Лабораторна робота №5

Тема: Налаштування основних параметрів підключення в мережевій операційній системі Cisco IOS

Мета роботи: навчитись налаштовувати підключення, виконуючи конфігурацію IP-адресації на комутаторах і ПК; навчитись використовувати різні команди **show**, щоб перевіряти налаштування, а також команду **ping** для перевірки основних параметрів підключення між пристроями.

Теоретичні відомості

IP-адресація пристроїв

Щоб пристрої виявили один одного і встановили наскрізний зв'язок по мережі Інтернет, використовуються IP-адреси, адреси IPv4 або IPv6. Фактично **IP-адреси** забезпечують зв'язок між пристроями від джерела до пункту призначення і в зворотному напрямку в будь-якій формі мережевої взаємодії.

Кожен прикінцевий пристрій в мережі повинен мати IP-адресу. До прикінцевих пристроїв відносяться наступні:

- комп'ютери (робочі станції, ноутбуки, файлові сервери, веб-сервери);
- мережеві принтери;
- VoIP-телефони;
- камери відеоспостереження;
- смартфони;
- мобільні кишенькові пристрої (наприклад, бездротові сканери штрих-кодів).

Структура адреси IPv4 – це точково-десяткове представлення у вигляді чотирьох десяткових чисел в діапазоні від 0 до 255. **Адреси IPv4** – це номери, присвоєні окремим пристроям, підключеним до мережі. Вони мають логічну природу, оскільки надають інформацію про місцезнаходження пристрою.

Крім IP-адреси необхідна маска підмережі. **Маска підмережі** – це особливий тип адреси IPv4, який спільно з IP-адресою визначає, до якої саме підмережі, що належить великій мережі, підключено даний пристрій.

IP-адреси можуть бути присвоєні фізичним портам і віртуальним інтерфейсам на всіх пристроях. Віртуальний інтерфейс означає, що з цим інтерфейсом не пов'язане додаткове фізичне обладнання.

Інтерфейси і порти

Передача даних по мережі залежить від інтерфейсів прикінцевих пристроїв, інтерфейсів мережевих пристроїв і кабелів, які реалізують з'єднання. Кожен фізичний інтерфейс визначається своїми технічними характеристиками або стандартами. Кабель, що використовується для з'єднання, повинен відповідати всім фізичним стандартам інтерфейсу. Передача даних здійснюється за допомогою витих мідних кабелів, оптоволоконних кабелів, коаксіальних кабелів або за допомогою бездротового зв'язку. Різні типи мережевих засобів передачі даних відрізняються один від одного характерними функціями і перевагами. Мережеві засоби передачі

даних можуть мати різні характеристики і виконувати різні завдання. До деяких відмінностей між різними типами засобів передачі даних відносяться наступні:

- відстань, яку може покривати засіб передачі даних;
- середовище, в якому може бути встановлено засіб передачі даних;
- обсяги даних і швидкість передачі;
- вартість засобу передачі даних і його встановлення.

Ethernet – найпоширеніша технологія локальної мережі (LAN) на сьогоднішній день. Порти Ethernet можна знайти на пристроях кінцевих користувачів, комутаційних і інших мережевих пристроях, які можуть здійснювати фізичне підключення до мережі за допомогою кабелю. Щоб кабель міг з'єднувати пристрої за допомогою порту Ethernet, кабель повинен бути забезпечений правильним роз'ємом – **RJ-45**.

Комутатори Cisco IOS не тільки оснащені фізичними портами для пристроїв, але також одним або декількома віртуальними інтерфейсами комутаторів (SVI). Такі інтерфейси називаються **віртуальними**, оскільки в пристрої немає пов'язаного з ними фізичного обладнання. Віртуальний інтерфейс створений в програмному забезпеченні. Віртуальний інтерфейс дозволяє дистанційно керувати комутатором через мережу за допомогою IPv4. Кожен комутатор поставляється з одним віртуальним інтерфейсом комутатора в конфігурації за замовчуванням. Віртуальним інтерфейсом за замовчуванням є **VLAN1**.

Налаштування віртуального інтерфейсу комутатора

Для віддаленого доступу до комутатора на віртуальному інтерфейсі комутатора потрібно налаштувати IP-адресу і маску підмережі:

- **IP-адреса** – спільно з маскою підмережі ідентифікує прикінцеве обладнання в мережевій взаємодії;
- **маска підмережі** – визначає, яка частина IP-адреси відноситься до адреси мережі, а яка – до адреси хосту в цій мережі.

В даний момент основна увага фокусується на адресах IPv4. Адреси IPv6 детально розглянемо пізніше.

Згодом ви зрозумієте важливість IP-адрес, але в даний момент необхідно навчитися швидко налаштовувати комутатор для підтримки віддаленого доступу. На рис. 5.1 показана команда для активації IP-з'єднання з комутатором **S1** за допомогою IP-адреси **192.168.10.2**:

- **`interface vlan 1`** – застосовується для переходу в режим налаштування інтерфейсу з режиму глобальної конфігурації;
- **`ip address 192.168.10.2 255.255.255.0`** – налаштовує IP-адресу і маску підмережі для комутатора (тільки одне з декількох можливих поєднань IP-адреси і маски підмережі);
- **`no shutdown`** – активує інтерфейс.

Після налаштування цих команд всі IP-елементи в комутаторі будуть готові для передачі даних по мережі.

Примітка. *Для віддаленого управління комутатором, як і раніше, необхідно налаштувати один або декілька фізичних портів, а також каналів **VTY**.*

Налаштування IP-адрес прикінцевих пристроїв вручну

Для забезпечення зв'язку прикінцевого пристрою з усією мережею, його потрібно правильно налаштувати. Як і віртуальному інтерфейсу комутатора, прикінцевому пристрою потрібно присвоїти IP-адресу і маску підмережі. Ці дані налаштовуються в параметрах ПК.

Увійдіть в режим конфігурації інтерфейсу для VLAN 1

```
Switch(config)#interface vlan 1
```

Налаштуйте IP-адресу у вигляді '192.168.10.2' і маску підмережі – у вигляді '255.255.255.0'

```
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
```

Активуйте інтерфейс

```
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#
```

Інтерфейс VLAN 1 налаштований

Рис. 5.1. Налаштування віртуального інтерфейсу комутатора

Щоб прикінцевий пристрій було правильно підключено до мережі, на ньому потрібно налаштувати всі ці параметри. Ця інформація налаштовується в області параметрів мережі ПК. Крім IP-адреси і даних про маску підмережі, можна вказати адресу шлюз і дані сервера DNS, як показано на рис. 5.2.

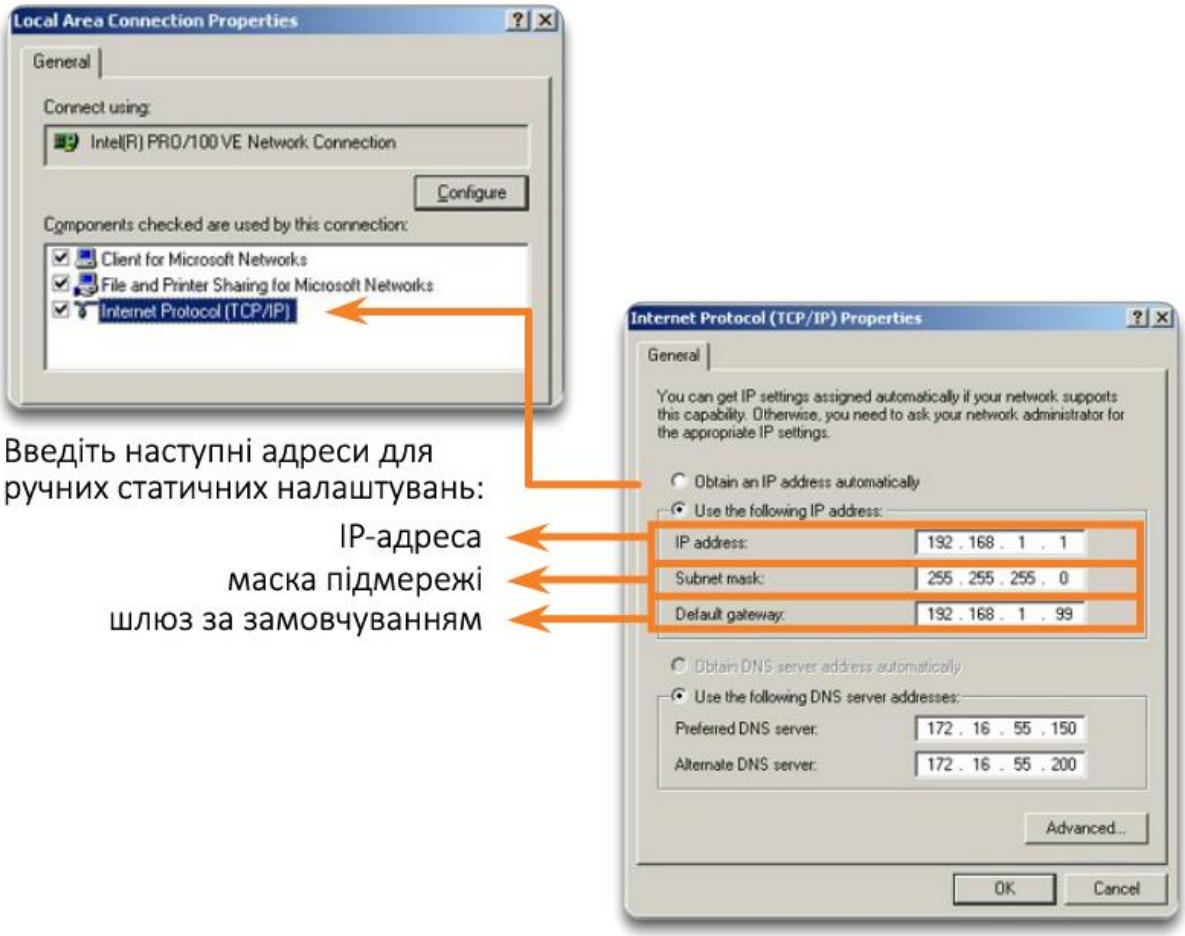

Рис. 5.2. Адресація прикінцевих пристроїв

Адреса шлюзу – це IP-адреса інтерфейсу маршрутизатора, що використовується для виходу мережевого трафіку з локальної мережі. **Шлюз** – це IP-адреса, яку часто призначає адміністратор. Його використовують, коли трафік потрібно направити в іншу мережу.

Адреса сервера DNS – це IP-адреса сервера служби доменних імен (DNS), який використовується для перетворення веб-адрес в IP-адреси. Доступ до пристроїв в Інтернеті здійснюється за допомогою IP-адреси. Однак користувачам легше запам'ятати імена, а не цифри. Тому для простоти веб-сайтам присвоюються імена.

Автоматичне налаштування IP-адрес прикінцевих пристроїв

Інформацію про IP-адресу можна ввести в ПК вручну або отримати автоматично за допомогою протоколу **динамічної конфігурації мережного вузла (DHCP)**. DHCP забезпечує автоматичне налаштування IP-даних прикінцевим пристроям.

DHCP – це технологія, яка використовується практично у всіх корпоративних мережах. Щоб зрозуміти переваги цієї технології, можна оцінити обсяг роботи, який довелося б виконувати без її застосування.

DHCP автоматично налаштовує адреси IPv4 для кожного кінцевого пристрою в мережі з увімкненим протоколом DHCP. Уявіть, скільки часу ви б витрачали, якби при кожному приєднанні до мережі вам доводилося б вручну вводити дані IP-адреси, маски підмережі, шлюзу і DNS-сервера. Помножте це на кількість користувачів і їх пристроїв в мережі, і ви відразу зрозумієте переваги DHCP.

DHCP – приклад надзвичайно ефективної технології. Одне з основних призначень будь-якої технології – полегшити роботу людини. При наявності DHCP, кінцевий користувач може прийти в будь-яке місце, де є підключення до мережі, і підключитися до мережі за допомогою кабеля Ethernet або за допомогою бездротової технології, і вся інформація IPv4, необхідна для повноцінного зв'язку з мережею, буде налаштована автоматично.

Як показано на рис. 5.3, для налаштування протоколу DHCP на ПК з ОС Windows необхідно тільки вибрати параметри «Отримати IP-адресу автоматично» та «Отримати адресу сервера DNS автоматично». Після чого вашому комп'ютеру будуть присвоєні дані з пулу IP-адрес, а також вся відповідна інформація, наявна на сервері DHCP. Щоб переглянути налаштування IP для ПК з ОС Windows, в командному рядку введіть команду **`ipconfig`** (рис. 5.4).

Конфлікти IP-адрес

Якщо для мережевих пристроїв, наприклад, для принтера, IP-адресу було налаштовано статично (вручну), а потім встановлено сервер DHCP, то між мережевим пристроєм і ПК, який автоматично отримує IP-дані з сервера DHCP, може статися конфлікт подвійної IP-адреси. Також конфлікт може виникнути, якщо в разі збою у роботі сервера DHCP вручну вказати статичну IP-адресу для мережевого пристрою. Конфлікт виникне після виправлення неполадок і відновлення роботи сервера DHCP в мережі.

Щоб вирішити такий конфлікт IP-адресації, потрібно підключити мережевий пристрій зі статичною IP-адресою до клієнта DHCP. Також можна виключити статичну IP-адресу кінцевого пристрою з діапазону адрес DHCP. У другому випадку необхідно мати права адміністратора на сервері DHCP і вміти працювати з DHCP на сервері.

Крім того, ви можете зіткнутися з IP-конфліктами при ручному налаштуванні IP на прикінцевому пристрої в мережі, в якій використовуються тільки статичні IP-адреси. В цьому випадку необхідно визначити, які IP-адреси доступні в конкретній підмережі IP, і налаштувати їх відповідним чином. Цей випадок демонструє, наскільки важливо адміністраторам вести детальну документацію, в тому числі призначення IP-адрес для прикінцевих пристроїв.

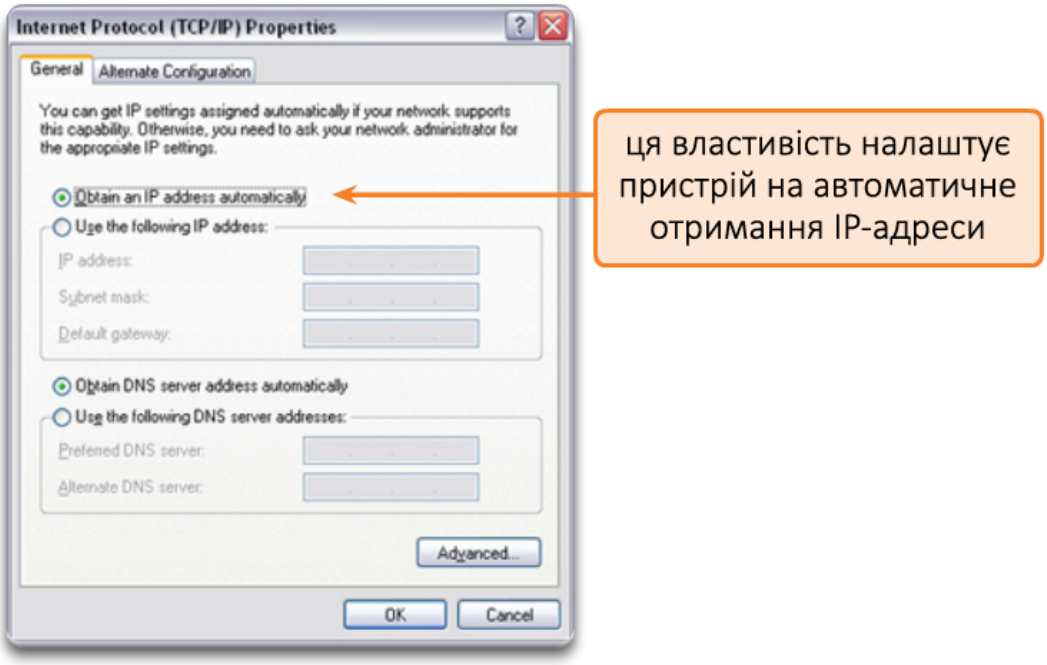

Рис. 5.3. Автоматичне одержання адрес

Введіть команду, щоб відобразити IP-конфігурацію на ПК з ОС Windows

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cisco.com
   Link-local IPv6 Address . . . . . :
fe80::b0ef:ca42:af2c:c6c7%16
   IPv4 Address. . . . . . . . . . . : 10.82.240.197
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.82.240.198

---------------------------------------
```

Відображення IP-конфігурації на ПК з ОС Windows виконано

Рис. 5.4. Перевірка IP-конфігурації на ПК з ОС Windows

Примітка. *Як правило, статичні IP-адреси використовуються для серверів і принтерів в мережах малого і середнього розміру, а дані IP, налаштовані автоматично за допомогою сервера DHCP, використовуються виділеними пристроями співробітників.*

Тестування логічного інтерфейсу Loopback

На рис. 5.5 показано перший крок в послідовності тестування логічного інтерфейсу **Loopback**. Для перевірки внутрішньої IP-конфігурації, на локальному вузлі використовується команда **`ping`**. Це тестування виконується за допомогою команди **`ping`** на зарезервованій loopback-адресі (127.0.0.1). Loopback-адреса, 127.0.0.1, визначається протоколом TCP/IP як зарезервована адреса, яка направляє пакети назад до вузла.

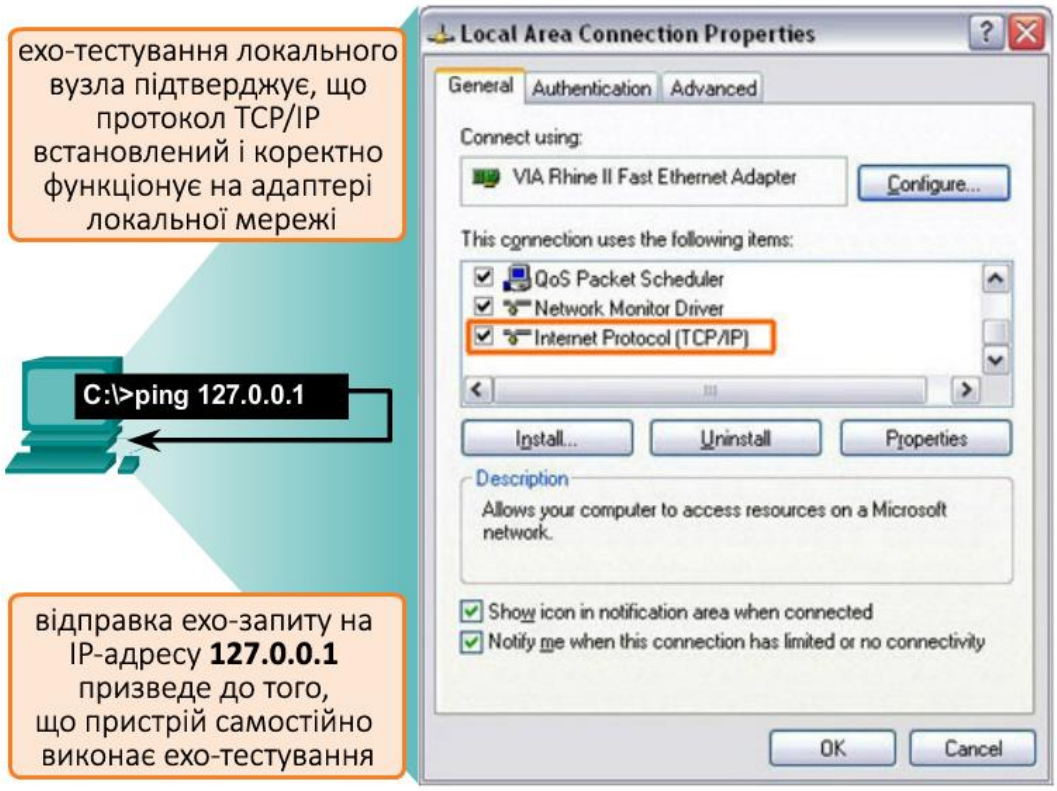

Рис. 5.5. Перевірка локального TCP/IP-стека

Команди **`ping`** вводяться в командному рядку на локальному вузлі за допомогою наступного синтаксису:

```
C:\> ping 127.0.0.1
```

Відповідь даної команди буде виглядати приблизно так:

```
Reply from 127.0.0.1: bytes = 32 time<1ms TTL = 128
Reply from 127.0.0.1: bytes = 32 time<1ms TTL = 128
Reply from 127.0.0.1: bytes = 32 time<1ms TTL = 128
Reply from 127.0.0.1: bytes = 32 time<1ms TTL = 128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Результат показує, що чотири тестових пакета, кожен по 32 байта, були відправлені і повернуті від вузла 127.0.0.1 швидше, ніж за 1 мс. Ці успішні ехо-запити доводять, що мережева інтерфейсна плата, драйвери і реалізація TCP/IP функціонують правильно.

Тестування призначення інтерфейсу

Так само, як ви використовуєте команди і утиліти для перевірки конфігурації вузла, ви використовуєте команди для перевірки інтерфейсів проміжних пристроїв. IOS надає команди для перевірки роботи інтерфейсів маршрутизатора і комутатора.

Перевірка інтерфейсів комутаторів. Використовуйте команду **`show ip interface brief`** для перевірки стану інтерфейсів комутаторів **S1** і **S2**, як показано на рис. 5.6. IP-адреса, призначена інтерфейсу **VLAN 1** на комутаторі **S1** – 192.168.10.2. IP-адреса, призначена інтерфейсу **VLAN 1** на комутаторі **S2** – 192.168.10.3. Фізичні інтерфейси **F0/1** і **F0/2** на комутаторі **S1** є робочими, як і фізичні інтерфейси **F0/1** і **F0/2** на комутаторі **S2**.

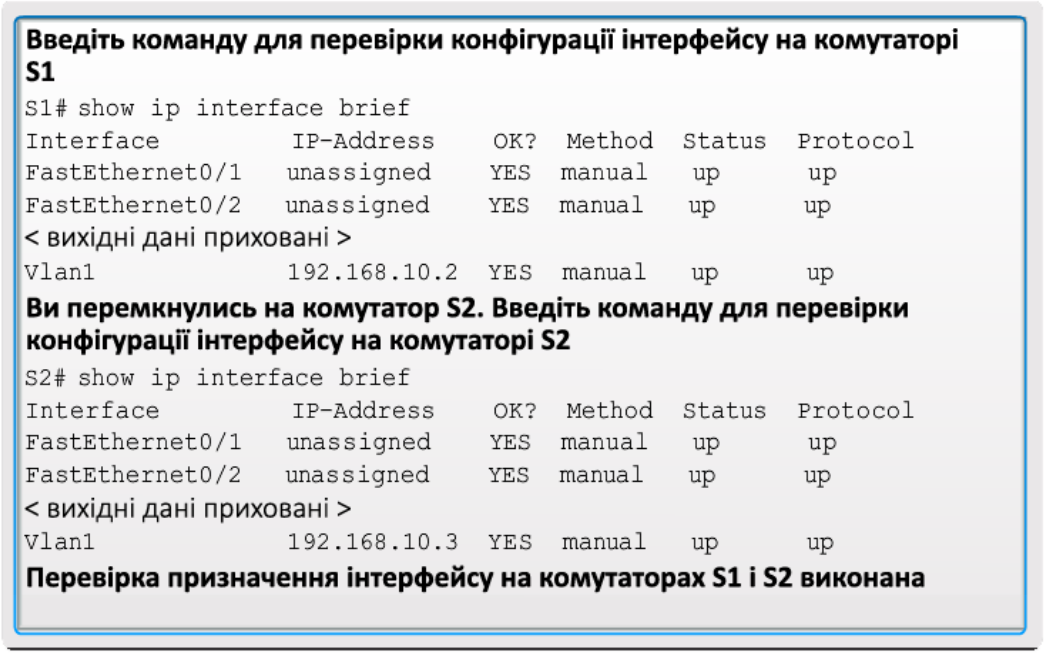

Рис. 5.6. Перевірка призначення інтерфейсу віртуальної локальної мережі (VLAN)

Тестування з'єднання між ПК і комутатором (наскрізного підключення)

Команду **`ping`** можна використовувати на ПК так само, як і на пристрої з Cisco IOS. На рис. 5.7 показано, що ехо-запит з ПК1 на IP-адресу інтерфейсу **VLAN 1** на комутаторі **S1**, 192.168.10.2 повинен бути виконаний успішно.

Тестування наскрізного підключення.

- IP-адреса ПК1 – 192.168.10.10, маска підмережі – 255.255.255.0, шлюз за замовчуванням – 192.168.10.1.
- IP-адреса ПК2 – 192.168.10.11, маска підмережі – 255.255.255.0, шлюз за замовчуванням – 192.168.10.1.

Ехо-запит з ПК1 на ПК2 також повинен бути виконаний успішно. Успішне тестування за допомогою команди **`ping`** з ПК1 на ПК2 підтверджує наскрізний зв'язок по мережі!

Ви знаходитесь в командному рядку для PC1. Введіть команду для перевірки підключення до інтерфейсу віртуальної локальної мережі (VLAN) на комутаторі S1 за адресою 192.168.10.2

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms
```

Введіть команду для перевірки підключення до PC2 за адресою 192.168.10.11

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>
```

Перевірка підключення до комутатора S1 і PC2 виконана

Рис. 5.7. Тестування наскрізного підключення

Завдання

Частина 1: Виконання базової конфігурації на комутаторах

Відкрийте у Packet Tracer файл ***lab*-5.*pka***.

Крок 1: Налаштуйте ім'я вузла для комутатора S1.

a. Клацніть **S1** і відкрийте вкладку **CLI**.
b. Введіть відповідну команду для налаштування імені вузла **S1**.

Крок 2: Налаштуйте паролі для консолі і привілейованого режиму.

a. В якості пароля консолі введіть **cisco**.
b. В якості пароля привілейованого режиму введіть **class**.

Крок 3: Перевірте паролі, налаштовані для S1.

a. Дайте відповідь на питання «**1.3a**» у формі **LW №5 CN Quiz**.

Крок 4: Налаштування повідомлення щоденного банера (MOTD).

a. Введіть текст попередження про несанкціонований доступ. Нижче представлено приклад тексту.

```
Authorized access only. Violators will be prosecuted to the full extent
of the law.
```

Крок 5: Збережіть файл конфігурації в NVRAM.

a. Дайте відповідь на питання «**1.5a**» у формі **LW №5 CN Quiz**.

Крок 6: Повторіть кроки 1-5 для комутатора S2.

Частина 2: Налаштування ПК

Налаштування IP-адрес для **PC1** і **PC2**.

Крок 1: Налаштуйте IP-адреси для обох ПК.

a. Клацніть на **PC1** і перейдіть на вкладку **Desktop** (Робочий стіл).
b. Натисніть кнопку **IP Configuration** (Налаштування IP-мережі). У таблиці адресації (табл. 5.1) можна побачити, що комп'ютер **PC1** повинен мати IP-адресу 192.168.1.1 і маску підмережі 255.255.255.0. Введіть ці дані для **PC1** у вікні **IP Configuration**.
c. Повторіть кроки **1a** і **1b** для комп'ютера **PC2**.

Таблиця 5.1. Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	Мережевий адаптер	192.168.1.1	255.255.255.0
PC2	Мережевий адаптер	192.168.1.2	255.255.255.0

Крок 2: Перевірка зв'язку з комутаторами.

a. Клацніть **PC1**. Закрийте вікно **IP Configuration**, якщо воно відкрито. На вкладці **Desktop** натисніть **Command Prompt** (Командний рядок).
b. Введіть команду **ping** з IP-адресою комутатора **S1** і натисніть клавішу **Enter**.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.253
```

c. Дайте відповідь на питання «**2.2c**» у наступному розділі форми **LW №5 CN Quiz**.

Частина 3: Налаштування інтерфейсу управління комутатором

Налаштування IP-адрес для комутаторів **S1** і **S2**.

Крок 1: Налаштування IP-адреси для комутатора S1.

Комутатори можна використовувати в якості пристрою «plug-and-play», тобто їх необов'язково потрібно налаштовувати для роботи. Комутатори пересилають дані між портами по MAC-адресам.

a. Дайте відповідь на питання «**3.1a**» у наступному розділі форми **LW №5 CN Quiz**.
b. Щоб налаштувати IP-адресу на комутаторі **S1**, використайте наступні команди.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
% LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
S1(config-if)#
S1(config-if)# exit
S1(config)# exit
S1#
```

c. Дайте відповідь на питання «**3.1c**» у формі **LW №5 CN Quiz**.

Крок 2: Налаштування IP-адрес для комутатора S2.

a. Використовуючи дані з таблиці адресації (табл. 5.1), налаштуйте IP-адресу для **S2**.

Крок 3: Перевірка налаштування IP-адрес на комутаторах S1 і S2.

a. Команда **`show ip interface brief`** інформує вас про IP-адресу, а також про стан всіх портів і інтерфейсів комутатора. Також, для одержання цієї інформації можна використовувати команду **`show running-config`**.

Крок 4: Збереження конфігурації для S1 і S2 в NVRAM.

a. Збережіть файли конфігурації для S1 і S2 з ОЗУ в NVRAM.
b. Дайте відповідь на питання «**3.4b**» у формі **LW №5 CN Quiz**.

Крок 5: Перевірте підключення до мережі.

Підключення до мережі можна перевірити за допомогою команди **`ping`**. Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вживати відповідні заходи по усуненню неполадок.

a. Клацніть **PC1** і відкрийте вкладку **Desktop** (Робочий стіл).
b. Клацніть **Command Prompt** (Командний рядок).
c. Надішліть ехо-запит на IP-адресу комп'ютера **PC2**.
d. Надішліть ехо-запит на IP-адресу комутатора **S1**.
e. Надішліть ехо-запит на IP-адресу комутатора **S2**.

Примітка. *Аналогічну команду* **`ping`** *можна використовувати в інтерфейсі командного рядка комутатора і на комп'ютері* **PC2***.*

Всі ехо-запити повинні бути оброблені успішно. Якщо для першого ехо-запиту було отримано 80% відповідей, спробуйте ще раз. Тепер результат повинен бути 100%. Пізніше ви дізнаєтесь, чому перший запит може дати збій. Якщо перевірити зв'язок з пристроями не вдається, перевірте конфігурацію на наявність помилок.