 172.16.2.128/25 надамо відповідно сегментам B та C наведеної топології. Підмережі з такою маскою можуть містити до 126 ($2^7$-2) хостів.

Далі використаємо адресу наступної вільної підмережі 172.16.3.0/25 (табл. 8.5) для створення на її основи підмереж, які містять по 30 хостів у кожній (D, E, F). При цьому використаємо маску /27, тобто позичимо ще два біти для створення підмереж, по 30 хостів у кожній.

Таблиця 8.6

| Вихідна адреса мережі 172.16.3.0/25 | | | | | |
|---|---|---|---|---|---|
| Номер під-підмережі | Значення 2-х перших октетів | Біти вихідної підмережі | Біти для утворення підпідмереж | Біти хостів | Десятковий вигляд адрес підмереж |
| 0 | 172.16. | **00000011.0** | *00* | 00000 | 172.16.3.0/27 |
| 1. | 172.16. | **00000011.0** | *01* | 00000 | 172.16.3.32/27 |
| 2 | 172.16 | **00000011.0** | *10* | 00000 | 172.16.3.64/27 |
| 3 | 172.16. | **00000011.0** | *11* | 00000 | 172.16.3.96/27 |

Для підмереж D, E та F використаємо адреси 172.16.3.0/27, 172.16.3.32/27 і 172.16.3.64/27 (табл. 8.6).

Отже, ми забезпечили окремими адресами всі локальні сегменти нашої топології. Залишилося визначити номери мереж для послідовних з'єднань, кожне з яких потребує дві адреси для кожного послідовного інтерфейсу маршрутизатора. Таким вимогам найкраще відповідатиме адресам мережі з маскою /30, адже вона забезпечить рівно $2^2$-2=2 адреси. Для створення підмереж для WAN-з'єднань використаємо вільну підмережу з найбільшою маскою: 172.16.3.96/ 27 (табл. 8.7).

Таблиця 8.7

| Вихідна адреса мережі 172.16.3.96/27 | | | | | |
|---|---|---|---|---|---|
| Номер під-підмережі | Значення 3-х перших октетів | Біти вихідної підмережі | Біти для утворення підпідмереж | Біти хостів | Десятковий вигляд адрес підмереж |
| 0 | 172.16.3. | **011** | *000* | 00 | 172.16.3.96/30 |
| 1. | 172.16.3. | **011** | *001* | 00 | 172.16.3.100/30 |
| 2 | 172.16.3. | **011** | *010* | 00 | 172.16.3.104/30 |
| 3 | 172.16.3. | **011** | *011* | 00 | 172.16.3.108/30 |
| 4 | 172.16.3. | **011** | *100* | 00 | 172.16.3.112/30 |
| 5 | 172.16.3. | **011** | *101* | 00 | 172.16.3.116/30 |
| 6 | 172.16.3. | **011** | *110* | 00 | 172.16.3.120/30 |
| 7 | 172.16.3. | **011** | *111* | 00 | 172.16.3.124/30 |

Перші чотири адреси з таблиці 8.7 використовуємо для послідовних з’єднань. Решта можна буде використати в майбутньому в разі розширення мережі.

Отже, метод створення підмереж з масками змінної довжини (VLSM) дозволяє суттєво заощадити IP-адреси, і на основі однієї лише IP-адреси 172.16.0.0/16 (табл. 8.3) створити цілу систему підмереж, довжина маски для яких визначалася за кількістю під’єднаних хостів, з можливістю подальшого розширення (табл. 8.8).

Безкласова адресація та CIDR (*Classless Inter-Domain Routing, безкласова міждоменна маршрутизація*), впроваджені у 1993, стали достойною заміною для попереднього покоління класових мереж з масками фіксованої довжини. Дана методика забезпечила більш ефективне використання та розподіл IP-адрес. Крім того, завдяки провадженню безкласової адресації виникла ціла низка протоколів маршрутизації, які підтримували підмережі та дозволяли декілька підмереж рекламувати як один сумарний маршрут (*summary route*) з маскою, меншою за класову. Завдяки цьому обсяг таблиць маршрутизації та повідомлень-обновлень значно зменшився.

Взагалі, втрачає зміст сам клас IP-адрес (A, B або C), адже границю між частинами мереж та вузлів можна визначити де завгодно, починаючи з 9-го біта. Тобто довжина маски більше не фіксується стандартом протоколу IP, а залежить від кількості хостів, з яких складається мережа.

Таблиця 8.8

Результат створення підмереж для топології (рис. 8.2) за заданими вимогами

| | 510 хостів | 126 хостів | 30 хостів | 2 хости |
|---|---|---|---|---|
| **172.16.0.0/20** | **172.16.0.0/23** | | | |
| | | | | |
| | | | | |
| | | | | |
| | **172.16.2.0/23** | **172.16.2.0/25** | | |
| | | **172.16.2.128/25** | | |
| | | **172.16.3.0/25** | **172.16.3.0/27** | |
| | | | **172.16.3.32/27** | |
| | | | **172.16.3.64/27** | |
| | | | **172.16.3.96/27** | **172.16.3.96/30** |
| | | | | **172.16.3.100/30** |
| | | | | **172.16.3.104/30** |
| | | | | **172.16.3.108/30** |
| | | | | 172.16.3.112/30 |
| | | | | 172.16.3.116/30 |
| | | | | 172.16.3.120/30 |
| | | | | 172.16.3.124/30 |
| | | 172.16.3.128/25 | | |
| | … | | | |
| | 172.16.4.0/23 | | | |
| | … | | | |
| | 172.16.6.0/23 | | | |
| | … | | | |
| | | | | |
| | 172.16.14.0/23 | | | |

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *набуття навичок розробки адресної схеми на основі однієї IP-адреси з урахуванням кількості необхідних підмереж та вузлів, які вони налічують за допомогою методу VLSM.*

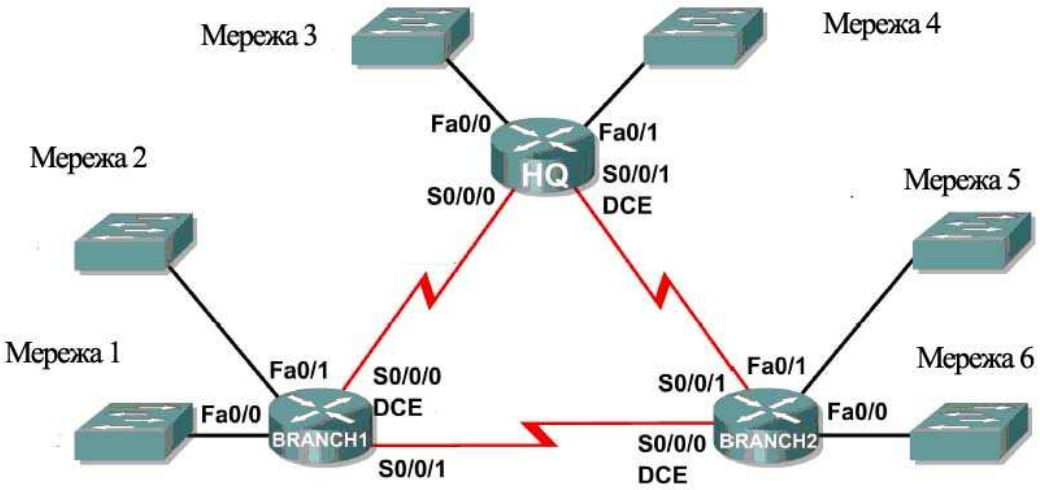



Рис. 8.3. *Схема мережі для розробки адресної схеми*

Дано мережну адресу 192.168.1.0/24, яку необхідно розбити на підмережі та забезпечити IP-адресацію для кожної мережі, наведеної на рис. 8.3. Для забезпечення вимог кожної мережі слід використати метод VLSM. Мережа має такі адресні вимоги:

- локальні мережі (3, 4), під'єднані до маршрутизатора HQ, потребують 50 IP-адрес для хостів кожна (2 підмережі);
- локальні мережі (1, 2), під'єднані до Branch1, складаються кожна з 20 хостів, яким необхідно призначити IP-адреси (2 підмережі);
- локальні мережі (5, 6), під'єднані до Branch2, містять 12 хостів кожна (2 підмережі);
- для кожного послідовного з'єднання між маршрутизаторами необхідно призначити IP-адресу для кожного кінця з'єднання (3 підмережі).

### 1. Вивчення адресних вимоги мережі

1. Скільки всього потрібно підмереж?_____
2. Яка максимальна кількість IP адрес потрібна в одній підмережі? _____
3. Скільки IP адрес потрібно для кожної локальної мережі маршрутизатора Branch1? _____
4. Скільки IP адрес потрібно для кожної локальної мережі маршрутизатора Branch2? _____

5. Скільки IP адрес потрібно для кожного послідовного з’єднання між маршрутизаторами? _____
6. Скільки всього IP адрес потрібно призначити? _____
7. Скільки всього IP адрес доступні в мережі 192.168.1.0/24?_____
8. Чи можна задовольнити дані адресні вимоги, використовуючи мережну адресу 192.168.1.0/24? _____

**2. Розробка адресної схеми**

**2.1. Визначення підмережі для мережного сегмента(ів) із найбільшою кількістю хостів**

1. Які локальні мережі мають найбільшу кількість хостів?_____
2. Скільки потрібно IP-адрес хостів для цієї локальної мережі? _____
3. Скільки бітів треба позичити для утворення підмереж_____, а скільки залишається під IP-адреси хостів _____ ?
4. Яка максимальна кількість IP-адрес хостів буде в кожній підмережі при такому розподілі?_____
5. Визначте адреси для кожної підмережі та занесіть їх у таблицю:

| Номер підмережі | IP-адреса підмережі / маска | Маска підмережі |
|---|---|---|
| Вихідна мережа | 192.168.1.0. | 255.255.255.0 |
| Підмережа 0 | | |
| Підмережа 1 | | |
| … | | |
| Остання підмережа №_ | | |

**2.2. Визначення адрес підмереж для локальних мереж маршрутизатора HQ**

1. Призначте першу доступну підмережу (тобто підмережу 1) локальній мережі 1 маршрутизатора HQ. Яка її адреса_____?
2. Заповніть таблицю параметрів даної підмережі.

**Локальна мережа 1 маршрутизатора HQ**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

3. Призначте наступну дозволену адресу підмережі другому найбільшому локального сегменту 2 маршрутизатора HQ.
4. Заповніть таблицю параметрами даної підмережі.

**Локальна мережа 2 маршрутизатора HQ**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

**2.3. Визначення параметрів для наступних найбільших підмереж**

Далі, наступними найбільшими сегментами є дві локальні мережі маршрутизатора Branch1.

1. Скільки IP адрес потрібно надати кожній локальній мережі? _____

2. Яка наступна дозволена для розподілу адреса підмережі?_____

3. Скільки бітів можна позичити в хостів для створення підмереж, які задовольняють вимогам даних мережних сегментів? _____

4.Якою буде маска підпідмережі після розподілу?

**2.4. Визначення параметрів для локальних мереж BRANCH1**

Розпочнемо з наступної IP адреси мережі після призначеної для локальних мереж HQ.

1. Призначте першу підпідмережу локальному сегменту Branch1.

2. Заповніть таблицю параметрів.

**Локальна мережа 1 маршрутизатора Branch1**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

3. Призначте адресу другої під-підмережі 2-й локальній мережі Branch1.

4. Заповніть таблицю параметрів даної мережі

**Локальна мережа 2 маршрутизатора Branch1**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

**2.5. Визначення підмережної інформації для наступних найбільших мереж**

У даному випадку це локальні мережі маршрутизатора Branch2.

1. Скільки IP-адрес потрібно призначити в кожній LAN? _____

2. Яка найменша підмережа може бути використана для виконання даних вимог? _____

3. Скільки бітів позичаємо в хостів, щоб одержати підмережу з кількістю хостів, що наближається до поставлених вимог?_____

3. Яку максимальну кількість хостів може містити мережа з такою адресою? _____

**2.6. Призначення підмереж для BRANCH2.**

Розпочнемо з IP адреси першої найменшої вільної підмережі.

1. Заповніть таблицю параметрів підмережі, яку призначаємо для 1-ї локальної мережі маршрутизатора Branch2.

**Локальна мережа 1 маршрутизатора Branch2**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

2. Призначте наступну дозволену під мережу для локальної мережі 2 маршрутизатора Branch2.

3. Заповніть таблицю параметрів.

**Локальна мережа 2 маршрутизатора Branch2**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

**2.7. Визначення підмережної інформації для з'єднань між маршрутизаторами**

1. Скільки IP адрес потребує кожен послідовний канал зв'язку? _____

2. Яка найменша підмережа найкраще (без надлишковості) забезпечить необхідну кількість адрес? _____

3. IP-адреса якої підмережі ще не використана?_____

4. Беручи за основу цю адресу, скільки бітів позичаємо у хостів для одержання адрес підмереж для з'єднань між маршрутизаторами?_____

5. Яку максимальну кількість IP-адрес можна призначити в кожній такій підмережі? _____

**2.8. Призначення підмереж на послідовних лініях з'єднання**

Для кожного WAN-з'єднання використайте окрему підмережу та заповніть таблиці параметрів.

**Підмережа для з’єднання між serial портами маршрутизаторів HQ та Branch1**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

**Підмережа для з’єднання між serial портами маршрутизаторів HQ та Branch2**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

**Підмережа для з’єднання між serial портами маршрутизаторів Branch1 та Branch2**

| Мережна адреса | Десяткова маска | Перша дозволена адреса хоста | Остання дозволена адреса хоста | Широкомовна адреса |
|---|---|---|---|---|
| | | | | |

### 3. Призначення IP-адрес мережним пристроям

Після розподілу адресного простору призначте відповідні адреси на інтерфейси мережних пристроїв та заповніть таблицю адрес (табл. 8.9).

#### 3.1. Призначення адрес портам маршрутизатора HQ

1. Призначте першу дозволену адресу хостів у першій локальній мережі HQ на локальний інтерфейс Fa0/0.
2. Призначте першу дозволену адресу хостів у другій локальній підмережі HQ на інтерфейс Fa0/1.
3. Призначте першу доступну адресу хостів підмережі з’єднання між HQ та Branch1 на інтерфейс S0/0/0.
4. Призначте першу дозволену адресу хостів у підмережі послідовного з’єднання між HQ та Branch2 на інтерфейс S0/0/1.

#### 3.2. Призначення адрес портам маршрутизатора Branch1

1. Призначте першу дозволену адресу хостів у 1-й локальній підмережі Branch1 на інтерфейс Fa0/0.
2. Призначте першу дозволену адресу хостів у 2-й локальній підмережі Branch1 на інтерфейс Fa0/1.

3. Призначте останню дозволену адресу хостів з підмережі між Branch1 та HQ на інтерфейс S0/0/0.

4. Призначте першу дозволену адресу хостів з підмережі з'єднання між Branch1 та Branch2 на інтерфейс S0/0/1.

**3.3. Призначення адрес на маршрутизаторі Branch2**

1. Призначте першу дозволену адресу хостів з діапазону 1-ї локальної підмережі Branch2 на інтерфейс Fa0/0.

2. Призначте першу дозволену адресу хостів з діапазону 2-ї локальної мережі Branch 2 на інтерфейс Fa0/1.

3. Призначте останню дозволену адресу хостів з підмережі з'єднання між HQ та Branch2 на інтерфейс S0/0/1.

4. Призначте останню адресу хостів з підмережі з'єднання між Branch1 та Branch2 на інтерфейс S0/0/0.

**3.4. Адреси та маски створених підмереж запишіть до табл.. 8.9.**

Таблиця 8.9

Таблиця адрес

| Пристрій | Інтерфейс | IP-адреса | Маска |
|---|---|---|---|
| **HQ** | **Fa0/0** | | |
| | **Fa0/1** | | |
| | **S0/0/0** | | |
| | **S0/0/1** | | |
| **Branch1** | **Fa0/0** | | |
| | **Fa0/1** | | |
| | **S0/0/0** | | |
| | **S0/0/1** | | |
| **Branch2** | **Fa0/0** | | |
| | **Fa0/1** | | |
| | **S0/0/0** | | |
| | **S0/0/1** | | |

**Додаткове завдання**

Дано мережну адресу 185.18.0.0/16, яку необхідно розбити на підмережі і забезпечити IP-адресацію для кожної мережі, що наведено на рис. 8.3, використавши метод VLSM. Параметри мереж, для кожного варіанту, наведені в табл. 8.10. Для кожного послідовного з'єднання між маршрутизаторами необхідно призначити окрему IP-адресу мережі (3 підмережі).

Таблиця 8.10

Кількість вузлів у кожній мережі (рис. 8.3)

| **Мережа** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **B10** |
|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 50 | 220 | 500 | 450 | 510 | 120 | 480 | 1000 | 850 | 250 |
| **2** | 50 | 150 | 250 | 120 | 450 | 120 | 240 | 120 | 700 | 220 |
| **3** | 25 | 60 | 120 | 110 | 200 | 124 | 210 | 100 | 430 | 140 |
| **4** | 25 | 60 | 30 | 50 | 55 | 100 | 35 | 25 | 60 | 40 |
| **5** | 12 | 40 | 30 | 25 | 60 | 58 | 24 | 25 | 54 | 20 |
| **6** | 14 | 30 | 10 | 20 | 28 | 30 | 16 | 6 | 12 | 10 |

***Контрольні запитання та завдання***

1. Дано такі IP- адреси, які належать до однієї підмережі:
192.168.223.99; 192.168.223.107;192.168.223.117; 192.168.223.127.
Визначте адресу підмережі, до якої вони належать, мережну маску та широкомовну адресу.

2. Що можна сказати про кількість вузлів, мережні параметри та способи створення для кожної, з наведених IP-адрес (під)мереж?
а)192.168.16.192/30; б)172.27.64.98/23; в)172.18.125.6/20;
г) 192.168.87.212/24; д) 172.31.16.128/19.

3. Запишіть значення останнього октету для таких масок підмереж:
/24, / 25, /26, /27, /28, /29, /30.

4. Для підмережі 159.124.163.151/27 запишіть маску підмереж, максимальну кількість вузлів, допустиму для кожної підмережі, та визначте IP-адресу 6-ї підмережі та широкомовну IP-адресу для неї.

5. Визначте сумарний маршрут, за допомогою якого граничний маршрутизатор буде рекламувати всі підключені до нього підмережі (рис. 8.4).

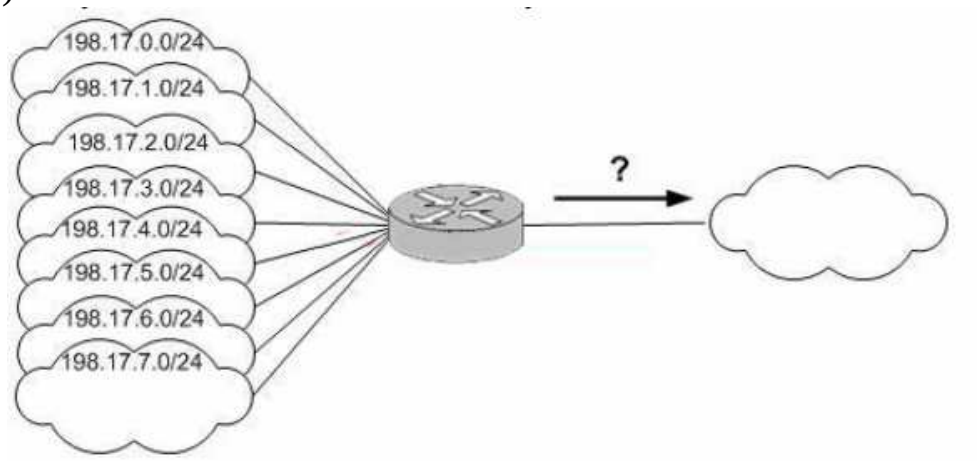



Рис. 8.4

# IX. ТРАНСЛЯЦІЯ МЕРЕЖНИХ АДРЕС (NAT)

Постійно зростаюча потреба в IP-адресах стала справжнім випробуванням для класової моделі IP-адресації. Більшість кампаній намагалася отримати адреси класу B, оскільки вони найбільше відповідали їх потребам завдяки оптимальному співвідношенню кількості мереж і хостів у них. Дійсно, для корпоративних мереж адреса класу A з 16 мільйонів хостів надавала більші можливості, ніж потрібно, а мережа класу C не могла задовольнити потреби великої кампанії через невелику кількість хостів, яким можна було надати адреси. До 1991 року стало очевидним, що витрачання адресного простору класу B набуло загрозливих масштабів і слід вживати негайних заходів, аби запобігти вичерпанню доступних адрес, зокрема:

- застосування безкласової міждоменної маршрутизації (classless interdomain routing, CIDR) і використання масок змінної довжини (VLSM);
- використання загальнодоступних (приватних) IP-адрес і механізму перетворення мережних адрес Network Address Translation (NAT);
- впровадження протоколу IP версії 6 (IPv6).

У зв’язку з постійною потребою в IP-адресах сумісно з проблемами їх вичерпання було переглянуто процедуру надання IP-адрес центральними органами. Спочатку повний контроль за призначенням і розподілом IP-адрес здійснювався організацією IANA та реєстром Internet – Internet Registry (IR). Усі IP-адреси розподілялися послідовно серед організацій, незалежно від їх географічного розташування та способу підключення до мережі Internet. Згодом було вирішено доручити цю задачу кільком адміністраціям (таким як сервіс-провайдери), які, у свою чергу, розподіляли б адреси серед клієнтів свого регіону з наданих їм діапазонів. Розподілом публічних Internet-адрес керують п’ять організацій (рис. 9.1):

- ARIN;
- RIPE;
- APNIC;
- LACNIC;
- AfricNIC.

У загальному такий метод розподілу виявився більш ефективним. Він до деякої міри подібний до підходу, який використовується при розподілі номерів у телефонній мережі, де коди відповідають географічним областям (мережам провайдерів), префікси при наборі номера – регіонам або районам міста (клієнтам провайдерів), а решта частини – індивідуальним номерам абонентів (кінцевим користувачам).


Рис. 9.1. *Організації, що розподіляють IP-адреси для визначених регіонів*

***Приватні адреси й перетворення мережних адрес***

Для зниження темпів розподілу IP-адрес важливо було визначити вимоги до мереж та розподілу адрес у них. Мережі організацій можуть мати:

• глобальну зв'язаність (Global connectivity);

• внутрішню зв'язаність (Private connectivity).

*Глобальна зв'язаність* означає, що всі хости всередині організації повинні мати доступ як до хостів внутрішньої корпоративної мережі, так і до хостів мережі Internet. У цьому випадку кінцевим пристроям потрібно призначити унікальні IP-адреси, які б відрізняли їх як у локальній мережі організації, так і за її межами. Організації, яким необхідний зв'язок на рівні глобальної мережі, беруть в оренду IP-адреси у своїх сервіс-провайдерів.

*Внутрішня зв'язаність* передбачає доступ до хостів лише в межах корпоративної мережі, без необхідності виходу в Internet. Прикладами хостів, які потребують внутрішнього з'єднання, можуть бути банкомати, електронні касові апарати в магазинах та інше обладнання, яке не вимагає з'єднання з хостами за межами компанії. Такі внутрішні хости можуть мати унікальні IP-адреси лише всередині корпоративної мережі організації. Для цих потреб організацією IANA зарезервовано три блоки так званих приватних IP-адрес, передбачені для використання всередині мережі :

• 10.0.0.0 -0.255.255.255 (одна мережа класу A);

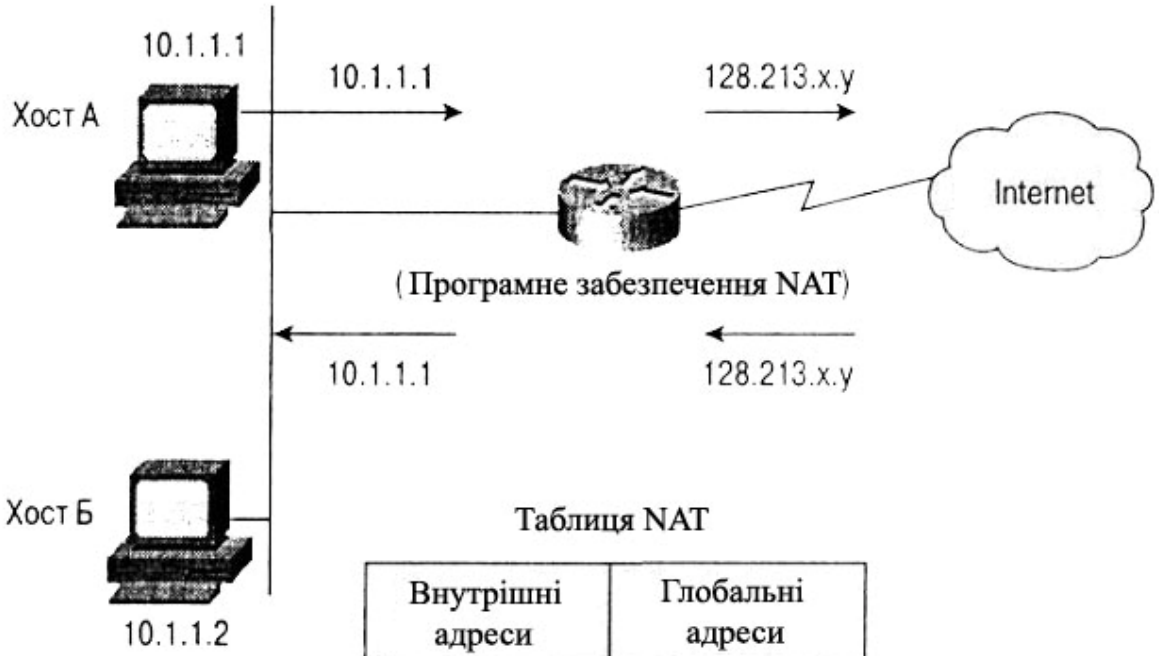
• 172.16.0.0 -172.31.255.255 (16 неперервних блоків класу B);

• 192.168.0.0 - 192.168.255.255 (256 неперервних мереж класу C).

Компанія, яка обирає адреси для внутрішньої мережі з вищенаведених діапазонів, не потребує спеціального дозволу на їх використання від IANA або реєстру мережі Internet. Хости, які отримують внутрішні IP-адреси, можуть з'єднуватися між собою всередині компанії, але не здатні надсилати запити назовні мережі організації без спеціальних пристроїв-посередників (proxy) або шлюзу (gateway). Хости внутрішньої мережі не можуть з'єднуватися з хостами мережі Internet, тому що пакети, які надсилаються, мають IP-адресу відправника, який невизначений у глобальній мережі. Насправді в світі може існувати безліч компаній, які для власних локальних мереж використовують одні і ті самі внутрішні адреси, що неприпустимо для мережі Internet, де для ідентифікації користувачів використовуються лише унікальні публічні IP-адреси.

***Транслятор мережної адреси***

Деякі компанії при переході від внутрішніх до глобальних IP-адрес використовують технологію трансляції (або перетворення) мережних адрес Network Address Translator (NAT).




Таблиця NAT

| Внутрішні адреси | Глобальні адреси |
|---|---|
| 10.1.1.1 | 128.213.x.y |
| 10.1.1.2 | 128.213.z.w |

Рис. 9.2. *Приклад трансляції мережних адрес*

Маршрутизатор з NAT розташовується зазвичай на границі домену й перетворює приватні IP-адреси у звичайні для мережі Internet глобальні адреси і навпаки.

На рис. 9.2 зображено хости А і Б з IP-адресами 10.1.1.1 і 10.1.1.2 відповідно.

Якщо цим хостам необхідно зв’язатися з вузлом поза мережею компанії, пристрій NAT перетворює IP-адресу джерела у пакетах згідно з встановленою (або динамічно наданою) IP-адресою з таблиці NAT. Таким чином, пакети від хоста А досягатимуть віддаленого вузла з IP-адресою джерела 128.213.x.y. Отримувач у глобальній мережі може навіть не підозрювати про перетворення IP-адрес і надсилатиме відповідь за глобальною IP-адресою. Пакети-відгуки, які надходять з мережі Internet як адресу пункту призначення, міститимуть IP-адресу вхідного інтерфейсу маршрутизатора, на якому здійснювалася трансляція IP-адрес. Далі цю глобальну адресу, відповідно до таблиці NAT, буде перетворено на внутрішню IP-адресу вузла, який розпочав сеанс зв’язку.

Функціонування NAT не завжди потребує встановлення окремого пристрою. Часто його можна організувати на базі програмного забезпечення маршрутизатора, який виконує роль шлюзу в системі. Зокрема, функції NAT є частиною операційної системи маршрутизаторів Cisco IOS.

Трансляція мережних адрес може здійснюватися статично або динамічно.

При *статичній трансляції* кожній внутрішній локальній адресі відповідає визначена постійна глобальна адреса. У такий спосіб обслуговуються пристрої, які потребують безперебійного доступу через Internet, зокрема корпоративні сервери та мережні пристрої.

Для здійснення *динамічної трансляції* компанія використовує набір зовнішніх адрес, кількість яких зазвичай менша за кількість використовуваних внутрішніх приватних адрес. Для звернення назовні хосту призначається будь-яка вільна зовнішня IP-адреса. Крім того, кожне звернення відстежується за унікальним номером порту. Це означає, що для надсилання запитів назовні різні відправники можуть використовувати одну й ту ж саму публічну адресу.

Переваги NAT:

- заощаджує зареєстровані зовнішні IP-адреси завдяки внутрішньому використанню приватних адрес;

- позбавляє необхідності перевизначати IP-адреси хостів усередині мережі при переході до іншого провайдера послуги;
- захищає безпеку мережі, оскільки справжні внутрішні адреси пристроїв не поширюються при зверненнях назовні.

Недоліки NAT:

- збільшення затримок за рахунок додаткової обробки пакетів;
- навантаження на CPU при надходженні кожного пакета з метою визначення, чи потребує він трансляції, обробка та зміна IP- і, можливо, TCP- або UDP-заголовків;
- неможливість використання прикладних мережних програм, які потребують реальних IP-адрес користувачів.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *навчитися налаштовувати на маршрутизаторі трансляцію мережних адрес (NAT) для перетворення внутрішніх приватних IP-адрес на зовнішні публічні адреси, придатні для маршрутизації назовні локальної мережі.*

Нехай потрібно налаштувати мережу невеликої компанії, якій ISP надав у користування мережну IP-адресу 199.99.9.32/27. Ця мережа містить 30 публічних IP-адрес. Оскільки компанія потребує для внутрішнього використання більше ніж 30 адрес, слід використати NAT. Адреси в діапазоні 199.99.9.33 – 199.99.9.39 слід використати для статичного призначення, а 199.99.9.40 – 199.99.9.62 – для динамічного. Між ISP та шлюзом виконується статична маршрутизація, а маршрут за замовчуванням, який веде до ISP, потрібно налаштувати на шлюзі. Адреса зворотної петлі (loopback) на маршрутизаторі ISP позначатиме під'єднання до мережі Internet.

З'єднайте пристрої в мережу за схемою, наведеною на рис. 9.3.

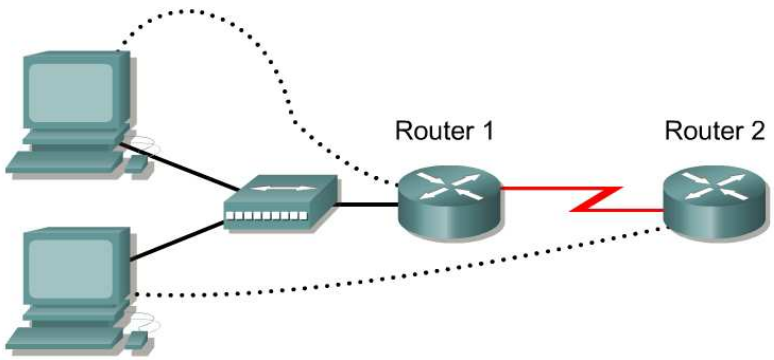



Рис. 9.3. *Топологія для налаштування NAT*

Таблиця 9.1

| Позначення | Назва | IP-адреса /маска Fa 0 | Тип інтерфейсу serial 0 | IP-адреса / маска serial 0 | IP-адреса / маска loopback 0 |
|---|---|---|---|---|---|
| Router1 | Gateway | 10.10.10.1/24 | DTE | 200.2.2.18/30 | - |
| Router2 | ISP | - | DCE | 200.2.2.17/30 | 172.16.1.1/32 |

**1. Налаштування маршрутизаторів**

Налаштуйте маршрутизатори згідно з параметрами, наведеними в табл. 9.1.

**2. Налаштування параметри хостів**

Робочі станції повинні безперешкодно з'єднуватися між собою і з маршрутизатором, до якого вони під'єднані. Налаштуйте на робочих станціях локальної мережі IP-адреси: 10.10.10.10/24 (PC1) та 10.10.10.12/24 (PC2). Як шлюз за замовчуванням оберіть адресу локального інтерфейсу маршрутизатора 10.10.10.1. Для перевірки зв'язку використайте команду **ping**. У разі невдалого виконання команди перевірте наявність фізичного з'єднання та правильність налаштованих параметрів робочих станцій.

**3. Створення статичного маршруту**

Налаштуйте статичний маршрут від ISP до маршрутизатора Gateway. Для доступу до мережі Internet для нашої мережі було надано адресу мережі 199.99.9.32/27. Отже, за цією адресою провайдер розпізнає нашу мережу серед усіх інших. За наявності єдиного з'єднання та незмінних мережних параметрів найкращим способом утворення зв'язку між ISP і граничним шлюзом мережі буде створення статичного маршруту. Використайте таку команду **`ip route`**:

`ISP(config)#ip route 199.99.9.32 255.255.255.224 200.2.2.18`

*Як перевірити вміст таблиці маршрутизації?*

*Чи з'явився статичний маршрут у таблиці маршрутизації?*

*Чи утворено зв'язок в обох напрямках між ISP та Gateway? Якщо ні, назвіть можливі причини, та команди, які допоможуть їх виявити.*

**4. Створення маршруту за замовчуванням**

Звернення назовні досліджуваної мережі можуть пролягати в найрізноманітніших напрямках до безлічі отримувачів, адреси яких не в змозі вмістити жодна таблиця маршрутів. Тому всі зовнішні запити слід спрямовувати до маршрутизатора провайдера, який визначатиме

подальший шлях їх проходження. Для цього від маршрутизатора Gateway до ISP потрібно створити статичний маршрут за замовчуванням, за яким спрямовуватимуться пакети, що не знаходять більш конкретного шляху передачі в таблиці маршрутизації. Маршрут за замовчуванням позначається як мережа з адресою і маскою 0.0.0.0 0.0.0.0 і створюється як звичайний статичний маршрут:

`Gateway(config)#`**`ip route`** 0.0.0.0 0.0.0.0 200.2.2.17

*Чи з'явився статичний маршрут у таблиці маршрутизації ?*

*Як позначається маршрут за замовчуванням?*

*Перевірте наявність зв'язку між однією з робочих станцій та послідовним інтерфейсом маршрутизатора ISP за допомогою команди* ***ping****.*

## 5. Налаштування NAT

Трансляція приватних IP-адрес здійснюється на маршрутизаторі Gateway, оскільки він є крайньою точкою локальної мережі.

### 5.1. Налаштування статичної трансляції

Припустимо, що для PC1 необхідно використовувати постійну зовнішню IP-адресу. Для цього слід виконати статичну трансляцію за допомогою команди:

**`Router(config)# ip nat inside source static`** *внутрішня_IP-адреса зовнішня_ IP-адреса*

Оберемо першу зовнішню адресу з діапазону 199.99.9.33 – 199.99.9.39, передбаченого для статичного призначення. Тоді команда налаштування матиме вигляд:

**`Gateway(config)# ip nat inside source static`** 10.10.10.10. 199.99.9.33

### 5.2. Налаштування динамічної трансляції

Динамічна трансляція налаштовується у декілька етапів:

5.2.1. За допомогою списку управління доступом визначається набір внутрішніх приватних IP-адрес, які необхідно перетворювати.

`Gateway(config)#`**`access-list 1 permit`** 10.10.10.0 0.0.0.255

Повідомлення відправника, IP-адреса якого потрапила у зазначений діапазон, транслюватиметься при зовнішніх зверненнях.

5.2.2. Далі визначається набір публічних адрес, які розподілятимуться для користувачів внутрішньої локальної мережі. Для цього

використовується команда глобальної конфігурації **ip nat pool** у форматі:

Router(config)# **ip nat pool** *назва_діапазону початкова_IP-адреса кінцева_IP-адреса* **netmask** *маска_мережі*

У випадку даної мережі за умовами динамічного розподілу набір публічних адрес команда матиме вигляд:

Gateway(config)#**ip nat pool** public-access 199.99.9.40 199.99.9.62 **netmask** 255.255.255.224

5.2.3. Наступний крок – зв'язування створеного діапазону публічних адрес з приватними адресами, які необхідно транслювати, визначеними за допомогою списку управління доступом. Для цього використовується команда **ip nat inside** вигляду:

Router(config)# **ip nat inside sourse list** *номер_списку* **pool** *назва_діапазону*

Gateway(config)#**ip nat inside source list** 1 **pool** public-access

### 5.3. Визначення інтерфейсів

На граничному маршрутизаторі, для інтерфейсів, які беруть участь у NAT, необхідно зазначити, чи вони належать до внутрішньої мережі, чи використовуються для виходу назовні. Для цього використовуються відповідні команди в режимі конфігурації інтерфейсу: **ip nat inside** або **ip nat outside**. В нашому випадку для маршрутизатора Gateway внутрішнім вважається інтерфейс fa 0, а зовнішні звернення до ISP виконуються через послідовний порт s0. Тому команди налаштування статусів цих інтерфейсів матимуть вигляд:

```
Gateway(config)#interface fa 0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface serial 0
Gateway(config-if)#ip nat outside
```

### 5.4. Перевірка налаштувань

На обох робочих станціях запустіть на виконання команду **ping** 172.16.1.1. *Чи успішний результат виконання?*

Переглянути загальні результати трансляції IP-адрес на маршрутизаторі Gateway можна за допомогою команди **show ip nat translations**. *Наведіть результат виконання команди*.

*Який вигляд має внутрішня локальна адреса* (inside local)?

*Які глобальні адреси були призначені?*
*Що означає адреса* outside local?
Статистику по трансляції надає команда **`show ip nat statistics`**.
*За допомогою цієї команди визначте такі параметри:*
Всього активних трансляцій: статичних_____, динамічних_____.
Вихідні інтерфейси:_____
Вхідні інтерфейси:_____
Джерело внутрішніх адрес:_____

***Контрольні запитання та завдання***

1. Який спосіб перетворення IP-адрес використовувався на маршрутизаторі, зважаючи на наведений результат:

NAT1# **show ip nat translations**

| Pro Inside global | Inside local | Outside local | Outside global |
|---|---|---|---|
| udp 198.18.24.211:123 | 192.168.254.7:123 | 192.2.182.4:123 | 192.2.182.4:123 |
| tcp 198.18.24.211:4509 | 192.168.254.66:4509 | 192.0.2.184:80 | 192.0.2.184:80 |
| tcp 198.18.24.211:4643 | 192.168.254.2:4643 | 192.0.2.71:5190 | 1982.0.2.71:5190 |
| tcp 198.18.24.211:4630 | 192.168.254.7:4630 | 192.0.2.71:5190 | 192.0.2.71:5190 |
| udp 198..18.24.211:1026 | 192.168.254.9:1026 | 198.18.24.4:53 | 198.18.24.4:53 |

```
Router1 (config)# ip nat inside source static 192.168.0.100 209.165.200.2
Router1 (config)# interface serial0/0/0
Router1 (config-if)# ip nat inside
Router1 (config-if)# no shut
Router1 (config-if)# ip address 10.1.1.2 255.255.255.0
Router1 (config)# interface serial 0/0/2
Router1 (config-if)# ip address 209.165.200.2  255.255.255.0
Router1 (config-if)# ip nat outside
Router1 (config-if)# no shut
```

2. Переглянувши наведені налаштування, відтворіть схему з’єднання пристроїв з позначенням адрес інтерфейсів, визначте адресу або адреси вузлів, які підлягатимуть трансляції, та глобальну адресу, яка для цього використовується.
3. Назвіть способи заощадження вільних IP-адрес.
4. Для чого використовується приватна адресації?
5. Який тип трансляції мережних адрес слід застосувати для серверів організації, доступних через мережу Інтернет.

# X. ІНЖЕНЕРІЯ ГОЛОСОВОГО ТРАФІКА

IP-телефонія (*VoIP, Voice over Internet Protocol, голос через протокол IP*) – технологія, яка використовує комп'ютерну мережу з пакетною комутацією повідомлень на базі протоколу IP для передачі голосу в режимі реального часу.

Під час розмови наші голосові сигнали перетворюються в пакети даних, які потім стискаються. Далі ці пакети з голосовими даними надсилаються через Інтернет до отримувача. Коли пакети досягають адресата, вони декодуються в аналоговий голосовий сигнал.

***Особливості IP-телефонії***

Чому IP-телефонія привертає до себе увагу і набуває дедалі більшої популярності?

Завдяки меншим витратам на традиційні телефонні розмови, зокрема на міжміські та міжнародні дзвінки та обладнання. Немає необхідності прокладати окрему абонентську телефонну лінію, купляти телефонний апарат, а також очікувати, коли з'явиться можливість підключення до комутатора.

Традиційні телефонні лінії належать до виділених підключень, які надають можливість постійного доступу до телефонної мережі. Плата за послугу зв'язку визначається за абонентською платою за телефонні послуги та часом використання телефонної лінії (тривалістю розмов).

На відміну від аналогової телефонії, IP-телефонія створює «з'єднання за вимогою», а для передачі голосових даних використовується персональний комп'ютер з додатковим програмним забезпеченням та засобами прийому/передачі голосу та відео, а також традиційна комп'ютерна мережа, через яку здійснюється доступ до мережі Інтернет.

При звичному способі передачі голосу (аналогова телефонія) використовується канал з пропускною здатністю 64 кбіт/с незалежно від того, розмовляє чи мовчить абонент під час телефонної розмови. У випадку передачі розмови по IP-мережах, завдяки цифровій обробці та компресії (стисненню), голос передається у вигляді цифрової інформації, з якої вилучаються паузи. Це дозволяє в одному каналі передавати від 8 і більше з'єднань одночасно, що у свою чергу забезпечує зменшення тарифів за послугу телефонного зв'язку.

Крім того, IP-телефонія приваблює додатковими можливостями сумісного доступу до мережі Інтернет. Голосові дані, факсимільні повідомлення передаються вже з використанням Інтернет-протоколів. Таким чином, голосова інформація і звичайні дані передаються по одній і

тій самій мережі. Це означає, що при підключенні до комп'ютерної мережі, в ній можна поєднувати телефонію, і голосовий трафік буде передаватися по тих самих каналах, що й дані (рис. 10.1).

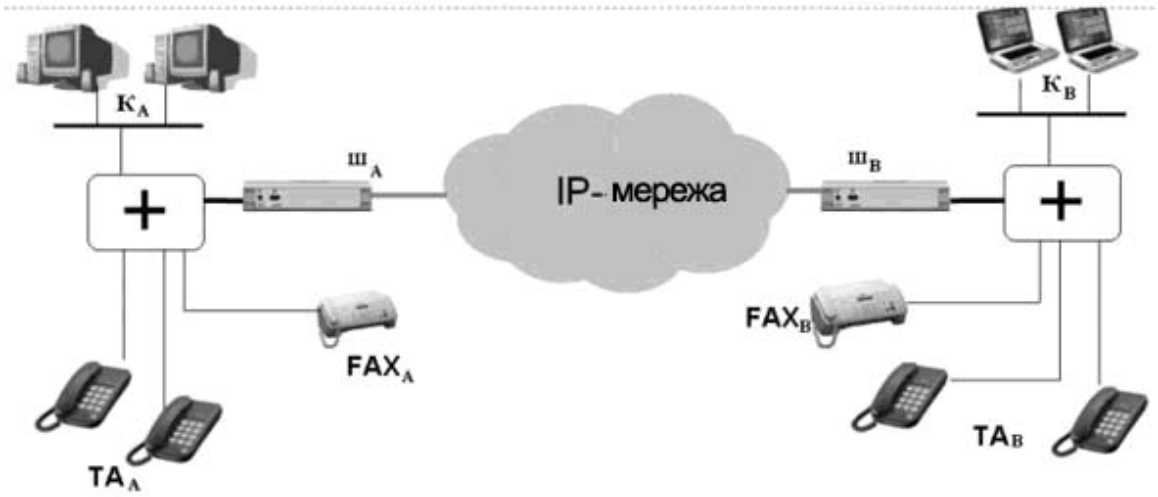



Рис. 10.1. *Комп'ютерна мережа, що надає послуги IP-телефонії*

На рис. 10.1 зображені:

- А, В – абоненти, які обмінюються інформацією по мережі.
- $К_А$, $К_В$ – комп'ютери абонентів А і В відповідно;
- $Ш_А$ і $Ш_В$ – шлюзи А і В;
- $FAX_А$ і $FAX_В$ – телефакси А і В;
- $TA_А$ і $TA_В$ – телефони А і В.

Ще одна важлива особливість VoIP – відкрита архітектура з використанням різними виробниками спільних протоколів IP-телефонії: H.323, MGCP, SIP тощо.

***Принципи пакетної передачі***

Для здійснення сеансу зв'язку ми набираємо номер потрібного абонента, після чого виконується з'єднання з мережним шлюзом, який дозволяє визначити мережну адресу пункту призначення

Голосове повідомлення абонента А за допомогою мікрофона перетворюється в електричний аналоговий сигнал, який далі кодується. Усередині шлюзу здійснюється цифрова обробка голосового сигналу.

Після цифрової обробки сигнал, який першопочатково вимагав, як і наша розмова, канал пропускної здатності 64 кбіт/с, стискається згідно з обраним кодеком і розбивається на пакети сигналів відповідно до типу пристрою кодування (кодеку). У перетвореннях беруть участь як апаратні, так і програмні засоби абонента А.

**Кодек** (кодер/декодер) в IP-телефонії – це алгоритм перетворення аналогової голосової інформації в цифровий потік байтів (IP-пакети), з одного боку, і зворотне перетворення цифрових даних у голосові – з боку приймаючої сторони.

Існує велика кількість кодеків, які відрізняються за якістю передачі вихідної голосової інформації та необхідною при цьому смуги пропускання. Усі ці кодеки стандартизовані й підтримуються в більшості VoIP-обладнання.

Кожен кодек кодує і стискає голос із певною інтенсивністю. Тому при його виборі слід розуміти, що чим більше кодек стискає голос, тим менша смуга пропускання Інтернет-з'єднання необхідна. Але водночас може значно погіршуватися якість голосу при розкодуванні. І навпаки, чим менше стискання, тим натуральніше звучить голос і потребує для передачі більше Інтернет–ресурсів.

Кодек G.711 – один з перших мінімально необхідних цифрових кодеків мовного сигналу. Це означає, що будь-який пристрій VoIP повинен підтримувати даний тип кодування.

Рекомендація G.723.1 затверджена ITU-T у листопаді 1995 р. Кодек G.723.1 є базовим для додатків IP-телефонії. Кодек G.723.1 передбачає дві швидкості передачі: 6.3 кбіт/с і 5.3 кбіт/с. Режим роботи може змінюватися динамічно від кадру до кадру.

Кодек G.726 забезпечує кодування цифрового потоку зі швидкістю 40, 32, 24 або 16 кбіт/с. Проте у додатках IP-телефонії цей кодек практично не використовується, оскільки він не забезпечує достатньої стійкості до втрат інформації.

Кодек G.728 спеціально розроблявся для обладнання ущільнення телефонних каналів і забезпечує малу затримку (< 5 мс).

Кодек G.729 дуже популярний у програмах передачі голосу по мережах Frame Relay. Кодек використовує кадр тривалістю 10 мс і забезпечує швидкість передачі 8 кбіт/с. Проте для кодера необхідний попередній аналіз сигнала тривалістю 5 мс.

Далі стиснуті дані надсилаються через мережу. З боку отримувача встановлено аналогічний набір пристроїв абонента В, які виконують перетворення у зворотному порядку. Пакети з мережі потрапляють до телефонного шлюзу, під'єднаного до телефонної лінії здійснюється декодування цифрового сигналу і його перетворення до аналогової форми, яка приводить у дію звуковий динамік.

Наведені етапи перетворення сигналів і передачі відбуваються за лічені частки секунди, практично в реальному часі, що дозволяє забезпечити розмову у двох напрямках одночасно.

Таблиця 10.1

Характеристики кодексів

| Кодек | Швидкість кодування, кбіт/с | Складність реалізації | Якість | Необхідна пропускна здатність, кбіт/с | Затримка |
|---|---|---|---|---|---|
| G. 726 | 32/24/16 | Низька | Добра (32 К), погана (16 К) | 57/52/39 | Дуже низька (0.125 мс) |
| G. 729 | 8 | Висока | Добра | 26 | Низька (10 мс) |
| G. 723 | 6.4/5.3 | Помірна | Добра(6.4), середня (5.3) | 183/173 | Висока (37 мс) |
| G. 728 | 16 | Дуже висока | Добра | 35 | Дуже низька (3-5 мс) |

***Протоколи управління голосовими з'єднанням***

Архітектуру технології VoIP можна спрощено уявити у вигляді двох площин. Нижня площина – це базова мережа з маршрутизацією пакетів IP, верхня – програмні засоби управління обслуговуванням викликів.

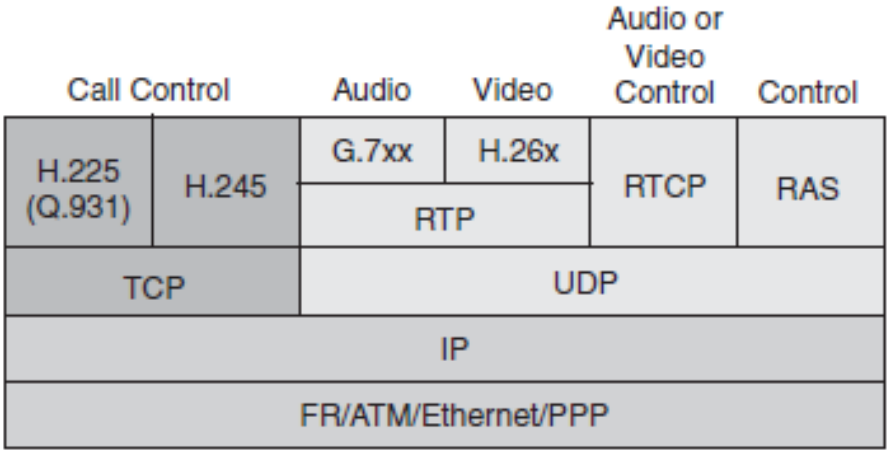



Рис. 10.2. *Стек протоколів для передачі голосу по мережі*

Нижня площина являє собою комбінацію взаємопов'язаних протоколів Інтернет, до яких належать RTP (Real Time Transport Protocol), що функціонує поверх транспортного протоколу UDP, який у свою чергу забезпечує роботу протоколу IP.

Отже, ієрархія протоколів RTP/UDP/IP відіграє роль транспортного механізму для голосового трафика. Зауважимо, що в мережах з маршрутизацією пакетів IP для передачі даних зазвичай передбачаються механізми повторної передачі пакетів у випадку їх втрат. При передачі голосової інформації в реальному часі цей спосіб не може застосовуватися, оскільки голосова інформація більш чутлива до затримок, аніж до втрат. Тому для передачі голосу, а також відеоінформації, використовується механізм негарантованої доставки інформації RTP/UDP/IP.

RTP забезпечує додаткове відстеження послідовності пакетів у часі, необхідне для передачі голосового трафіка. RTP використовує порядковий номер для відновлення правильної послідовності пакетів при отриманні, часові мітки дозволяють визначити час між надходженням пакетів, а отже – коливання затримки, яке називають тремтінням. Ця інформація надзвичайна важлива для забезпечення високоякісних VoIP-розмов.

Використання RTP важливе для даних реального часу; проте цей протокол має деякі недоліки. Заголовки пакетів IP/UDP/RTP мають розмір 20, 8 та 12 байтів, що створює заголовок загальним розміром 40 байтів. Це вдвічі більше за розмір голосового пакета, стиснутого при використанні кодека G.729. Збільшення заголовку зумовлює значний надлишок голосового трафіка та зменшує пропускну здатність.

Проте великі заголовки IP/UDP/RTP можна стиснути за допомогою компресії RTP-заголовка (compressed RTP, cRTP).

Верхня площина архітектури VoIP управляє обслуговуванням запитів зв’язку, тобто адресацією, куди потрібно доправити виклик, і способом налаштування з’єднання між абонентами. Один з інструментів такого управління – протокол SIP (Session Initiation Protocol).

Для налаштування й управління сеансом зв’язку використовується протокол транспортного рівня TCP.

Стандарт ITU-T H.323 – це основа для передачі аудіо, відео і даних через IP-мережу, завдяки якому мультимедійні продукти та прикладні програми від різних виробників можуть безперешкодно взаємодіяти, дозволяючи користувачам передавати інформацію, не турбуючись про сумісність.

Стандарт H.323 широкий за обсягом і стосується спеціалізованих пристроїв, таких як IP-телефони та голосові шлюзи, вбудовані технології для персональних комп’ютерів (наприклад, Microsoft NetMeeting), а також засоби конференц-з’єднання. H.323 містить засоби управління дзвінками (налаштування сеансу, підтримка та припинення), керування

мультимедійними даними та пропускною здатністю, підтримка конференції в багатьох напрямках.

З'єднання з використанням H.323 складається із суміші сигналів аудіо, відео, даних та керуючих сигналів. Для налаштування голосового дзвінка H.323 використовує інші стандарти, зокрема H.225 і H.245. Стандарт H.225 описує сигнали, для налаштування сеансу та упаковки даних між двома пристроями. Зокрема, повідомлення про установку H.225 містить інформацію про номери абонентів обох сторін. H.245 – це стандарт управління для передачі мультимедійної інформації, який описує повідомлення та процедури для відкриття та закриття каналів для аудіо, відео, даних.

Протокол SIP визначений у RFC 3261, *SIP: Session Initiation Protocol– протокол встановлення сеансу в'язку*. Він регламентує налаштування і завершення мультимедійних сесій – сеансів зв'язку, в ході яких користувачів можуть говорити один з одним, обмінюватися відео-матеріалами та текстом, сумісно працювати над додатками тощо.

SIP поєднується з іншими службами IP, такими як e-mail, www, голосова пошта, миттєві повідомлення, конференції та мультимедійна співпраця. При використанні в інфраструктурі IP, SIP забезпечує з'єднання з багатьма пристроями різного виробництва та середовищ.

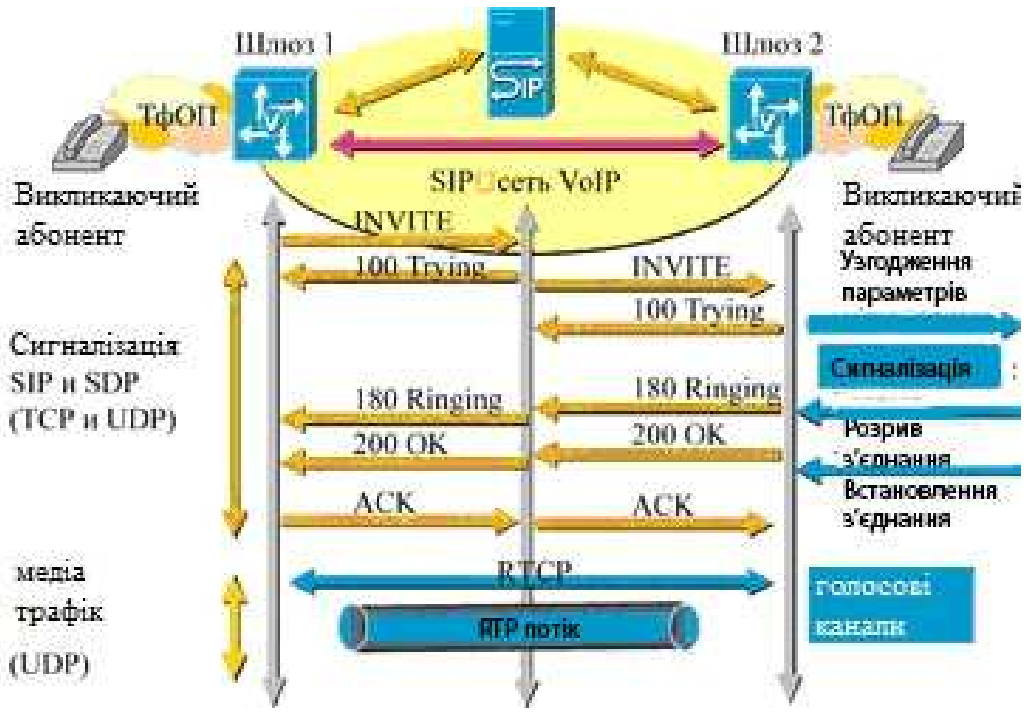



Рис. 10.3. *Сценарій з'єднання за протоколом SIP*

SIP може прокладати окремі голосові дзвінки або підтримувати конференц-зв’язок, відеоконференції та відеодзвінки між двома абонентами, колективну роботу через мережу Інтернет або обмін повідомленнями в чаті.

SIP дуже схожий на протокол HTTP, оскільки розроблявся за принципами специфікацій HTTP і SMTP. SIP – це клієнт-серверний протокол, робота якого складається з послідовності запитів і відгуків, причому всі SIP-заголовки передаються у форматі ASCII-тексту, і тому легко читаються. SIP дозволяє використовувати логічну адресацію (URL) на базі протоколу TCP або UDP. Користувач у мережі під управлінням протоколу SIP ідентифікується за допомогою унікальної адреси SIP, яку називають універсальним ідентифікатором ресурсу (uniform resource identifier (URI)), *SIP URI*. Формат SIP URI подібний до e-mail адреси. Він звичайно складається з імені користувача та ідентифікатора провайдера, наприклад sip:nicholas@sipprovider.com, де sipprovider.com – провайдер SIP послуги користувача. При цьому допускають використання різноманітних параметрів, які визначають функціональність SIP-адреси або тип протоколу з’єднання. Наприклад, можна зазначити, що з’єднання здійснюється зі звичайним телефоном за номером абонента традиційної телефонної мережі – sip:tel:+999999.

SIP має кілька комплементарних протоколів, які служать для реалізації додаткових можливостей. Найбільш важливі з них – SDP (Session Description Protocol, RFC 2327), протокол узгодження таких параметрів сеансу зв’язку, як типи кодеків, номери UDP-портів, тощо. SDP підтримує зміни параметрів сеансу з’єднання "на ходу", під час сеансу. Передача повідомлень SDP базується на протоколі Session Announcement Protocol (SAP, RFC 2974).

Інший приклад комплементарного протоколу – SIMPLE (SIP for Instant Messaging and Presence Levering Extension). Фактично – це розширення SIP, яке служить для надання інформації про події (presence) і для поширення "миттєвих" повідомлень (instant messaging).

**Клієнт SIP** (SIP user agent) – це пристрій (IP-телефон, шлюз та інший користувацький термінал) або програмний додаток для ПК тощо. Зазвичай SIP-клієнт містить і клієнтську, і серверну частини (User Agent Client, або UAC, і User Agent Server, або UAS). Основні функції даного компонента – ініціювати або завершувати виклики.

**Проксі-сервер SIP** керує маршрутизацією викликів і роботою прикладної програми. Проксі-сервер не може ініціювати або припиняти виклики.

**Redirect-сервер SIP** перенаправляє дзвінки згідно з визначеними умовами.

**Сервер реєстрації SIP** (registrar/location) виконує реєстрацію користувачів і утримує базу відповідності імен користувачів їх адресам, телефонним номерам і т. ін.

З цих компонентів, як із функціональних "цеглин", можна будувати мережі VoIP довільної топології, складності і масштабу, зокрема мережі, які повністю заміщують функції сучасних АТС. Можна також створювати зовсім нові сервіси – інтеграцію Інтернет- і бізнес-додатків, програмовані служби, багатоадресний пошук абонента, мультимедійні сервіси, повідомлення про події тощо.

У найбільш загальній формі сценарій з'єднання за протоколом SIP за участі проксі-сервера наведений на рис. 10.3. Абонент надсилає до проксі-сервера запит на з'єднання за допомогою повідомлення Invite. Проксі-сервер повертає повідомлення Trying і передає повідомлення Invite абоненту, який викликається. Той, в свою чергу, відповідає повідомленням Ringing, яке проксі-сервер надсилає до сторони, яка викликає. Після того, як абонент на другому кінці з'єднання підніме слухавку, стороні, що ініціювала виклик, надсилається повідомлення ОК, яке транслюється проксі-сервером. Абоненту, що викликається, повертається повідомлення-підтвердження Ack.

З цього моменту з'єднання вважається налаштованим і починається обмін медіа-трафіком за протоколами RTP/cRTP. Сторона, яка бажає завершити з'єднання, надсилає повідомлення Bye, і після отримання підтвердження ОК, з'єднання переривається.

### *Види з'єднань, взаємодія з комп'ютерною мережею*

Виокремлюють три найбільш поширені сценарії IP-телефонії:

- комп'ютер–комп'ютер;
- телефон–комп'ютер;
- телефон–телефон.

Перший сценарій "комп'ютер–комп'ютер" реалізується на базі стандартних комп'ютерів, обладнаних мультимедійними засобами, під'єднаними до мережі Інтернет.

Компоненти сценарію "комп'ютер-комп'ютер" подані на рис. 10.4. За цим сценарієм аналогові голосові сигнали з мікрофона абонента А перетворюються в цифрову форму за допомогою аналого-цифрового перетворювача (АЦП). Далі зразки голосових даних у цифровій формі стискаються кодуючим пристроєм для скорочення смуги, потрібної для їх

передачі, у співвідношенні 4:1, 8:1 або 10:1. Вихідні дані після стиснення формуються в пакети, до яких додаються заголовки протоколів, після чого пакети передаються через IP-мережу до системи IP-телефонії, яка обслуговує абонента Б. Коли пакети приймаються системою абонента Б, заголовки протоколу видаляються, а стиснуті голосові дані потрапляють на пристрій, який відновлює їх первинну форму, після чого голосові дані знову перетворюються в аналогову форму за допомогою цифро-аналогового перетворювача (ЦАП) і надходять у динамік телефону абонента Б.

Для звичайного з'єднання між двома абонентами системи IP-телефонії на кожному кінці одночасно реалізують як функції передачі, так і функції прийому. Під IP-мережею розуміють або глобальну мережу Інтернет, або корпоративну мережу підприємства (організації) Intranet.

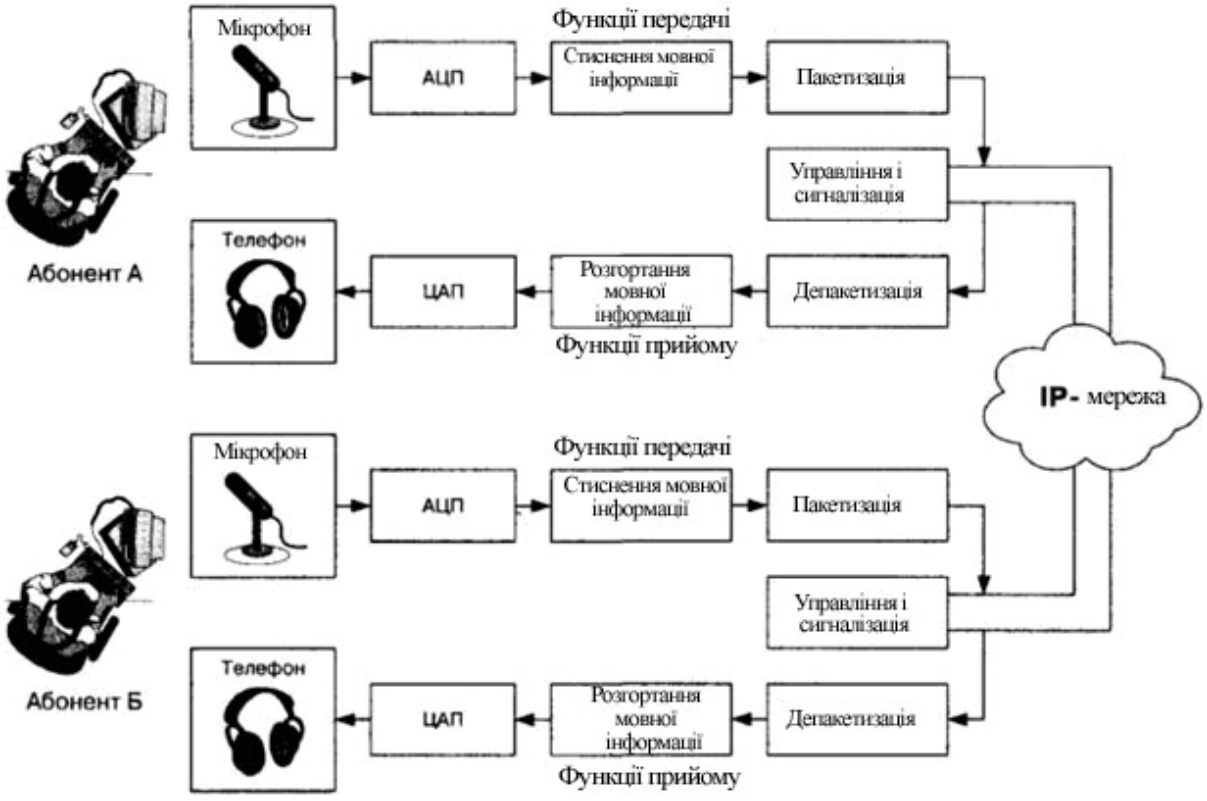



Рис. 10.4. *Сценарій IP-телефонії "комп'ютер–комп'ютер"*

Інший сценарій "телефон–комп'ютер" знаходить застосування в різних довідково-інформаційних службах Інтернет, у службах збуту товарів або технічної підтримки. Користувач, який під'єднався до веб-серверу будь-якої компанії, має можливість звернутися до оператора довідкової служби.

Третій сценарій "телефон–телефон" значною мірою відрізняється від перших двох сценаріїв IP-телефонії, оскільки він надає звичайним абонентам альтернативну можливість межміського та міжнародного телефонного зв’язку.

***Якість передачі голосової інформації по IP-мережі***

IP-телефонія є однією з областей передачі даних, де всі процеси передачі інформації повинні відбуватися в режимі реального часу і де особливо важлива динаміка передачі сигналу, яка забезпечується сучасними методами кодування і передачі інформації; в результаті збільшується пропускна здатність каналів у порівнянні з традиційними телефонними мережами.

До факторів, які впливають на якість IP-телефонії, належать:

- максимальна пропускна здатність – максимальний обсяг даних, який проходить по мережі за одиницю часу;
- затримка – проміжок часу, необхідний для передачі пакета через мережу;
- джитер – затримка між двома послідовно надісланими пакетами;
- втрата пакету – пакети або дані, втрачені при передачі через мережу.

Втрата невеликої кількості голосових пакетів вважається прийнятною і може бути компенсована за допомогою механізму кодування/декодування, а також різних методів інтерполяції мови, тобто за допомогою заповнення відсутніх звуків за допомогою DSP-технології, яка аналізує форму звукового коливання й передбачає втрачений звук.

Організація ITU-T серйозно займалася дослідженням проблем, пов’язаних із затримками при передачі голосу по мережі. У результаті був розроблений стандарт ITU-T G.114, який рекомендує, щоб затримка при передачі голосу в одному напрямку не перевищувала 150 мс. Стандарт рекомендує також розглядати затримку від 150 до 400 мс як прийнятну. У тому випадку, коли затримка перевищує 400 мс, вона стає помітною. Для порівняння можна навести спілкування через супутник: затримка при передачі по супутниковому зв’язку в одному напрямку становить приблизно 170 мс, при цьому не враховується затримка, що виникає в наземних пристроях. Стандарт також встановлює, що при передачі голосу затримка більш ніж 400 мс неприйнятна.

Можна виділити такі причини затримки при передачі мови від джерела до отримувача:

- **затримка накопичення** (іноді називається алгоритмічною затримкою): зумовлена необхідністю збору голосових кадрів у мовному

кодері. Величина затримки визначається типом мовного кодера й змінюється від невеликих величин (0,125 мкс) до одиниць мілісекунд;

• **затримка обробки**: процес кодування і збору закодованих відліків в пакети для передачі через пакетну мережу створює певні затримки. Затримка кодування або обробки залежить від швидкості роботи процесора й обробки використовуваного типу алгоритму;

• м**ережна затримка**: зумовлена фізичним середовищем і протоколами, які застосовують для передачі мовних даних, а також буферами, використовуваними для видалення джитер пакетів з боку отримувача.

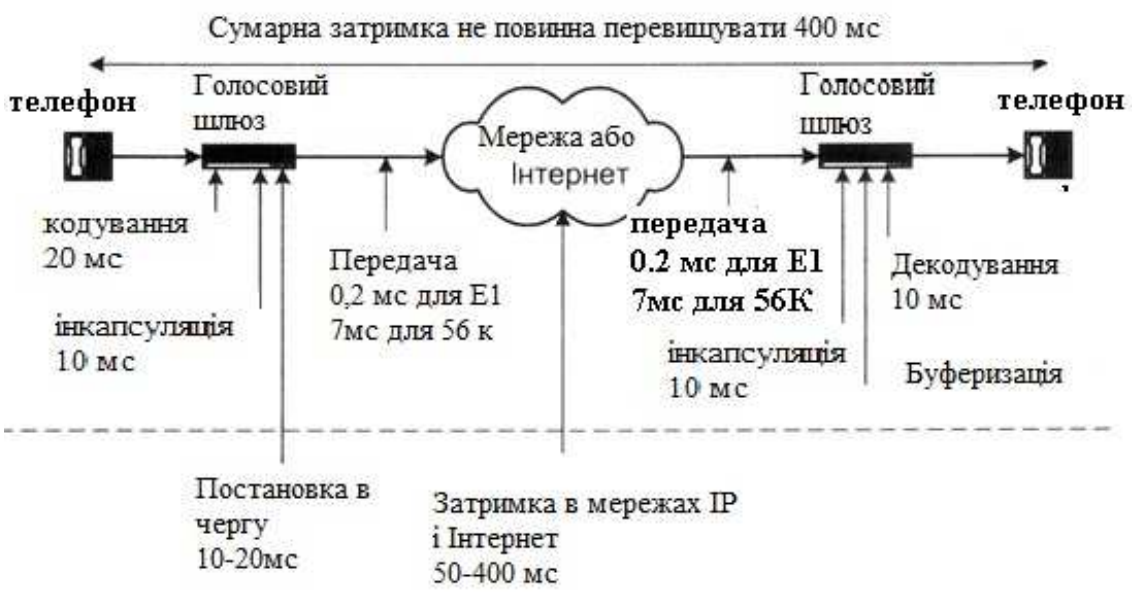



Рис. 10.5. *Джерела затримки при передачі мови по IP-мережі*

Важливо зазначити той факт, що затримки в мережах з комутацією пакетів впливають не тільки на якість передачі мовного трафіка в реальному часі. Не менш істотно, що дані затримки в певних ситуаціях можуть порушити правильність функціонування телефонної сигналізації в цифрових трактах типу E1/T1 на стику голосових шлюзів з обладнанням комутованих телефонних мереж.

Для передачі голосової інформації характерним є таке явище, як *джитер*.

Коли мова або дані розбиваються на частини для передачі через IP-мережу, пакети часто прибувають в пункт призначення в різний час і в різній послідовності. Це створює різницю часу доставки пакетів – джитер (від англ.. «jitter» – тремтіння). Джитер призводить до специфічних

порушень передачі мови, вони сприймаються як тріск і клацання. Розрізняють три форми джитера:

1) джитер, залежний від даних (Data Dependent Jitter – DDJ), відбувається у випадку обмеженої смуги пропускання або при порушеннях у роботі мережних компонентів;

2) спотворення робочого циклу (Duty Cycle Distortion – DCD), зумовлене затримкою поширення між передачею знизу вгору і згори вниз;

3) випадковий джитер (Random Jitter – RJ) є результатом теплового шуму.

Задовільними вважаються умови передачі голосових даних, коли величина джитера не перевищує 20 мс.

### *Оцінка пропускної здатності каналу голосового з'єднання*

Достатня пропускна здатність каналу зв'язку – це ключове питання, яке слід враховувати при проектуванні VoIP мереж. Величина пропускної здатності, потрібна для здійснення одного дзвінка, може суттєво змінюватися в залежності від типу кодеку та кількості голосових зразків, які передаватимуться в пакеті. Найкращий механізм кодування не гарантує високої якості передачі голосу; зокрема, чим більша компресія, тим гірша якість відтворення голосу. Проектувальники голосових мереж повинні вирішити що важливіше: краща якість голосу чи ефективне використання пропускної здатності каналу зв'язку.

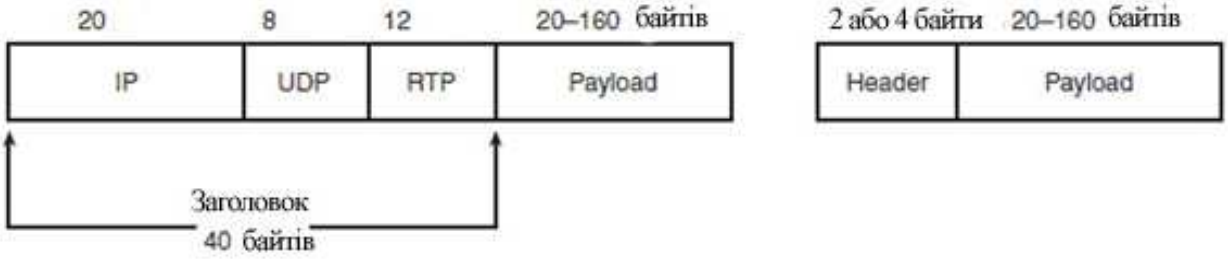
Існує дві методики зменшення надлишку голосових даних на один дзвінок, а отже, підвищення ефективності використання наявної пропускної здатності – cRTP та VAD:

**1. Стиснутий протокол RTP (Compressed Real-Time Transport Protocol, cRTP).** Всі голосові пакети інкапсулюються в IP-пакети, що складаються з двох частин: корисне навантаження, яким є голосові дані, й IP/UDP/RTP заголовки. Хоча зразки голосу стискаються і можуть мати змінний розмір залежно від кодеку, що використовується, заголовки мають однаковий розмір – 40 байтів. Якщо порівняти з голосовими зразками, розміром 20 байтів, який забезпечує кодек G.729 (табл. 10.1), заголовки створюють додатковий обсяг трафіка.

При використанні протоколу cRTP, заголовки зменшуються до 2 або 4 байтів, забезпечуючи значне заощадження пропускної здатності каналу, що особливо важливо для низькошвидкісних послідовних ліній з'єднання зі швидкістю передачі даних до 768 кбіт/с. Проте, не слід використовувати протокол cRTP для швидкісних з'єднань, оскільки використання даного

протоколу висуває значні вимоги до обладнання, через споживання ресурсів процесора.

**2. Виявлення голосової активності (Voice Activity Detection, VAD).** У середньому, близько 35 % голосових дзвінків складає тиша. У традиційних телефонних мережах, усі голосові дзвінки використовують фіксовану смугу пропускання 64 кбіт/с, незалежно від складу та насиченості розмов. При використанні VoIP, тиша також упаковується й передається, як і решта розмови. VAD вилучає такі пакети, тому надсилаються саме IP-пакети з елементами розмови. Отже, шлюзи можуть поєднувати потік даних з голосовими пакетами, ефективно використовуючи пропускну здатність мережі передачі даних.




***а*** ***б***

Рис. 10.6. *Структура голосового пакета: а – без стиснення, б – із використанням стиснення заголовка RTP*

При побудові голосової мережі смуга пропускання каналу – один з найважливіших показників, який необхідно брати до уваги, а саме яка частина пропускної здатності використовується для здійснення одного VoIP-дзвінка.

Таблиця 10.2

Параметри голосового з’єднання

| Кодек | Корисне навантаження пакета, байт | Мінімальна пропускна здатність, кбіт/с | Алгоритмічна затримка, мс |
|---|---|---|---|
| G.711 | 160 | 64 | 20 |
| G.723(6.3) | 24 | 6.3 | 37.5 |
| G.723(5.3) | 20 | 5.3 | 37.5 |
| G.726-32 | 60 | 32 | 20 |
| G.726-24 | 40 | 24 | 20 |
| G.728(16) | 40 | 16 | 3-5 |
| G.729 (8) | 20 | 8 | 25 |

У таблиці 10.2 наведено перелік кодеків та відповідні ним розміри корисного навантаження голосових пакетів і необхідна пропускна здатність.

Розглянемо приклад розрахунку пропускної здатності, необхідної для голосового сеансу зв'язку.

Дано такі умови:

- розмір заголовка IP/UDP/RTP становить 40 байтів;
- стиснення RTP-заголовка може зменшити розмір IP/UDP/RTP-заголовків до 2 або 4 байтів;
- заголовок кадру 2-го рівня додає ще 6 байтів.

Для визначення пропускної здатності, потрібної для здійснення одного голосового дзвінка, використовуються такі розрахункові формули:

1. Розмір голосового пакета, $\mathbf{Р_{ГП}}$ (байти):

$\mathbf{Р_{ГП}}$ = (Заголовок 2 рівня (байти)) + (Заголовок IP/UDP/RTP(байти)) + +(корисне навантаження пакета, $\mathbf{КН_{П}}$ (байти)).

2. Кількість голосових пакетів за секунду, $\mathbf{К_{ГПС}}$ (п/с):

$$\mathbf{К_{ГПС}} = \frac{\text{швидкість передачі даних кодека, } \mathbf{Ш_{К}} \text{ (біт/с)}}{\mathbf{КН_{П}} \text{ (біти)}}.$$

3. Пропускна здатність на дзвінок, **ПЗ** (біти/с):

$$\mathbf{ПЗ} = \mathbf{Р_{ГП}} \text{ (біти)} * \mathbf{К_{ГПС}} \text{(п/с)}.$$

Наприклад, для розрахунку пропускної здатності, необхідної для голосового з'єднання при використанні G.729 (швидкість передачі даних кодека 8-кбіт/с) з cRTP і корисним навантаженням пакета, що дорівнює за замовчуванням 20 байтів (табл. 10.2):

$\mathbf{Р_{ГП}}$ (байти) = (Заголовок 2 рівня=6 байтів) + (стиснутий заголовок IP/UDP/RTP =2 байти) + ($\mathbf{КН_{П}}$=20 байтів) =6+2+20= 28 байтів

$\mathbf{Р_{ГП}}$ (біти) = (28 байтів) * 8 бітів = 224 біти

$\mathbf{К_{ГПС}}$ = (швидкість передачі даних кодека G.729 =8 кбіт/с)/(8 бітів * $\mathbf{КН_{П}}$=20 байтів) = (8 кбіт/с)/(160 бітів) = 50 п/с

**ПЗ** = $\mathbf{Р_{ГП}}$ (224 біти) * $\mathbf{К_{ГПС}}$ (50 п/с) = 11.2 кбіт/с

**Результат:** Сеанс голосового з'єднання з використанням G.729 та cRTP вимагає пропускної здатності 11.2 кбіт/с. Цю величину в □абл.. 10.2 заокруглено до 11 кбіт/с.

## ПРАКТИЧНЕ ЗАВДАННЯ

**Мета:** *визначення параметрів голосового сеансу з'єднання*

Відповідно до номера варіанта потрібно оцінити параметри VoIP мережі з характеристиками, наведеними у табл. 10.3. Зокрема, визначте пропускну здатність, необхідну для одного дзвінка, та кількість голосових дзвінків, які можна здійснити одночасно по каналу зв'язку з наведеними показниками.

Таблиця 10.3

Показники VoIP мережі

| Варіант | Кодек | Пропускна здатність каналу зв'язку | Використання cRTP |
|---|---|---|---|
| 1. | G.711 | 768 кбіт/с | Ні |
| 2. | G 728 | 256 кбіт/с | Так |
| 3. | G.726 (24) | 1,544 Мбіт/с | Ні |
| 4. | G.726 (32) | 2048 кбіт/с | Ні |
| 5. | G.723(6.3) | 1024 кбіт/с | Так |
| 6. | G.729 | 128 кбіт/с | Ні |
| 7. | G.723(5.3) | 768 кбіт/с | Ні |
| 8. | G 728 | 512 кбіт/с | Так |
| 9. | G.711 | 256 кбіт/с | Так |
| 10. | G.726 (32) | 1024 кбіт/с | Так |

Наведіть покрокові розрахунки параметрів та обґрунтуйте отримані результати.

При оцінці Інтенет-каналу зв'язку слід звернути увагу на такі моменти. Якщо даний канал використовується не лише для IP-телефонії, але й для роботи в мережі зі звичайних комп'ютерів (перегляду сайтів, надсилання повідомлень електронної пошти, скачування файлів тощо), тоді його швидкість повинна бути ще вищою, ніж дають розрахунки (оскільки в цьому випадку і робочі станції, і голосовий шлюз повинні одночасно приймати і передавати дані).

Слід також мати на увазі, що ця необхідна пропускна здатність використовується як для прийому так і для передачі інформації. Деякі види Інтернет-підключень пропонуються різну швидкість у двох напрямках, як правило, більша швидкість завантаження. Це не дуже суттєво при використанні традиційних мережних послуг. Проте у випадку IP-телефонії з'єднання інтерактивне (на наше запитання ми одержуємо відповідь), тому необхідна достатньо велика швидкість прийому й передачі даних.

***Контрольні запитання та завдання***

1. Що таке конвергентні (змішані) мережі передачі даних. Які переваги та особливості їх проектування та обслуговування в порівнянні з традиційними комунікаційними мережами?
2. Опишіть обладнання, протоколи та процеси, які використовуються для передачі голосу по комп'ютерній мережі.
3. Що таке кодек? Які існують типи кодеків і чим вони відрізняються?
4. Порівняйте протоколи RTP та cRTP та назвіть умови їх застосування.
5. Які небажані явища виникають у комп'ютерній системі при передачі голосових даних? Чим вони викликані і як їх можна уникнути?
6. Які з наведених нижче характеристик впливають на обрання кодеку при проектуванні мережі з послугою IP-телефонії:

а) розмір заголовка голосового пакета;
б) пропускна здатність, необхідна для здійснення дзвінка;
в) якість голосового сигналу;
г) тривалість мовчання у голосових пакетах.

7. Який із наведених нижче кодеків найкраще підходить для здійснення якісного телефонного зв'язку через послідовні WAN-з'єднання з ефективним використанням пропускної здатність?

а) G.711;
б) G.723;
в) G.728;
г) G.729.

8. Затримки якої тривалості вважаються прийнятними для голосового сеансу з'єднання?
9. Наведіть порівняльну характеристику локальних і глобальних мереж.
10. Як класифікуються технології підключення до глобальних мереж? Чим відрізняються мережі передачі даних з комутацією каналів і пакетів. Які особливості їх використання?

# ПЕРЕЛІК СКОРОЧЕНЬ

**ACL** – Access Control List, *список управління доступом*
**AfricNIC** – Africa Network Information Center, *Африканський мережний інформаційний центр*
**ANSI** – American National Standards Institute, *Американський національний інститут стандартів*
**APNIC** – Asia-Pacific Network Information Center, *Азійсько-Тихоокеанський мережний інформаційний центр*
**ARIN** – American Registry for Internet Numbers, *Американьский реєстатор Інтернет-номерів*
**ARP** – Address Resolution Protocol, *протокол визначення адрес*
**AS** – Autonomous System, *автономна система*
**AUX** – auxiliary, *допоміжний*
**BDR** – Backup Designeted Router, *запасний визначений маршрутизатор*
**BIOS** – Basic input/output system , *базова система вводу-виводу*
**CIDR** – Classfull Interdomain Routing, *безкласова міждомена маршрутизація*
**CPU** – Central Processing Unit, *центральний процесор*
**cRTP** – Compressed Real-Time Transport Protocol, *стиснутий транспортний протокол реального часу*
**CSMA/CD** – Carrier Sense Multiply Access with Collision Detection, *метод багаторазового доступу до середовища з прослуховуванням несучої для виявлення колізій*
**CSU/DSU** – channel service unit/data service unit, *пристрій обслуговування каналу/пристрій обслуговування даних*
**D** – D
**DNS** – Domain Name Server, *сервер доменних імен*
**DR** – Designated Router, *визначений маршрутизатор*
**DTE** – Data Terminal Equipment, *кінцевий пристрій даних*
**EIA** – Electronic Industries Alliance, *Альянс електронної промисловості*
**Fa** – Fast Ethernet, інтерфейс
**FTP** – File Transfer Protocol, *протокол передачі даних*
**HTML** – HyperText Markup Language, *мова розмітки гіпертексту*
**HTTP** – Hypertext Transfer Protocol, *протокол передачі гіпертекстових повідомлень*
**IANA** – Internet Assigned Numbers Authority, *Адміністрація адресного простору Інтернет*
**ICMP** – Internet Control Message Protocol, *протокол міжмережних*

*керуючих повідомлень*

**IEEE** – Institute of Electrical and Electronics Engineers, *Інститут інженерів з електротехніки та електроніки*

**InterNIC** – Internet Network Information Center, *Інформаційний центр Інтернет-мережі*

**IOS** – Internetwork Operating System, *міжмережна операційна система*

**IP** – Internet Protocol, *міжмережний протокол*

**IPv6** IP version 6, протокол IP версії 6

**ISO** – International Organization for Standardization, *Міжнародна організація із стандартизації*

**ISP** – Internet Service Provider, *провайдер Інтернет-послуги*

**LACNIC** – Latin America and Caribbean Network Information Centre, мережний інформаційний центр

**LAN** – Local Area Network, *локальна мережа*

**Lo** – Loopback interface, *інтерфейс зворотньої петлі*

**LSA** – Link-state Advertisement, *повідомлення про стан каналу*

**MAC** – Media Access Control, *контроль доступу до середовища*

**NAT** – Network Address Translatio, *трансляція мережних адрес*

**NIC** – Network interface card, *мережна карта*

**NVRAM** – Non-volatile random access memory, *енергонезалежна пам'ять*

**OSI** – Open System Interconnection, *Еталонна модель взаємодії відкритих систем*

**OSPF** – Open Shortest Path First, *перший відкритий протокол найкоротшого шляху*

**PDU** – Protocol Data Unit, *протокольний блок даних*

**POST** – Power-On Self Test, *самотестування при запуску*

**RAM** – Random Access Memory, *оперативна пам'ять*

**RIP** – Routing Information Protocol, *протокол маршрутизації даних*

**RIPE** – фр. Réseaux IP Européens(англ. Network Coordination Centre), *мережний координаційний центр*

**RJ** – Registered jack, *зареєстроване рознімання*

**ROM** – Read-Only Memory, *постійний запам'ятовуючий пристрій*

**RTP** – Real-Time Transport Protocol, *транспортний протокол реального часу*

**SDP** – Session Description Protocol, *протокол опису сеансу*

**SIMPLE** – SIP for Instant Messaging and Presence Levering Extension, *протокол відкриття сеансу зв'язку, призначений для систем миттєвих повідомлень і*

*повідомлення про присутність*

**SIP** – Session Initiation Protocol, *протокол відкриття сеансу зв'язку*

**SMTP** – Simple Mail Transfer Protocol, *простий протокол передачі повідомлень електронної пошти*

**SNMP** – Simple Network Management Protocol, *простий протокол управління мережею*

**SPF** – Shortest Path First, *перший алгоритм найкоротшого шляху*

**TCP** – Transport Control Protocol, *протокол контролю передачі даних*

**TFTP** – Trivial File Transfer Protocol, *простий протокол передачі файлів*

**TIA** – Telecommunications Industry Association, *Асоціація телекомунікаційної промисловості*

**UDP** – User Datagram Protocol, *протокол користувацьких блоків даних*

**VAD** – Voice Activity Detection, *виявлення голосової активності*

**VLAN** – Virtual Local Area Network, *віртуальна локальна мережа*

**VLSM** – Variable Length Subnet Mask, *підмережі з масками змінної довжини*

**VoIP** – Voice over IP, *передача голосу через IP-мережу*

**VTY** – Virtual terminal lines, *віртуальні термінальні лінії*

**WAN** – Wide Area Network, *глобальна мережа*

**WWW** – World Wide Web, *всесвітня мережа*

**АПД** – апаратура передачі даних

**АС** – автономна система

**ОС** – операційна система

**ПК** – персональний комп'ютер

**ЦП** – центральний процесор

# СПИСОК ЛІТЕРАТУРИ


1. Кулаков Ю.А. Компьютерные сети. Выбор, установка, использование и администрирование: учебное пособие / Кулаков Ю.А., Омелянский С. В. – К. : Юниор, 1999. – 544 с.
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник / Олифер В.Г., Олифер Н.А – СПб. : Питер, 2006. – 958 с.
3. Олифер В.Г. Новые технологии и оборудование IP-сетей / Олифер В.Г., Олифер Н.А. – СПб. : БХВ –Петербург, 2001. – 512 с.
4. Амато В. Основы организации сетей Cisco : в 2 т. : пер. с англ. / Амато В. – М. : Вильямс, 2002.
5. Комп’ютерні мережі: конспект лекцій / укл. : Омельянюк Н.В., Танасюк Ю.В. – Чернівці : Рута, 2007. – 140 с.
6. Технології комп’ютерних мереж: навчальний посібник / укл.: Танасюк Ю.В. – Чернівці : ЧНУ, 2010. – 100 с.
7. Хабракен Д. Как работать с маршрутизаторами Cisco : пер. с англ. / Хабракен Д. – М. : ДМК Пресс, 2005. – 320 с.
8. Хелеби С. Принципы маршрутизации в Internet : пер. с англ. / Хелеби С., Мак-Ферсон Д. – М. : Вильямс, 2001. – 448 с.
9. Шиндер Д. Л. Основы компьютерных сетей.: пер. с англ. / Шиндер Д. Л. – М. : Вільямс, 2003. – 656 с.
10. Леинванд А. Конфигурирование маршрутизаторов Cisco : пер. с англ., 2-е изд. / Леинванд А., Пински Б. – М. : Вильямс, 2001. – 368 с.
11. Конахович Г. Ф. Сети передачи пакетных даннях / Конахович Г. Ф., Чуприн В. М. – К. : МК-Пресс, 2006. – 272 с.
12. Столлингс В. Современные компьютерные сети / Столлингс В. – СПб. : Питер, 2003. – 783 с.
13. Корпорация Cisco Systems Программа сетевых академий Cisco CCNA1, CCNA2. Вспомагательное руководство : пер. с англ. – М. : Вильямс, 2005. – 1168 с.
14. Sportack M. A. IP Addressing Fundamentals / Sportack M. A. – Cisco Press, 2002. – 368 p.

*Навчальне видання*

# МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

*Навчальний посібник*

Укладач ***Танасюк Юлія Володимирівна***

Відповідальний за випуск ***С.В. Мельничук***

Літературний редактор ***О.В. Колодій***

*Реєстраційне свідоцтво ДК №891 від 08.04.2002 р.*

Підписано до друку ..... Формат 60 х 84/16
Папір офсетний. Друк Офсетний. Ум. друк. арк.
Обл.-вид. арк. Зам. Тираж
Друкарня видавництва „Рута” Чернівецького національного університету
58012, Чернівці, вул.. Коцюбинського, 2