Міністерство освіти і науки України
Чернівецький національний університет
імені Юрія Федьковича

Л. І. Д'яченко

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Навчально-методичний посібник з лабораторних робіт

(видання електронне)

Чернівці
Чернівецький національний університет

2022

УДК 004.42(078)
Д674

Друкується за ухвалою
Вченої ради навчально-наукового інституту фізико-технічних та комп’ютерних наук
Чернівецького національного університету
імені Юрія Федьковича
Протокол № 8 від 22.09.2022 р.

Д’яченко Л.І.
Д674 Програмне забезпечення мережевих технологій: навч.-метод. посіб. лаб. роб. / Л. І. Д’яченко. – Чернівці: Чернівецький нац. ун-т, 2022. – 68 с.

Навчально-методичний посібник з лабораторних робіт містить теоретичні матеріали та покрокові завдання, що мають за мету навчити студентів проводити початкове налаштування проміжних мережевих пристроїв (комутаторів та маршрутизаторів), протоколів динамічної маршрутизації, створювати та налаштовувати віртуальні мережі та обмежувати доступ за допомогою списків керування доступом.

Для студентів вищих навчальних закладів, які навчаються за спеціальностями 121 - Інженерія програмного забезпечення, 122 – Комп’ютерні науки та суміжними.

УДК 004.42(078)

ЗМІСТ

ВСТУП

Розвиток локальних комп'ютерних мереж для об'єднання комп'ютерів починався з використанням найрізноманітніших не стандартизованих пристроїв і програмного забезпечення. Створення мережі в цей час вимагало від розробників великих зусиль і винахідливості. В середині 80-х років ситуація почала кардинально змінюватися в сторону створення стандартних технологій об'єднання комп'ютерів в єдину мережу. Були розроблені спеціальні методи і правила обміну інформацією між комп'ютерами, серед яких найбільш відомими стали стандарти Ethernet, Token Ring, FDDI, Arcnet. У зазначених стандартах були строго регламентовані довжина, вид і порядок проходження кодів, що посилаються комп'ютерами в мережу, правила доступу до мережі окремими комп'ютерами і т.д. Крім цього в цей час інтенсивно почали використовуватися динамічні протоколи маршрутизації. Розроблені стандартні мережеві технології, а так само використання персональних комп'ютерів значно спростили процес створення комп'ютерних мереж. З'явилася можливість швидкого доступу до поділюваних обчислювальних ресурсів, до бази даних відразу декількома користувачами, причому користувач використовував на своєму мережевому комп'ютері ті ж знайомі команди, як і при роботі з окремим комп'ютером. Завдання обробки цих команд і розподілу завдань між окремими комп'ютерами взяла на себе мережева операційна система.

Лабораторних практикум складається з дев’яти лабораторних робіт, які охоплюють налаштування основних протоколів маршрутизації, списків керування доступом та інших важливих характеристик проміжних мережевих пристроїв.

ЛАБОРАТОРНА РОБОТА №1
Початкове налаштування маршрутизатора

Мета: Навчитися налаштовувати основні параметри маршрутизатора з використанням CLI у середовищі моделювання Cisco Packet Tracer.

Теоретичні відомості

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 трафіку. Використовуючи протоколи маршрутизації, маршрутизатори приймають рішення про перенаправлення даних по мережі.

Інтерфейси

Інтерфейси 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 підключення маршрутизатора до глобальної мережі. Крім зазначених типів інтерфейсів існують також порти призначені для налаштування параметрів маршрутизатора **(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.

Призначення елементів маршрутизатора (рис. 1.1):

1. Перемикач ввімкнення/вимкнення.
2. Слот модуля WIC 1 (WAN Interface Card).
3. Індикатор стану WIC1.
4. Індикатор роботи апаратного забезпечення VPN.

Рис. 1.1. *Елементи задньої панелі маршрутизатора Cisco 1841*

5. Консольний порт.
6. AUX (auxiliary) порт (допоміжний).
7. 10/100 Mbps Ethernet порт.
8. Індикатори роботи порту Ethernet.
9. Слоти розширення.
10. Індикатор стану послідовних портів.
11. Сокет для ключа (з його допомогою можна підвищити фізичну безпеку пристрою).

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

Таблиця 1.1.

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

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:

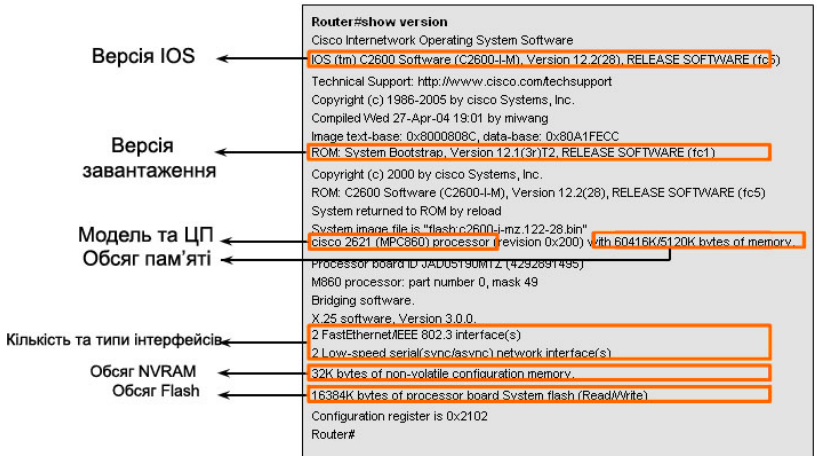
- **режим конфігурації інтерфейсу `Router(config-if)#`:**

```
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)#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 настройку 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 переходу зі певного специфічного режиму конфігурації назад у глобальний режим конфігурації використовується команда `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;



- `show ARP` – ARP-таблицю маршрутизатора;
- `show protocol` – глобальні та специфічні для кожного інтерфейсу параметри настройки протоколів мережного рівня;
- `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
```

Хід роботи

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.

Для виконання даної лабораторної роботи використовуємо середовище моделювання Cisco Packet Tracer.

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

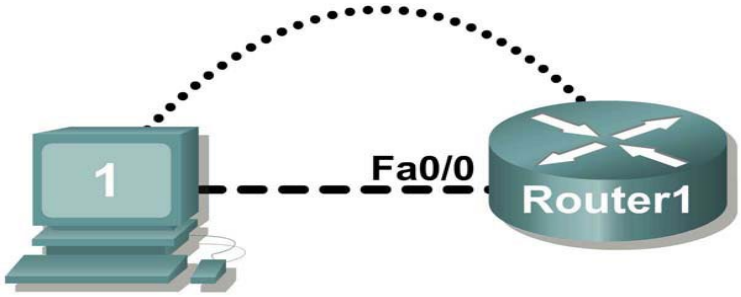


Рис. 1.2. *Схема з’єднання пристроїв*

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

Будуємо пропоновану схему в середовищі Cisco Packet Tracer, заходимо на комп’ютер, відкриваємо вкладку ***terminal***, залишаючи значення вказані за замовчуванням, підключаємось до маршрутизатора для здійснення налаштувань.

Налаштування параметрів маршрутизатора

Коли на маршрутизаторі відсутні початкові налаштування, IOS запропонує користувачеві увійти в режм початкових налаштувань. На екрані з’являється питання:

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

Оскільки на лабораторних роботах, ми не будемо використовувати цей режим для налаштування маршрутизатора, вводимо «**no**». Якщо випадково ввести «**yes**» і увійшли 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`.

Налаштування імені маршрутизатора

Перейдіть до режиму глобальної конфігурації:

```
Router# configuration terminal
Router(config)#
```

Зауважте, що команди можна записувати скорочено, натискаючи для їх продовження клавішу **TAB**.

Змініть ім’я маршрутизатора за власним бажанням, наприклад:

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

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.

Налаштування паролю на перехід до привілейованого режиму

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

Як вже 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 файлу.

Встановіть пароль **cisco** на привілейований режим.

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

Налаштування паролю 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 таблиці 1.2 налаштуємо на консолі пароль **class**.

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

Налаштування паролю 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**.*

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
```

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**.

Перегляд налаштувань

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

Перегляньте поточні налаштування за допомогою команди:

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

Для перевірки стану саме інтерфейсів маршрутизатора виконайте команду:

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

Збереження налаштувань

Оперативна пам'ять втрачає свій вміст після вимкнення живлення, тому 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]
```

Після успішного збереження параметрів налаштування, перезавантажте маршрутизатор:

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

Налаштування параметрів комп'ютера

Слід налаштувати мережні параметри робочої станції для мережі з адресою 10.0.0.0/24.

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

Контрольні запитання та завдання

1. Які існують типи конфігураційних файлів маршрутизатора? Де вони зберігаються?

2. Який кабель з'єднує консольний порт маршрутизатора та COM-порт комп'ютера? Як його можна виготовити?

3. За допомогою команди **`show version`** визначте:

а) версію IOS;

б) модель маршрутизатора та тип процесора;

в) загальний обсяг оперативної пам'яті;

г) загальний обсяг енергонезалежної пам'яті;

д) обсяг флеш-пам'яті.

4. Яка команда дає повну інформацію про обсяг і вміст флеш-пам'яті. Застосуйте її для визначення назви файлу Cisco IOS та його розміру.

5. Який статус повинен мати інтерфейс для успішної передачі даних?

6. Які існують способи захисту маршрутизатора і як їх можна реалізувати за допомогою команд Cisco IOS?

7. Як переглянути поточні налаштування маршрутизатора?

ЛАБОРАТОРНА РОБОТА №2
Вивчення роботи протоколу DHCP

Мета: навчитися проводити налаштування протоколу DHCP на маршрутизаторах та виправляти помилки в роботі даного протоколу.

Завдання:

1. Налаштувати протокол DHCP на маршрутизаторі та сервері.
2. Продемонструвати їх роботу та можливі проблеми.
3. Показати шляхи вирішення проблемних ситуацій в роботі даного протоколу.
4. Відповісти на контрольні запитання

Теоретичні відомості

Протокол DHCP (dynamic host configuration protocol) - це наступник BOOTP у великих гетерогенних мережах. Він дозволяє повністю автоматизувати процес отримання IP- адреси; адміністратору залишається лише вказати межі використовуваних IP-адрес. При використанні цього протоколу вся мережева конфігурація може бути отримана у одному повідомленні.

DHCP працює по клієнт-серверній технології. Під час завантаження системи клієнт надсилає DHCP- серверу запит на отримання IP-адреси. DHCP-сервер у відповідь надсилає повідомлення, яке містить IP- адресу клієнта та інші параметри мережі.

У якості транспортного протоколу DHCP використовує протокол UDP. Цей протокол є досить розповсюдженим і зручним у використанні; більшість виробників впроваджують його підтримку у своїх продуктах.

Найчастіше проблеми, пов'язані з DHCP, полягають в призначенні неправильної IP адреси. Наприклад, припустимо, що ваш сервер DHCP був налаштований на використання інтервалу IP адрес з 192.168.0.1 по 192.168.50. Вам слід очікувати, що мережному комп'ютеру буде присвоєно IP адресу з цього інтервалу. Тепер припустимо, що робоча станція у вашій мережі почала зазнавати проблеми при зверненні до інших мережевих серверів. Вам необхідно використовувати команду IPCONFIG / ALL для того, щоб побачити мережеву конфігурацію і IP адреси. Замість адреси з очікуваного інтервалу адрес ми бачимо, що робочій станції було присвоєно адресу, що починається з 169.254. Так що ж сталося? Якщо комп'ютеру у вашій мережі несподівано було присвоєно адресу, що починається з 169.254, то ви можете бути абсолютно впевнені, що ця адреса була присвоєна не вашим DHCP сервером. Сталося так, що ваша робоча станція не змогла з'єднатися з сервером DHCP сервером. Якщо таке відбувається, що робоча станція сама призначає собі IP адресу, за допомогою засобу Windows під назвою Automatic Private IP Addressing (APIPA або автоматична адресація).

Microsoft вмонтував автоматичну адресацію в операційну систему Windows в якості допомоги тим, хто використовує дуже маленькі мережі. Наприклад, якщо ви створили невелику мережу Windows, то вам не потрібно

вручну настроювати IP адреси, навіть якщо немає сервера DHCP в мережі. APIPA допоможе вам автоматично привласнити унікальну адресу класу B кожній машині в мережі. Це чудово для невеликих домашніх мереж, але абсолютно непридатно для великих мереж. Якщо робоча станція скористалася послугами APIPA, то це означає, що на її запит на отримання IP адреси не прийшло відповіді. Причин виникнення такої ситуації може бути кілька. Якщо ви знаєте, що всі інші комп'ютери у вашій мережі нормально запитують IP адресу у вашого DHCP сервера, то ви можете зробити висновок, що причиною проблеми є не DHCP сервер.

Більш ніж імовірно, проблема пов'язана з мережевим апаратним забезпеченням, яке встановлено на робочій станції. Наприклад, для карти мережного інтерфейсу використовується неправильна драйвер. Інша можлива причина може полягати в тому, що мережевий кабель не підключений з іншого боку до перемикача.

Звичайно, тільки те, що один комп'ютер не може отримати IP адресу, зовсім не означає, що наш сервер є джерелом проблеми. Якщо інші робочі станції успішно отримують IP, то ви можете бути впевнені, що сервер працює правильно. Однак, може виникнути така ситуація, що сервер вичерпав ліміт IP адрес, які він може призначити клієнтам. Ви можете легко виявити таку проблему, порівнявши кількість адрес, що входять в інтервал, виділений для сервера DHCP, з кількістю пристроїв, які запитують IP адресу у сервера DHCP.

Якщо кілька робочих станцій мають проблеми з отриманням IP адрес, то скоріш за все проблема полягає в самому DHCP сервері. Якщо ви підозрюєте, що проблеми викликає DHCP сервер, то ви можете перевірити це за допомогою декількох простих тестів на перевірку з'єднання (ping test) і доступність сервера DHCP по мережі.

Якщо сервер DHCP може зв'язатися з іншими комп'ютерами в мережі, то рекомендується перевірити, що серверу DHCP присвоєно IP адресу, і що ця адреса сумісна з тим інтервалом адрес, для якого цей сервер налаштований присвоювати адреси для робочих станцій. Наприклад, якщо інтервал адрес, які сервер DHCP присвоює робочих станцій, варіюється з 192.168.0.1 до 192.168.0.50, то сервер не зможе привласнювати адреси робочим станціям до тих пір, поки йому самому не буде привласнений статичний адресу в тому ж самому сегменті підмережі, наприклад, 192.168.0.0 або 192.168.0.51.

Якщо це як і раніше не допомагає вирішити проблему, то рекомендується перевірити основи. Наприклад, ви повинні переконатися, що сервер DHCP все ще авторизований Active Directory для роздачі IP адрес. Ви повинні також перевірити, що цей інтервал активний, і що всі необхідні служби запущені на сервері DHCP.

Інша проблема полягає у конфлікті IP адрес які динамічно розподіляються. Коли ви створюєте DHCP пул, то сервер DHCP відповідає за те, щоб адреси всередині інтервалу були унікальні для кожної машини. Якщо це дійсно так, то звідки ж виникає конфлікт динамічних адрес?

Проблема з конфліктом адрес виникає, коли використовуються кілька DHCP серверів, і ці сервера DHCP мають пересічні пули адрес. Якщо у вас тільки один сервер DHCP у вашій мережі, то не робіть помилки, і не виключайте можливість виникнення такої ситуації у вашій мережі. Є ймовірність того, що у вашій мережі з'явився піратський (rogue) DHCP сервер, який конфліктує з вашим основним сервером DHCP.

Операційні системи Windows 2000 Server і Windows Server 2003 спроектовані таким чином, щоб уникнути проблем з піратськими (rogue) DHCP серверами. У них сервер DHCP може привласнювати IP адреси лише після того, як він був авторизований Active Directory. Але проблема полягає в тому, що це може бути застосовано лише для серверів DHCP, які працюють на платформі Windows. Сервера DHCP, що працюють на інших операційних системах можуть привласнювати IP адреси клієнтам без необхідності бути авторизованими Active Directory.

Так чи існує яка-небудь складність установки піратського сервера DHCP, який працює на платформі Linux? Ймовірно, немає. Набагато більш ймовірне пояснення полягає в тому, що вашою проблемою є бездротова точка доступу, або маршрутизатор. Такі пристрої практично завжди мають вбудований DHCP сервер. Ці пристрої зазвичай використовують інтервал адрес з 192.168.0.x або 192.168.1.x. Якщо так сталося, що цей же самий інтервал IP адрес використовується на вашому основному DHCP сервері, що тоді ви зіткнетеся з ситуацією, коли обидва сервера DHCP присвоюють адреси з одного і того ж інтервалу, що призводить до конфлікту.

Базове налаштування DHCP на маршрутизаторі Cisco

Розглянемо найпростіший випадок, коли на маршрутизаторі конфігурується один пул адрес і сервер знаходиться в тому ж широкомовному домені, що й клієнти:

! в режимі глобальної конфігурації визначимо адреси, які будуть виключені з пулу, в даному випадку це адреси 192.168.13.1 і 192.168.13.10 ... 192.168.13.15

ip dhcp excluded-address 192.168.13.1

ip dhcp excluded-address 192.168.13.10 192.168.13.15

! створимо пул адрес з ім'ям lan_pool1

ip dhcp pool lan_pool1

! визначимо підмережу, з якої будуть видаватися адреси

network 192.168.13.0/24

! визначимо адресу шлюзу за замовчуванням

ip default-router 192.168.13.1

! визначимо адреси DNS-серверів

dns-server 192.168.13.10 192.168.13.11

! визначимо ім'я домену

domain-name example.ua

! визначимо час оренди адреси 5 днів (по-замовчуванню 1 день)

lease 5

При такій конфігурації сервер видаватиме адреси тільки тим клієнтам, запит від яких прийшов через інтерфейс, адреса якого знаходиться в тій же мережі, що і сконфігурованих пул.

Хід роботи

1. Сконфігуруйте DHCP протокол на маршрутизаторі, використовуючи середовище моделювання Cisco Packet Tracer.
2. Підключіть до маршрутизатора декілька комп‘ютерів, використовуючи свіч, введіть в їх мережевих налаштування автоматичне отримання IP адреси та перевірте роботу DHCP, використовуючи команду ipconfig.
3. Підключіть до одного з вільних портів свіча сервер та налаштуйте на ньому ще один DHCP сервер.
4. Промоделюйте виникнення описаних вище проблемних ситуацій у використанні DHCP протоколу.
5. Поясніть шляхи вирішення проблем у використанні DHCP протоколу.

Контрольні запитання

1. Для чого призначений протокол DHCP?
2. Які ще протоколи динамічної адресації Ви знаєте?
3. В чому переваги та недоліки кожного протоколу динамічної адресації.
4. Що таке мережевий пул?
5. За допомогою якої команди можна перевірити чи правильні мережеві налаштування отримав локальний комп‘ютер при використанні динамічної адресації?
6. Які проблеми можуть виникати при роботі з DHCP протоколом? Як їх вирішити?

ЛАБОРАТОРНА РОБОТА №3
Налаштування статичних маршрутів

Мета: навчитися проводити налаштування статичних маршрутів.

Завдання:

1. Налаштувати статичні маршрути у схемі за заданою топологією.
2. Продемонструвати таблицю маршрутизації.
3. Продемонструвати таблицю хостів.
4. Пропінгувати кожен інтерфейс всіх маршрутизаторів топології.
5. Відповісти на контрольні запитання

Теоретичні відомості

Для конфігурування статичних маршрутів між маршрутизаторами необхідно спочатку відповідним чином налаштувати IP-адреси з'єднаних інтерфейсів. Це робиться з допомогою наступних команд:

```
Router# configure terminal
Router(config)# interface fastethernet 0
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# description This is int FE0 of router Lab_A
Router(config-if)# exit
```

При конфігуруванні послідовних інтерфейсів слід пам'ятати про те, що один з маршрутизаторів обов'язково повинен бути сконфігурований як DCE-пристрій. На його інтерфейсі слід задати тактову частоту наступною командою:

```
Router(config-if)# clock rate 56000
```

Після того, як всі інтерфейси маршрутизаторів сконфігуровано, можна переходити до настройки маршрутів між ними.

Статичний маршрут встановлюється наступною командою, яка вводиться у глобальному режимі конфігурації:

```
Router(config)# ip route <destination network><mask><next hop|outgoing interface><administrative distance>
```

У цій команді використовуються наступні параметри:

Destination network – мережа, для якої призначені пакети

Mask – маска мережі

Next hop – IP-адреса наступного інтерфейсу

Outgoing interface – ідентифікатор вихідного інтерфейсу

Administrative distance – адміністративна відстань

Після введення машрутів для ВСІХ мереж, які існують у певній топології, можна перевірити таблицю маршрутизації наступною командою:

```
Router# show ip route
```

Для того, щоб не використовувати для зв'зку з іншими маршрутизаторами лише IP-адреси, використовуються імена вузлів. Заповнення таблиці імен проводиться наступними командами:

```
Router(config)#ip host <name><address list>
```

Name – ім’я маршрутизатора, який вноситься у таблицю імен
Address list – список IP-адрес його інтерфейсів.

Якщо в якості параметра команди ping використовується не IP-адреса конкретного інтерфейсу маршрутизатора, а його ім’я, то звернення відбувається за тією адресою, яка стоїть першою у списку, потім – друга, і т.д.

Хід роботи

Практична частина цього розділу передбачає налаштування основних параметрів маршрутизаторів, створення статичних маршрутів, перевірку з’єднання між усіма пристроями мережі. Схема мережі для налаштувань зображена на рис. 3.1. Параметри налаштувань подано в таблиці 3.1.

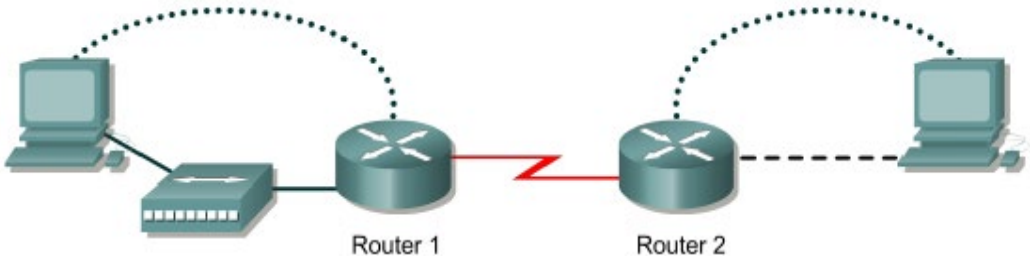


Рис. 3.1. *Топологія мережі для налаштування*

1. З’єднайте пристрої за вказаною схемою.

Таблиця 3.1

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	Kyiv	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. Змініть імена маршрутизаторів.

3. Налаштуйте на маршрутизаторах відповідні паролі на консольне з'єднання, привілейований режим та віртуальні термінальні лінії.

4. Налаштуйте параметри інтерфейсів обох маршрутизаторів.

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

5. Збережіть конфігурацію.

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

6. Перевірте наявність зв'язку.

Використайте команду **ping** для перевірки наявності з'єднання між пристроями та інтерфейсами.

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

Перегляньте стан інтерфейсів маршрутизатора, з якими відсутній зв'язок.

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

Перегляньте мережі, з якими може з'єднуватися маршрутизатор.

Для кожного маршрутизатора наведіть вміст таблиці маршрутизації.

7. Налаштуйте статичні маршрути.

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.

Для кожного маршрутизатора заповніть табл. 3.2, внісши туди відповідні параметри для налаштування статичних шляхів.

Таблиця 3.2

Параметри віддалених мереж

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

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

Перегляньте таблиці маршрутизації на кожному шлюзі.

8. Протестуйте параметри з'єднання.

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

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

Встановіть з’єднання по протоколу **telnet** з одним із маршрутизаторів.

Контрольні запитання

1. Що таке адміністративна відстань? Для чого вона використовується?
2. Для чого встановлювати параметр тактової частоти на DCE-стороні послідовного з’єднання?
3. За якими показниками обирається оптимальний шлях передачі даних по мережі?
4. Які переваги та недоліки використання статичних маршрутів?
5. Які існують способи перегляду активних маршрутів на робочій станції та маршрутизаторі?

ЛАБОРАТОРНА РОБОТА №4

Налаштування динамічного протоколу маршрутизації RIP

Мета: навчитися проводити налаштування динамічних маршрутів та протоколу маршрутизації RIP.

Завдання:

1. Налаштувати динамічні маршрути у схемі за заданою топологією.
2. Продемонструвати таблицю маршрутизації.
3. Продемонструвати таблицю хостів.
4. Пропінгувати маршрути між всіма комп'ютерами топології.
5. Відповісти на контрольні запитання

Теоретичні відомості

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 і 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 відтані та напрямку. Відстань визначається за допомогою метрики, такої як кількість проміжних вузлів, а напрямком є інтерфейс сусіднього маршрутизатора (шлюза) 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 не є ефективним, оскільки обновлення не лише споживають пропускну здатність каналу передачі даних, але й ресурси маршрутизатора, зокрема його ЦП для обробки інформації, яка надходить

Одним з 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 становить 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.

Налаштування та перевірка роботи протоколу маршрутизації RIP

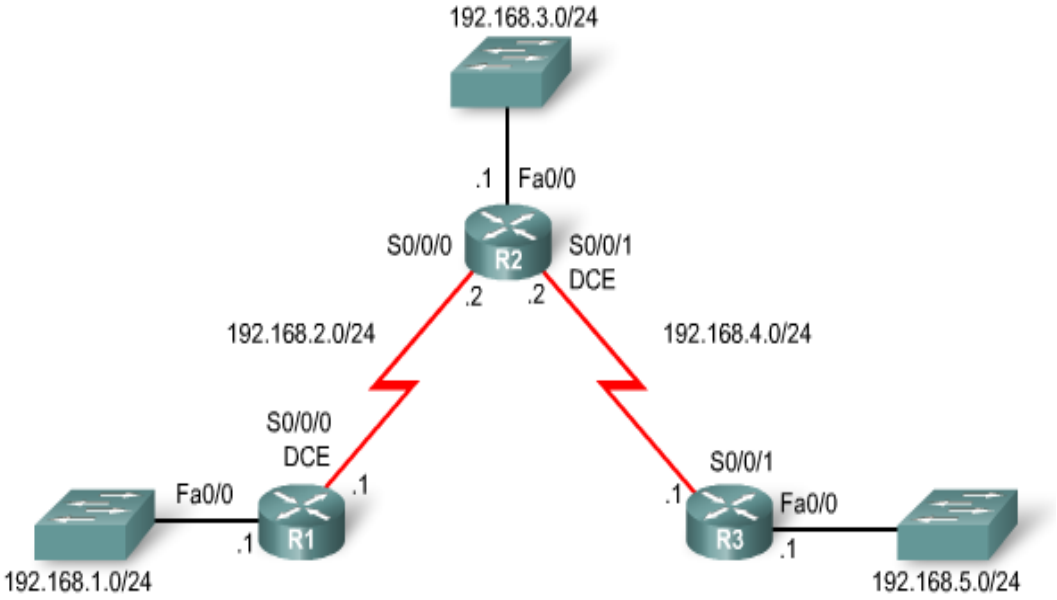


Рис. 4.1.

Налаштування та перевірка роботи протоколу маршрутизації RIP

До конфігурування будь-якого динамічного протоколу маршрутизації можна переходити після налаштувань відповідним чином 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 10.1.0.0**

R1(config-router)#**network 10.2.0.0**

Зауважте, що 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.

Отже, подібні налаштування необхідно виконати на кожному маршрутизаторі в системі, вказавши відповідні під'єднані мережі.

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

Перевірка маршрутизації RIP.

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

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

R <адреса віддаленої мережі>/<маска> [адмін.відстань/метрика] via <IP-адреса шлюза> <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:

- який протокол маршрутизації налаштований

- часові параметри протоколу

- інтерфейси, які беруть участь в розсиланні та отриманні обновлень

- які мережі 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 і 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 в 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

Зауважте, що надсилання усіх повідомлень-обновлень виконується за широкомовною адресою 255.255.255.255.

Вивід команди **debug** показав, що R1 отримує обновлення від R2. Зауважте, що це обновлення містить мережі, які не під'єднані до маршрутизатора R1. Не зважаючи на те, що інтерфейс FastEthernet0/0 не під'єднаний до іншого маршрутизатора, але 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 є небезпечною, 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 та 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, проте долучивши мережу, до якої він належить, до таблиці маршрутів і обновлень, використовується команда **passive-interface** <назва інтерфейса> <номер інтерфейса>

В режимі налаштування протоколу маршрутизації використовуйте команду у 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 в реальному часі можна за допомогою команди:

R1#**undebug all**

All possible debugging has been turned off

Хід роботи

1. З’єднайте пристрої за наведеною схемою на рис 4.1.
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 вірному 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 маршрутизаторів.
5. Налаштуйте роботу динамічного протоколу маршрутизації RIP у системі.
На кожному маршрутизаторі налаштуйте протокол маршрутизації RIP і вкажіть мережі, інформацію про які необхідно поширити по мережі.

6. Перевірте виконані налаштування маршрутизації RIP. Перегляньте таблиці маршрутизації. Порівняйте отримані дані з початковими таблицями маршрутизації.

Контрольні запитання

1. Які переваги динамічної маршрутизації?
2. Які переваги дистанційно-векторних протоколів маршрутизації?
3. Чому,не зважаючи на те, що у команді network маски не вводяться, у таблиці маршрутизації відображаються класові маски?
4. Яка за замовчуванням адміністративна відстань протоколу RIP?
5. Як можна дізнатися, коли був отриманий останній апдейт від сусіда і коли очікується наступний?
6. Яку проблему дозволяє вирішити команда passive-interface? Як її використовують?
7. Як маршрутизатори в системі дізнаються про недосяжність деякої мережі? Які засоби допомагають виявити та уникнути поширення помилкової інформації про маршрути?
8. Що таке балансування навантаження і як воно реалізоване у протоколі RIP.

ЛАБОРАТОРНА РОБОТА № 5.

Налаштування динамічного протоколу маршрутизації RIPv2.

Мета: навчитися проводити налаштування динамічних маршрутів та протоколу маршрутизації RIPv2. Дізнатися про основні відмінності між двома версіями протоколу RIP.

Завдання:

1. Налаштувати динамічні маршрути у схемі за заданою топологією.
2. Продемонструвати таблицю маршрутизації.
3. Пропінгувати маршрути між всіма комп'ютерами топології.
4. Відповісти на контрольні запитання

Хід роботи

У даній лабораторній роботі необхідно з'єднати пристрої у мережу за схемою, наведеною на рис. 5.1, виконати основні налаштування маршрутизаторів та робочих станцій (табл. 5.1) перевірити проведені налаштування та роботу протоколу маршрутизації RIPv2.

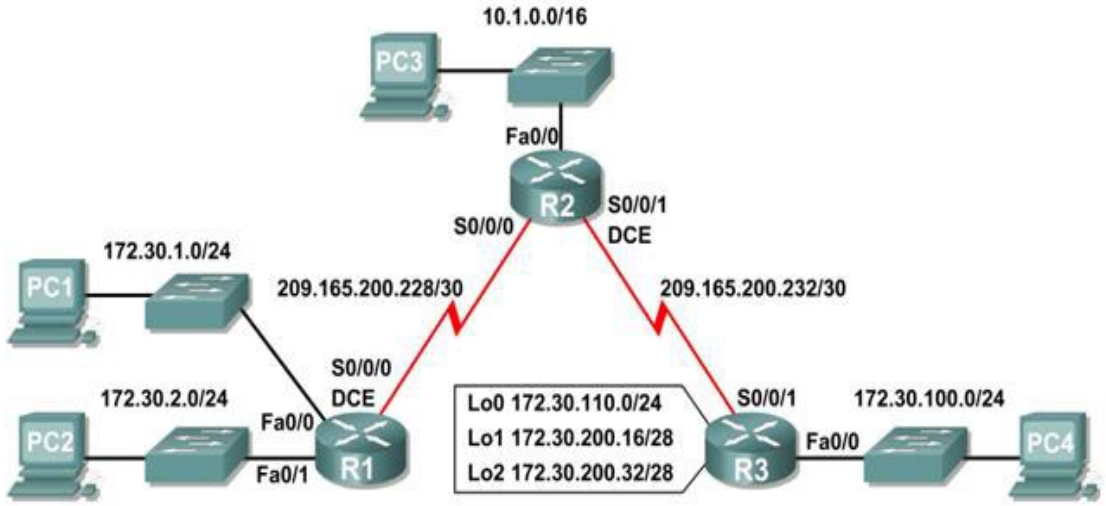


Рис. 5.1. Топологія мережі для налаштування протоколу маршрутизації RIPv2

Мережа, що наведена на топології містить розділену мережу 172.30.0.0. Ця мережа поділена на підмережі з використанням технології VLSM. Вона розділена іншою класовою мережею, в даному випадку це дві мережі 209.165.200.228/30 і 209.165.200.232/30. У випадку використання класових протоколів динамічної маршрутизації, мережа, що зображена на топології,

працювати не буде, тому що не передається інформація про маску. RIPv2 відноситься до безкласових протоколів, тому може використовуватись для налаштування подібних мереж.

Таблиця 5.1

Параметри налаштування

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	N/A
	Fa0/1	172.30.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
R2	Fa0/0	10.1.0.1	255.255.0.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.233	255.255.255.252	N/A
R3	Fa0/0	172.30.100.1	255.255.255.0	N/A
	S0/0/1	209.165.200.234	255.255.255.252	N/A
	Lo0	172.30.110.1	255.255.255.0	N/A
	Lo1	172.30.200.17	255.255.255.240	N/A
	Lo2	172.30.200.33	255.255.255.240	N/A
PC1	NIC	172.30.1.10	255.255.255.0	172.30.1.1
PC2	NIC	172.30.2.10	255.255.255.0	172.30.2.1
PC3	NIC	10.1.0.10	255.255.0.0	10.1.0.1
PC4	NIC	172.30.100.10	255.255.255.0	172.30.100.1

1: З'єднайте пристрої за наведеною схемою.

2: Налаштуйте параметри робочих станцій.

3. Налаштуйте параметри маршрутизатора R1 наступним чином:

```
!
hostname R1
!
!
!
interface FastEthernet0/0
 ip address 172.30.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.30.2.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.230 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 172.30.0.0
 network 209.165.200.0
!
line con 0
line vty 0 4
 login
!
end
```

4. Налаштуйте параметри маршрутизатора R2 наступним чином:

```
hostname R2
!
!
!
interface FastEthernet0/0
 ip address 10.1.0.1 255.255.0.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.229 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.200.233 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 passive-interface FastEthernet0/0
 network 10.0.0.0
 network 209.165.200.0
!
line con 0
line vty 0 4
 login
!
end
```

5. Налаштуйте параметри маршрутизатора R3 наступним чином:

```
hostname R3
!
!
!
interface FastEthernet0/0
 ip address 172.30.100.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.200.234 255.255.255.252
 no shutdown
!
interface Loopback0
 ip address 172.30.110.1 255.255.255.0
!
interface Loopback1
 ip address 172.30.200.17 255.255.255.240
!
interface Loopback2
 ip address 172.30.200.33 255.255.255.240
!
router rip
 passive-interface FastEthernet0/0
 network 172.30.0.0
 network 209.165.200.0
!
line con 0
line vty 0 4
 login
!
end
```

Після налаштувань перегляньте стан інтерфейсів. *Яка команда для цього використовується?* Запустіть команду на виконання і збережіть її результат.

При вірному з’єднанні та конфігурації задіяні інтерфейси повинні знаходитися у відкритому стані. Якщо ні, виявіть та усуньте причини.

6. Перевірте з’єднання між усіма пристроями в мережі. *Які проблеми виникли і чому? Перегляньте і збережіть вміст початкових таблиць маршрутизації для R1 і R2 та R3.*

Для перевірки того які повідомлення про оновлення отримує маршрутизатор R2 використайте команду debug ip rip

```
R2#debug ip rip
RIP protocol debugging is on
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
      172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
      172.30.0.0 in 1 hops
```

Поясніть вивід даної команди. Чому в таблиці маршрутизації маршрутизатора R2 до мережі 172.30.0.0 записано два маршрути?

7. Налаштуйте роботу динамічного протоколу маршрутизації RIPv2 у системі.

```
R2(config)#router rip
R2(config-router)#version 2

R1(config)#router rip
R1(config-router)#version 2

R3(config)#router rip
R3(config-router)#version 2
```

7.1. Перевірте чи змінився вміст таблиць маршрутизації на всіх трьох маршрутизаторах. Поясніть чому.

8. На кожному маршрутизаторі відключіть автоматичне об’єднання по класовій границі.

```
R2(config)#router rip
R2(config-router)#no auto-summary

R1(config)#router rip
R1(config-router)#no auto-summary

R3(config)#router rip
R3(config-router)#no auto-summary
```

9. Перевірте виконані налаштування маршрутизації RIPv2.

9.1. Перегляньте таблиці маршрутизації.

Порівняйте отримані дані з початковими таблицями маршрутизації.

Якщо не всі з наявних мереж відображаються у таблиці маршрутизації, перевірте правильність налаштувань протоколу RIP, стан інтерфейсів та з’єднань.

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

Запустіть команду на виконання 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 обновлення	
Версія протоколу RIP для обновлень, які розсилаються надходять	
Адреса шлюзу	
Адміністративна відстань	

9.3. Перегляньте процес формування та розповсюдження обновлень протоколом RIP в реальному часі.

9.4. Припиніть процес моніторингу

Контрольні запитання

6. Які переваги протоколу динамічної маршрутизації RIPv2 над RIPv1?
7. Що таке loopback інтерфейси та для чого вони використовуються?
8. Що таке балансування навантаження і як воно реалізоване у протоколі RIPv2. Де в лабораторній роботі можна було побачити рівноцінні маршрути?
9. Що таке класова та безкласова маршрутизація? Яка з них використовується по замовчуванню у протоколі RIPv2?
10. Як відключити автоматичне об’єднання по класовій границі?

ЛАБОРАТОРНА РОБОТА №6

Налаштування протоколу маршрутизації стану каналу OSPF

Мета: навчитися проводити налаштування протоколу маршрутизації OSPF. Дізнатися про основні відмінності між протоколами OSPF та RIP.

Завдання:

1. Налаштувати динамічні маршрути у схемі за заданою топологією.
2. Продемонструвати таблицю маршрутизації.
3. Пропінгувати маршрути між всіма комп'ютерами топології.
4. Відповісти на контрольні запитання

Теоретичні відомості

Інформація про стан каналу

OSPF є ієрархічним протоколом маршрутизації з оголошенням стану каналу з'єднання (link-state). Він був спроектований як протокол роботи усередині автономної системи - AS (Autonomous System), що являє собою групу маршрутизаторів і мереж, об'єднаних по ієрархічному принципу, які знаходяться під єдиним керуванням і спільно використовують загальну стратегію маршрутизації (рис. 6.1).

Обмін інформацією про маршрути усередині AS протокол OSPF здійснює за допомогою обміну повідомленнями про стани каналу з'єднань між маршрутизаторами і мережами області (link-state advertisement - LSA). Ці повідомлення передаються між об'єктами мережі, що знаходяться в межах автономної системи.

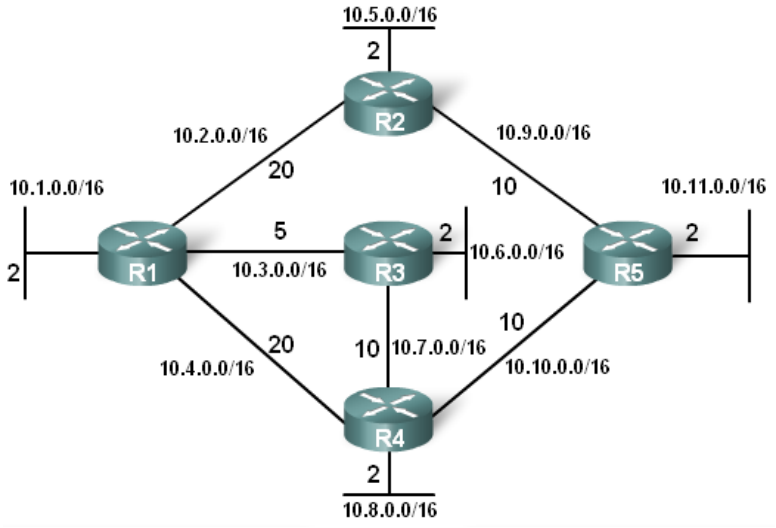


Рис. 6.1. Приклад автономної системи, у якій використовується протокол маршрутизації OSPF. Кожен канал зв'язку характеризується вартістю.

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. 6.1), таблиця маршрутів матиме схематичний вигляд, наведений в табл.6.2.

Таблиця 6.1.

Таблиця маршрутів для маршрутизатора R1 (рис.6.2)

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.

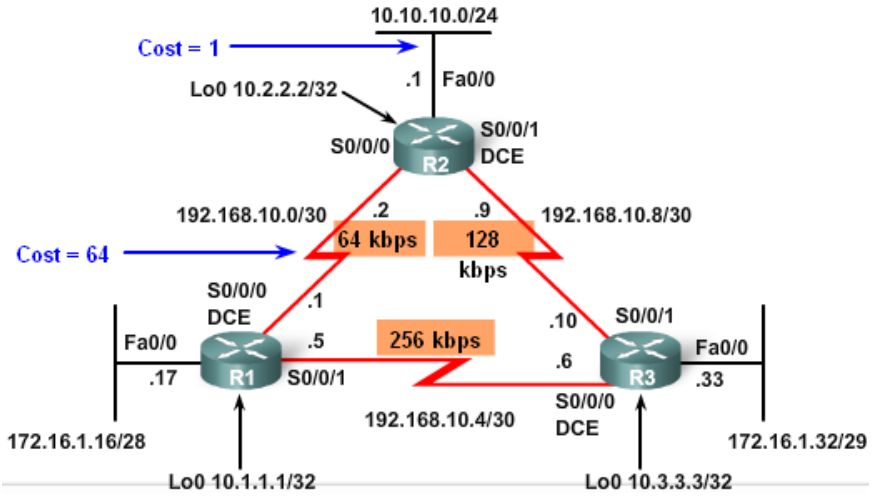


Рис. 6.2. Топологія мережі з позначеннями вартості маршрутів

Вартість з'єднання залежить від пропускної знатності інтерфейсу і визначається як показано в табл. 6.2. Переглянути пропускну здатність інтерфейсу можна за допомогою команди **show interface** *назва номер.*

Наприклад, переглянемо фрагмент таблиці маршрутизації для R1 (рис. 6.2):

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

В таблиці маршрутизації R1 (рис. 6.2) вказано, що вартість шляху до мережі 10.10.10.0/24 маршрутизатора R2 рівна 65. Оскільки мережа 10.10.10.0/24 під'єднана до інтерфейсу FastEthernet, її вартість на R2 рівна 1, до якої R1 додає вартість послідовного з'єднання T1 (64) між маршрутизаторами R1 і R2.

Таблиця 6.2.

Вартість з'єднання для інтерфейсів різних типів

Тип інтерфейса	**Вартість з'єднання 10^8/(пропускна _здатність.біт/с)**
FastEthernet	1
Ethernet	10
E1	48
T1	64
128 кбіт/с	781
64 кбіт/с	1562
56 кбіт/с	1785

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 у цій команді, буде брати участь у надсиланні та отриманні OSPF-пакетів, а інформацію про саму мережу (або підмережу) буде долучено до повідомлень-обновлень.

Формат команди у режимі конфігурації маршрутизатора є таким.

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

У даній команді використовується комбінація мережної адреси і шаблона маски, комбінація яких 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 у такий спосіб:

255.255.255.255

-

255.255.255.240 (Віднімаємо мережну маску)

---

0. 0. 0. 15 (Шаблон маски)

Номер області (або AC) визначає групу маршрутизаторів, які будуть обмінюватися інформацією про стани каналів та маршрути. Тому номер області для всіх маршрутизаторів у системі повинен бути однаковий.

Визначення ID маршрутизатора

Кожен маршрутизатор у OSPF-системі має свій ідентифікатор, який визначається за трьома критеріями у 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**.

Router(config)#interface loopback *номер*

Router(config-if)#ip address ip-address *мережна_маска*

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

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

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 інтерфейса.

- Стан інтерфейса стосовно роботи протокола OSPF. Стан FULL означає, що маршрутизатор і його сусідии 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 інтерфейса.

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 AC, а також час останнього обчислення найкоротшого шляку 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 інтерфейса. Для того щоб встановити сусідські відносини, Hello і Dead інтервали на з'єднаних маршрутизаторах повинні співпадати. За замовчуванням вони становлять 10 с і 40 с відповідно. Вразі відсутності зв'язку між двома сусідніми маршрутизаторами слід використовувати дану команду для перевірки ідентичності таймерів.

ПРАКТИЧНЕ ЗАВДАННЯ

Мета даного практичного завдання полягає в налаштуванні протоколу OSPF для заданої мережі в AC area 0, а також перевірці його роботи та досяжності усіх пристроїв системи.

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

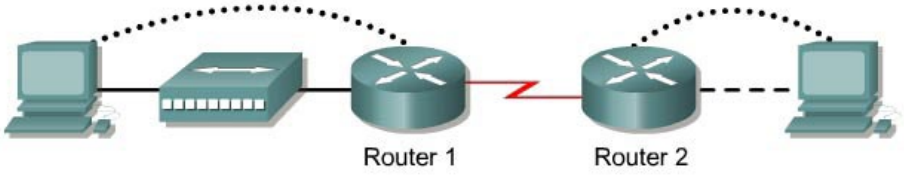


Рис. 5.4.*Тестова топологія та параметри для налаштування протоколу OSPF*

Таблиця 5.4

Праметри налаштування протоколу OSPF (рис.)

Позначення марш-ра	***Ім'я маршр-ра***	***Адреса інт-са FastEthernet***	***Адреса інт-са Serial***	***Тип інтерфейса 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 в режимі глобальної конфігурації налаштуйте імена та параметри інтерфейсів, згідно з таблицею 5.4.

2. Налаштування параметрів робочих станцій

Параметри для налаштування робочої станції:

а) підє'днаної 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 шлюза визначіть самостійно на основі конфігураційних параметрів маршрутизаторів (табл.. 5.4).

3. Перевірка налаштувань маршрутизаторів:

В привелийованому режимі:

а) перевірте поточну конфігурацію;

б) перегляньте коротку інформацію про інтерфейси; *Наведіть результат перевірки. В якому стані знаходятьс під'єднані інтерфейси?*

в) перевірте наявність зв'язку між усіма точками мережі в обох напрямках. Який результат перевірки і чим він пояснюється?

г) перегляньте і збережіть таблиці маршрутів для обох маршрутизаторів.

4. Налаштування протоколу маршрутизації OSPF на маршрутизаторах

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

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

Для кожного маршрутизатора вкажіть адреси мереж, та відповідні ним шаблони масок, які будуть налаштовані у команді ***network****.*

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

Як у таблиці маршрутизазії позначаються маршрути OSPF?

Яка адміністративна відстань та метрика для OSPF-маршрутів?

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

Визначіть та запишіть ідентифікатори кожного маршрутизатора.

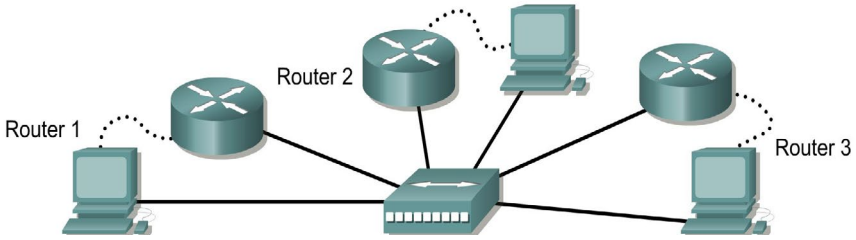
Перегляньте і збережіть таблиці сусідів.

6. Переверте досяжність крайніх точок мережі.

Контрольні запитання

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

2. Які параметри необхідно налаштувати для успішного OSPF-процеса маршрутизації?
3. Що таке loopback-інтерфейс? Яке його призначення?
4. На рис. 5.5 наведено схему з'єднання та параметри маршрутизаторів



Параметри інтерфейсів маршрутизатрів

Позначення марш-ра	Адреса /маска інтерфейса FastEthernet	Адреса /маска інтерфейса loopback
Router 1	192.168.1.1./24	192.168.31.11/32
Router2	192.168.1.2 /24	192.168.31.22/32
Router3	192.168.1.3/24	192.168.31.33/32

Рис. 5.5.

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

5. Які характеристики з'єднання враховуються протоколом OSPF при обчисленні метрики?
6. Визначіть шаблон маски для мережі 172.16.32.128/26.
7. Що таке ідентифікатор маршрутизатора і як він використовується протоколом OSPF?

ЛАБОРАТОРНА РОБОТА №7

Налаштування динамічного протоколу маршрутизації EIGRP

Мета: навчитися проводити налаштування протоколу маршрутизації EIGRP. Дізнатися про основні відмінності між протоколами EIGRP, OSPF та RIP.

Завдання:

5. Налаштувати динамічні маршрути у схемі за заданою топологією.
6. Продемонструвати таблицю маршрутизації.
7. Пропінгувати маршрути між всіма комп'ютерами топології.
8. Відповісти на контрольні запитання

ПРАКТИЧНЕ ЗАВДАННЯ

У даній лабораторній роботі необхідно з'єднати пристрої у мережу за схемою, наведеною на рис. 7.1, виконати основні налаштування маршрутизаторів та робочих станцій (табл. 7.1) перевірити проведені налаштування та роботу протоколу маршрутизації EIGRP.

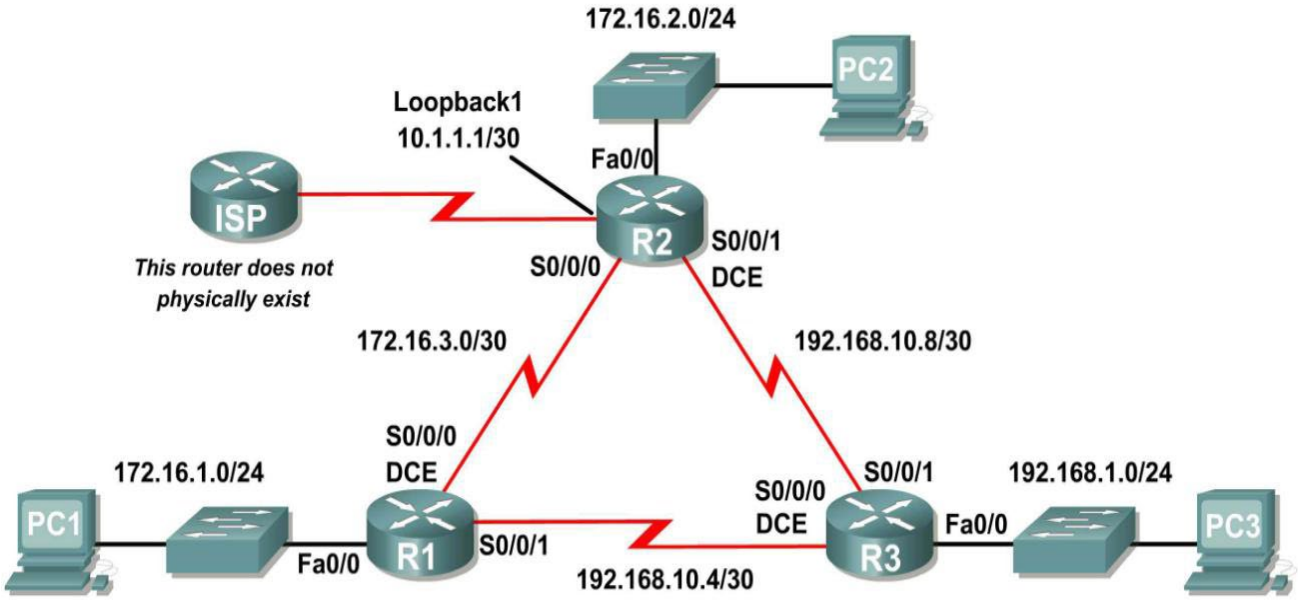


Рис. 7.1. Топологія мережі для налаштування протоколу маршрутизації EIGRP

1: З'єднайте пристрої за наведеною схемою.

2: Налаштуйте параметри робочих станцій.

Таблиця 7.1

Параметри налаштування

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	Lo1	10.1.1.1	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

3. Налаштуйте інтерфейси маршрутизаторів R1, R2 та R3 згідно наведеної вище таблиці та перевірте налаштування за допомогою команди *show ip interface brief*

4. Налаштуйте протокол EIGRP на маршрутизаторі R1 наступним чином:

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

Та задайте командою ***network*** класову мережу 172.16.0.0 та підмережу 192.168.10.4/30

5. Налаштуйте протокол EIGRP на маршрутизаторі R2 наступним чином:

```
R2(config)#router eigrp 1
R2(config-router)#

R2(config-router)#network 172.16.0.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up:
new adjacency
```

Як видно із сервісного повідомлення, DUAL, посилає повідомлення про те, що встановлений новий зв'язок з сусіднім маршрутизатором який теж використовує протокол EIGRP.

За допомогою команди ***network*** задайте підмережу 192.168.10.8/30

6. Налаштуйте протокол EIGRP на маршрутизаторі R3 наступним чином:

- Використайте 1 для номеру процесу;
- Використовуйте класову адресу мережі для FastEthernet інтерфейсу;
- Включайте шаблони масок для підмереж, що під’єднані до інтерфейсів Serial 0/0/0 та Serial 0/0/1;
- Після завершення, поверніться в привілейований режим.

Перевірка роботи протоколу EIGRP

7. Перевірте таблицю сусідів на маршрутизаторі R1:

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   172.16.3.2      Ser0/0/0        10   00:36:51  40     500   0   13
1   192.168.10.6    Ser0/0/1        11   00:26:51  40     500   0   4
R1#
```

8. Перевірте налаштування протоколу за допомогою команди *show ip protocols*

Пам'ятайте, що для правильної роботи протоколу EIGRP необхідно щоб номер процесу був на всіх маршрутизаторах однаковим. Команда ***show ip protocols*** відображає інформацію про мережі, для яких сконфігурований протокол EIGRP, а також IP адреси сусідніх маршрутизаторів, для яких встановлені зв'язки.

```
Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.4/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.3.2      90            4811399
    192.168.10.6    90            5411677
  Distance: internal 90 external 170
```

9. Виведіть таблицю маршрутизації на маршрутизаторі R1

Маршрути протоколу EIGRP відображаються з кодом D (по назві алгоритму DUAL, що використовується для обрахунку найкращих маршрутів).

Поясніть наявність в таблиці маршрутизації маршруту, який виділений нижче:

```
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 01:16:19, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
```

10. Перегляньте таблицю маршрутизації на маршрутизаторі R3

Поясніть наявність виділеного маршруту

```
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:15:35, Serial0/0/0
                   [90/2172416] via 192.168.10.9, 01:15:22, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:15:22, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
```

Як називаються такі маршрути?

11. Налаштуйте пропускну здатність інтерфейсів маршрутизаторів

Спочатку перегляньте метрики по замовчуванню, що використовує протокол EIGRP:

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Налаштуйте пропускну здатність інтерфейсів маршрутизатора наступним чином:

R1 router:

```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
```

R2 router:

```
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 1024
```

R3 router:

```
R3(config)#interface serial0/0/1
R3(config-if)#bandwidth 1024
```

Перевірте чи змінилось значення пропускної здатності інтерфейсів. Яка команда для цього використовується? Як змінилось значення метрики для відповідних маршрутів? Чи залишились без змін таблиці маршрутизації маршрутизаторів?

Перевірка основних та запасних маршрутів протоколу EIGRP (Successors and Feasible distance)

12. Перевірте таблицю маршрутизації маршрутизатора R2

Наступник (Successor) це сусідній маршрутизатор, який в даний час використовується для передачі пакетів у віддалену мережу. Тобто це найкращий маршрут до мережі призначення. Адресу наступника можна побачити в таблиці маршрутизації після ключового слова via.

Можлива відстань (Feasible distance FD) це найменша з обрахованих метрик для досягнення певної мережі. FD можна побачити в таблиці маршрутизації, як метрику конкретного маршруту.

```
R2#show ip route

<output omitted>

     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:52, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:11, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
```

- Який найкращий шлях до комп'ютера PC1?
- Яка IP адреса та ім'я наступника для цього маршруту?
- Яка можлива відстань (FD) для мережі, в якій знаходиться PC1?

13. Визначте чи може R1 бути можливим наступником (Feasible Successor) для маршруту від R2 до мережі 192.168.1.0

Можливий наступник це сусідній маршрутизатор який має правильний запасний маршрут до відповідної мережі. Для того щоб бути можливим наступником R1 повинен задовольняти вимогам можливості (Feasible condition). Ці вимоги задовольняються у випадку якщо повідомлена відстань (Reported distance, RD) до мережі призначення на сусідньому маршрутизаторі є меншою ніж FD до цієї ж мережі на локальному маршрутизаторі.

Для того щоб відповісти на поставлене в завданні питання необхідно виконати наступні кроки:

- Переглянути таблицю маршрутизації маршрутизатора R1

```
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:42:59, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:43:00, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:42:26, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:42:20, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:42:20,
Serial0/0/1
```

Яка RD до мережі 192.168.1.0?

- Переглянути таблицю маршрутизації маршрутизатора R2

```
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:52, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:11, Null0
D       192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
```

Яка FD до мережі 192.168.1.0?

- Чи буде R2 вважати R1 можливим наступником для мережі 192.168.1.0?

14. Перегляньте топологічну таблицю

Для перегляду детальної інформації про конкретний запис в топологічній таблиці можна використовувати конкретну адресу мережі. Перегляньте спочатку всю топологічну таблицю маршрутизатора R2, а потім детальну інформацію для мережі 192.168.10.0 за допомогою команди ***show ip eigrp topology 192.168.10.0***. Скільки наступників є для даної мережі в топологічній таблиці? Які їх IP адреси? Яка FD і RD до мережі 192.168.10.0?

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
         via Connected, Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 192.168.10.0/24, 1 successors, FD is 3011840
         via Summary (3011840/0), Null0
P 172.16.1.0/24, 1 successors, FD is 40514560
         via 172.16.3.1 (40514560/28160), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
         via 192.168.10.10 (3014400/28160), Serial0/0/1
         via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
         via 192.168.10.10 (3523840/2169856), Serial0/0/1
```

Контрольні запитання

1. Які переваги протоколу динамічної маршрутизації EIGRP над іншими протоколами динамічної маршрутизації?
2. Що таке технологія VLSM та для чого вона використовується?
3. Що таке loopback інтерфейси та для чого вони використовуються?
4. Що таке балансування навантаження і як воно реалізоване у протоколі EIGRP. Де в лабораторній роботі можна було побачити рівноцінні маршрути?
5. Що таке класова та безкласова маршрутизація? Яка з них використовується по замовчуванню у протоколі EIGRP?
6. Як відключити автоматичне об’єднання по класовій границі?

ЛАБОРАТОРНА РОБОТА № 8

Налаштування стандартного списку управління доступом

Мета: навчитися проводити налаштування стандартних списків керування доступом та фільтрувати з їх допомогою трафік у мережі.

Завдання:

1. Налаштувати список керування доступом у схемі за заданою топологією.
2. Застосувати його на правильному інтерфейсі.
3. Перевірити зв'язок між комп'ютерами топології та впевнитися, що список керування доступом працює коректно.
4. Відповісти на контрольні запитання

ТЕОРЕТИЧНІ ВІДОМОСТІ

Списки управління доступом (Access Control List (ACL)) є набором 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.

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

Список керування доступом представляє 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 керування доступом. Якщо параметри пакету відповідають наступній умові, яка представляє 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.

В стандартних списках управління доступом параметром пакету, 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 порта або назва протокола прикладного рівня, дані від якого передаються в пакеті.

Кожен список управління доступом характеризується своїм індивідуальним номером з певного діапазона, який визначає тип списку та протокол, для якого він використовується (табл. 8.1). Зокрема, номера 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 номеру дозволено також використовувати ім'я. Тому іменовані списки можуть бути як стандартними так і розширеними і позначаються не номерами, а змістовними назвами.

Таблиця 8.1.

Протоколи та їх допустимі діапазони номерів списків управління доступом

Протокол	**Діапазон змін номерів списків керування 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

1. 3. Налаштування стандартних списків 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 дія складається з створення списка, а друга – зі застосування списка на конкретному інтерфейсі.

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 заданій умові.

На другому етапі ACL прив'язується до певного інтерфейса, 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:

вцілому:

no access-list номер-списку

з інтерфейса:

no ip access-group номер-списку

1. 4. 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, а біт рівний 1 означає, що умова для нього перевірятись не буде (рис. 8.1) .

Рис. 8.1. Використання шаблону маски для обрання одного або декількох IP-адрес для виконання перевірки на дозвіл доступу або відмову в доступі

Шаблон маски використовується для виокремлення або групування однієї або декількох 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, під мережі (одиниці), а які – частину хостів (нулі).

Тоді як в шаблоні маски нулі та одиниці вказують списку керування доступом на необхідність перевіряти або не перевіряти відповідні біти в IP-адресі. На рис.8.2 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 октета позначають номер мережі, а третій октет призначений для номеру підмережі. 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 показано на рис. 8.2.

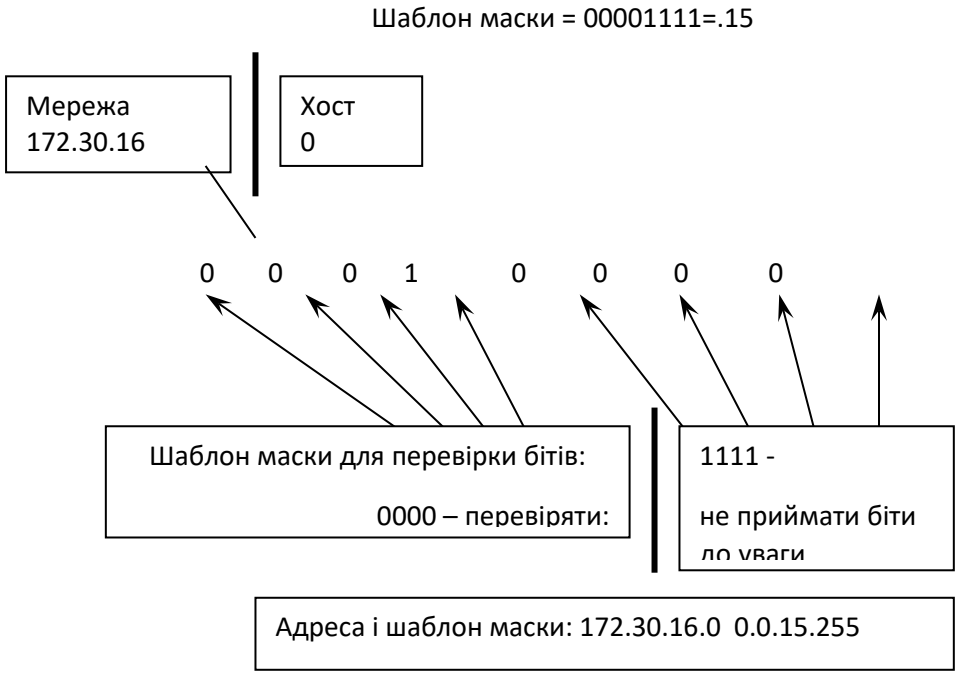


Рис. 8.2. Адреса 172.30.16.0 з шаблоном маски 0.0.15.255 відповідає мережам з номерами від 172.30.16.0 до 172.30.31.0

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

В третьому октеті шаблон маски рівний 15 (00001111), а IP-адреса 16 (00001000). Перші чотири нуля шаблон маски вказують маршрутизатору на

необхідність перевірки перших чотирьох бітів IP-адреси (0001). Так як останні чотири біта не беруться до уваги, всі числа в інтервалі від 16 (00010000) до 31 (00011111) будуть задовольняти умові перевірки, оскільки всі вони починаються з 0001.В наведеному прикладі адреса 172.30.16.0 з маскою 0.0.15.255 відповідає підмережам з номерами від 172.30.16.0 до 172.30.31.0. Інші підмережі не задовольняють умовам маски.

Деколи замість шаблону маски можна використовувати ключові слова. Наприклад, якщо потрібно відкрити доступ для всіх номерів одержувачів, можна вказати IP-адреси 0.0.0.0 для зазначення того, що список управління доступом не повинен приймати до уваги значення адрес (пропускати їх без перевірки), а всі біти шаблону маски адрес встановити в одиниці (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 складатись 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, зображеній на рис. 8.3.

Приклад 8.1. 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

Зауважте, що згідно цій умові всім іншим буде відвідмовлено у 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.

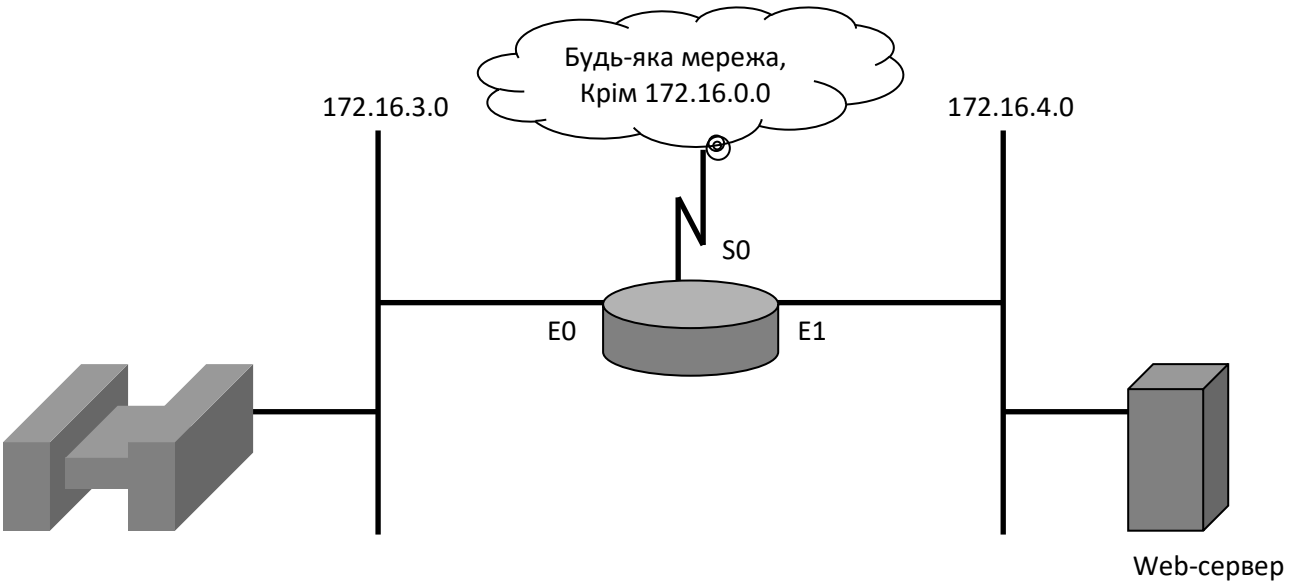


Рис. 8.3.

В другому прикладі 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** створює групу списка 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

В 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**

Особливості створення і 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, всі б 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 як на адресі відправника, так і отримувача і забезпечують більш гнучкий механізм керування потоками даних не лише на основі адрес, але й протоколів.
- при потраплянні на інтерфейс рух пакету розглядаєть 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 самимми параметрами. Для кожного напрямку потрібно створювати окремий набір директив.
- В 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 вже призначено на інтерфейс неможна додавати нові умови перевірки. Для цього потрібно видалити список і створити новий, додавши необхідні директиви. Виключення – іменовані списку, у яких нові умови долучаються в кінець списку.

ПРАКТИЧНЕ ЗАВДАННЯ

1. **Базові налаштування маршрутизатора.** З'єднайте пристрої за схемою, наведеною на рис. 8.4. На маршрутизаторі налаштуйте під'єднаний локальний інтерфейс відповідною адресою та маскою (табл. 8.2). Переведіть інтерфейс у відкритий стан.
2. **Налаштування робочих станцій Ethernet-сегменту.** *Для цього спочатку знайдіть і запишіть адресу підмережі, до якої належать робочі станції. Після цього, визначіть 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?*

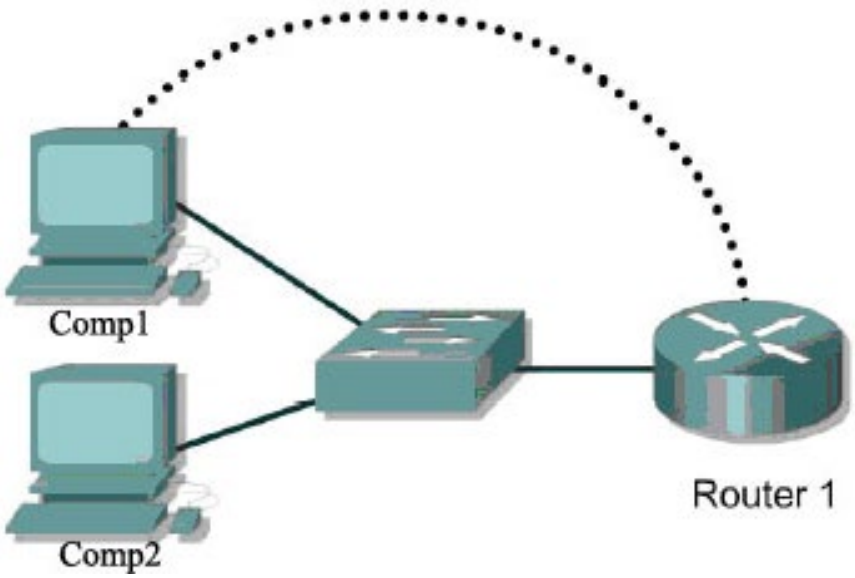


Рис. 8.4. З'єднання пристроїв для налаштування стандартних списків управляння доступом

Таблиця 8.2.

Праметри налаштування

Позначення пристрою	**Адреса інтерфейса 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 звертатися до маршрутизатора робочій 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 викнує цю діяю. 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'язаних до локального інтерфейса.

4.5. Створіть новий стандартний список управління доступом під номером 2, який заборонить звертатися до маршрутизатора усім користувачам 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 викнує цю діяю. В якому напрямку перевірятимуться пакети на відповідність умовам списку?*

4.7. Видаліть створений список управління доступом.

4.8. Створіть ще один список управління доступом, access-list 3, який би надавав дозвіл хостам з 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 октета рівний 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-інтерфейса маршрутизатора з кожної робочої станції. Які результати тестування і чи досягнуто мету завдання 4.8?

Контрольні запитання

1. Призначення списків управління доступом і їх типи.
2. Що таке шаблон маски? Як він визначається і для чого використовується?
3. Як у списках управління доступом задати умові для окремого хоста?
4. Створено 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
   Що він означає (оберіть 2 варіанти):
   a) заборонено вхід до підмережі 10.10.10.16/28 всім окрім мережі 192.168.1.0;
   b) дозволено вхід до підмережі 10.10.10.16/28 всім окрім користувачів мережі 192.168.1.0;
   c) заборонено вхід до підмережі 192.168.1.0 всім окрім користувачів мережі 10.10.10.16/28;
   d) обмежується Интернет трафік;
   e) обмежується доступ по протоколу Telnet;
   f) обмежується доступ до 80-го комп′ютера.
5. Знайдіть у преліку справа пояснення для команд, поданих зліва:
   a) any
   b) show running-config
   c) show access-list

d) host
e) show ip interface
1) використовується замість шаблону 0.0.0.0
2) дозволяє перевірити чи на інтерфейсі налаштовано ACL
3) відображає вміст усіх списків управління доступом на маршрутизаторі
4) аналогічне використанню 0.0.0.0 255.255.255.255
5) відображає списки управління доступом та інтерфейси, з якими вони пов’язані.

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

ЛАБОРАТОРНА РОБОТА № 9

Налаштування протоколу VTP та inter-VLAN взаємодії

Мета: навчитися проводити налаштування віртуальних мереж на свічах та використовувати протокол VTP для автоматичного розповсюдження такої конфігурації на інші свічі мережі.

Завдання:

1. Створити віртуальні мережі за заданою топологією.
2. Налаштувати VTP режими на свічах згідно завдання.
3. Перевірити з'єднання між віртуальними мережами.
4. Налаштувати inter-VLAN взаємодію за допомогою маршрутизатора
5. Відповісти на контрольні запитання

Для виконання даної лабораторної роботи складіть в Cisco Packet Tracer наступну топологію:

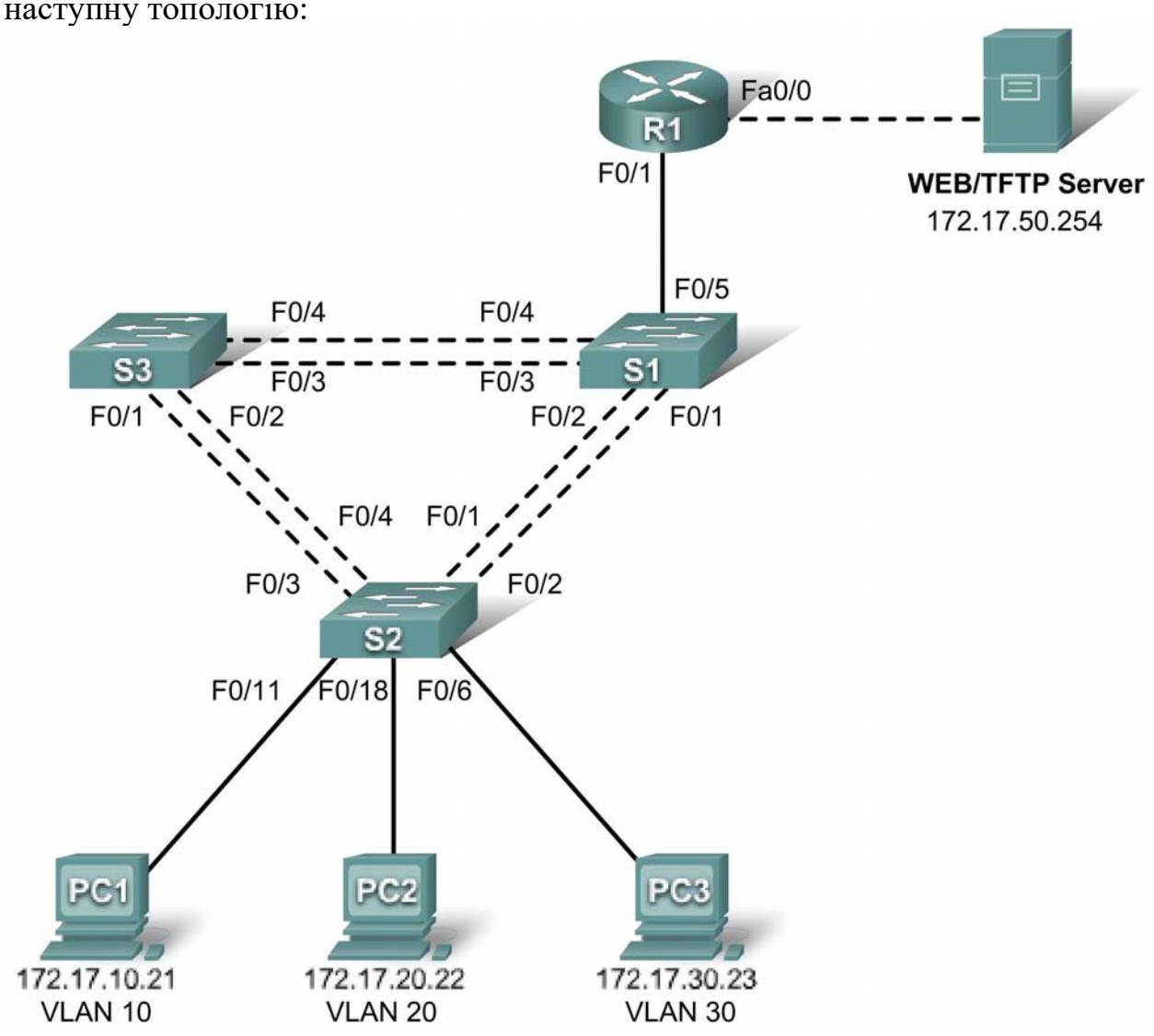


Рис. 9.1. Топологія мережі

Таблиця адресації пристроїв мережі наведена нижче:

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.1
R1	Fa 0/0	172.17.50.1	255.255.255.0	N/A
R1	Fa 0/1	See Interface Configuration Table		N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 - Students	172.17.20.0 /24

Interface Configuration Table – Router 1

Interface	Assignment	IP Address
Fa0/1.1	VLAN1	172.17.1.1 /24
Fa0/1.10	VLAN 10	172.17.10.1 /24
Fa0/1.20	VLAN 20	172.17.20.1 /24
Fa0/1.30	VLAN 30	172.17.30.1 /24
Fa0/1.99	VLAN 99	172.17.99.1 /24

1. Переконайтесь, що всі мережеві пристрої мають конфігурацію VLAN по замовчуванню:

```
S1#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

2. Для того щоб запобігти несанкціонованим підключенням спочатку відключіть всі порти свічів за допомогою команди ***interface range***

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

3. А потім заново включіть порти, які Вам потрібні:

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

4. Проведіть конфігурацію комп’ютерів відповідно з таблицею конфігурації, що наведена вище.

5. Проведіть конфігурацію протоколу VTP на трьох свічах згідно з таблицею наведеною нижче:

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab6	cisco
S2	Client	Lab6	cisco
S3	Client	Lab6	cisco

S1:

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S1(config)#vtp password cisco
Setting device VLAN database password to cisc
S1(config)#end
```

S2:

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S2(config)#vtp password cisco
Setting device VLAN database password to cisc
S2(config)#end
```

S3:

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S3(config)#vtp password cisco
Setting device VLAN database password to cisc
S3(config)#end
```

6. Проведіть конфігурацію магістральних портів свіча та визначте native VLAN для них:
Для свіча S1 магістральними будуть порти з fa0/1 по fa0/4:

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

Аналогічно для свічів S2 та S3:

```
S2(config)# interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

7. На VTP сервері створіть наступні VLANs

VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

8. Перевірте чи додалися новостворені VLAN в конфігурацію за допомогою команди ***show vlan brief***

9. Перевірте за допомогою цієї ж команди чи з’явились створені VLAN в конфігурації інших свічів.

10. Проведіть конфігурацію інтерфейсів для керування на всіх трьох свічах:

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

11. Для того щоб впевнитись, що конфігурація свічів здійснена правильно перевірте з'єднання між трьома свічами за допомогою команди ***ping.*** Якщо результат не успішний перевірте конфігурацію, можливо були допущені помилки.

12. Призначте порти на свічі S2 створеним VLAN

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

13. Перевірте з'єднання між VLANs. Для цього з командного рядка PC1 (172.17.10.21) виконайте команду ping до PC2 (172.17.20.22). А з PC2 до PC3 (172.17.30.23). Чи успішно передаються пакети? Чому?

14. Для передачі даних між віртуальними мережами налаштуйте маршрутизатор R1 використовуючи команди наведені нижче:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Як видно, ми використовуємо технологію sub-інтерфейсів.
15. Налаштуйте мережу до якої під‘єднаний сервер:

```
R1(config)# interface FastEthernet0/0
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

16. Перевірте, чи знаходяться в таблиці маршрутизації R1 всі 6 сконфігурованих мереж:

```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 6 subnets
C       172.17.50.0 is directly connected, FastEthernet0/1
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.20.0 is directly connected, FastEthernet0/0.20
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

17. Перевірте передачу даних між віртуальними мережами. З PC1 використайте команду ping до віддаленого сервера (172.17.50.254) та двох інших комп’ютерів (172.17.20.22 і 172.17.30.23). Всі пакети повинні передаватись.

Контрольні запитання

1. Для чого призначений протокол VTP?
2. В яких режимах можуть знаходитись свічі, що підтримують протокол VTP? Який режим використовується по замовчуванню?
3. Що таке номер конфігурації та для чого він використовується? За допомогою якої команди можна його подивитись?
4. Які дві технології використовуються для передачі даних між віртуальними мережами? Які переваги та недоліки кожної з них? Яка технологія була використана в даній лабораторній роботі?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Wendell Odom, Sean Wilkins. CCNA 200-301 Official Cert Guide and Network Simulator Library. – Cisco Press, 2022, 560p.
2. Scott Empson. CCNA 200-301 Portable Command Guide, 5th Edition. – Cisco Press, 2019, 320p.
3. Billy Calvert. CCNA: CCNA 200-301: Cisco Certified Network Associate. – Cisco Press, 2020, 206p.
4. Johnson Allan. 31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam. – Cisco Press, 2020, 464p.
5. Todd Lammle, Jon Buhagiar. CCNA Certification Study Guide and Practice Tests Kit: Exam 200-301. – SYBEX, 2020, 1360p.
6. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 1. – Cisco Press, 2020, 848p.
7. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 2. – Cisco Press, 2020, 624p.

Навчально-методичне видання

Д’яченко Лілія Іванівна

Програмне забезпечення мережевих технологій
Навчально-методичний посібник з лабораторних робіт
(видання електронне)

для студентів спеціальностей
121 - Інженерія програмного забезпечення, 122 – Комп’ютерні науки
усіх форм навчання

Відповідальний за випуск – Л.І. Д’яченко
Літературний редактор – О.В. Лупул
Технічний редактор та дизайнер обкладинки – А.В. Цвіра

Підписано до друку 1.10.2022. Формат 60х84/16.
Папір офсетний. Друк різографічний. Умов.-друк. арк. 18,59.
Обл.-вид. Арк. 16,73. Тираж 150. Зам. Н-008п.
Видавництво та друкарня Чернівецького національного університету.
58012, Чернівці, вул. Коцюбинського, 2.
e-mail: ruta@chnu.edu.ua

Свідоцтво суб’єкта видавничої справи ДК № 891 від 08.04.2002.