МЕРЕЖНА МАРШРУТИЗАЦІЯ ТА КОМУТАЦІЯ

Методичні вказівки до виконання лабораторних робіт

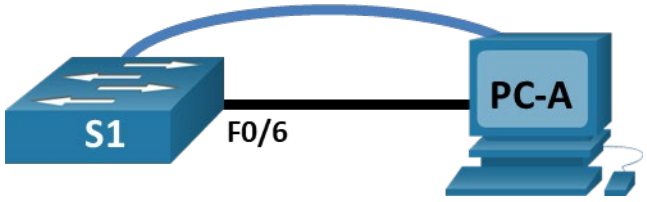
для студентів ЗДІА
спеціальності 121 «Інженерія програмного забезпечення»
денної та заочної форм навчання

Лабораторна робота 1

Тема: Packet Tracer. Базові налаштування комутатора, маршрутизатора

Лабораторна робота - Базове налаштування комутатора

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:3 /64
		fe80::3

Завдання

Частина 1: Створення мережі і перевірка налаштувань комутатора за замовчуванням

Частина 2: Налаштування базових параметрів мережних пристроїв

- Налаштуйте основні параметри комутатора.
- Налаштуйте відповідну IP-адресу на ПК.

Частина 3: Тестування та перевірка зв’язку в мережі

- Відобразіть конфігурації пристроїв.
- Протестуйте наскрізне з'єднання за допомогою команди ping.
- Протестуйте можливості віддаленого керування за допомогою Telnet.

Частина 4. Керування таблицею MAC-адрес

- Запишіть MAC-адресу вузла.
- Визначте отримані комутатором MAC-адреси.
- Перелічіть параметри команди **show mac address-table**.
- Налаштуйте статичну MAC-адресу.

Довідкова інформація / Сценарій

На комутаторах Cisco можна налаштовувати спеціальну IP-адресу, яка називається віртуальним інтерфейсом комутатора (SVI). SVI, або адресу керування, можна використовувати для віддаленого

доступу до комутатора з метою відображення або налаштування параметрів. Якщо SVI мережі VLAN 1 присвоєно IP-адресу, всі порти в VLAN 1 мають доступ до IP-адреси керування SVI за замовчуванням.

У цій лабораторній роботі вам потрібно побудувати просту топологію за допомогою кабелю Ethernet локальної мережі і отримати доступ до комутатора Cisco через консольне з'єднання і методи віддаленого доступу. Перед налаштуванням основних параметрів комутатора потрібно перевірити конфігурацію комутатора за замовчуванням. До основних параметрів комутатора належать: ім'я пристрою, опис інтерфейсу, локальні паролі, банерне повідомлення дня (MOTD), IP-адреса та статична MAC-адреса. Ви також використаєте IP-адресу керування для віддаленого керування комутатором. Топологія складається з одного комутатора і одного вузла, що використовують тільки порти Ethernet і консольні порти.

Примітка: Використовуються комутатори Cisco Catalyst 2960s під керуванням Cisco IOS Release 15.2(2) (образ lanbasek9). Можна використовувати інші комутатори та версії Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від показаних у лабораторній роботі.

Примітка: Переконайтесь, що налаштування на комутаторах були видалені, та пристрої не мають стартової конфігурації. Якщо ви в цьому не впевнені, зверніться до свого інструктора. Порядок ініціалізації та перезавантаження комутатора наведено в додатку A.

Шаблон **default bias**, який використовується за замовчуванням в диспетчері баз даних комутатора (SDM, Switch Database Manager), не забезпечує можливостей для використання IPv6-адрес. Переконайтеся, що SDM використовує шаблон **dual-ipv4-and-ipv6** або шаблон **lanbase-routing**. Новий шаблон буде використано після перезавантаження, навіть якщо конфігурацію не збережено.

```
S1# show sdm prefer
```

Використовуйте наведені нижче команди, щоб призначити шаблон **dual-ipv4-and-ipv6** як шаблон SDM за замовчуванням.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Необхідні ресурси

- 1 комутатор (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2) з образом lanbasek9 або аналогічним).
- 1 ПК (під керуванням Windows з програмою емуляції терміналу, наприклад, Tera Term).
- 1 консольний кабель для налаштування пристроїв Cisco IOS через консольний порт.
- 1 кабель Ethernet, як показано в топології.

Частина 1: Створення мережі і перевірка налаштувань комутатора за замовчуванням

У Частині 1 вам потрібно налаштувати топологію мережі та перевірити налаштування комутатора за замовчуванням.

Крок 1: З'єднайте пристрої відповідно до схеми топології.

a. Під'єднайте консольний кабель так, як показано в топології. На даному етапі не під'єднуйте кабель Ethernet комп'ютера PC-A.

Примітка: Якщо ви використовуєте Netlab, вимкніть F0/6 на S1. Це матиме такий же ефект, що і від'єднання PC-A від комутатора S1.

b. Під’єднайтеся до комутатора з PC-A за допомогою Tera Term або іншої програми емуляції терміналу.

   Чому необхідно використовувати консольне з'єднання для початкового налаштування комутатора? Чому немає можливості під'єднатися до комутатора через Telnet або SSH?

Крок 2: Перевірте конфігурацію комутатора за замовчуванням.

На цьому кроці вам потрібно перевірити такі параметри комутатора за замовчуванням: поточна конфігурація комутатора, інформація про IOS, властивості інтерфейсу, інформація про VLAN та флеш-пам'ять.

Ви можете отримати доступ до всіх команд комутатора у привілейованому режимі EXEC. Оскільки привілейований режим EXEC забезпечує прямий доступ до глобального режиму налаштування та команд, які використовуються для налаштування робочих параметрів, доступ до нього слід обмежувати за допомогою паролю, щоб запобігти несанкціонованому використанню. Паролі в цій лабораторній роботі ви встановите пізніше.

Набір команд привілейованого режиму EXEC включає в себе ті команди, які доступні в користувацькому режимі EXEC, а також команду **configure**, що забезпечує доступ до решти режимів. Введіть команду **enable** для входу в привілейований режим EXEC.

a. Припустимо, що комутатор не мав конфігураційного файлу, який зберігається в енергонезалежній пам'яті (NVRAM). Консольне з'єднання за допомогою Tera Term або іншої програми емуляції терміналу надасть вам доступ до командного рядка користувацького режиму EXEC на комутаторі з підказкою Switch>. Введіть команду **enable** для входу в привілейований режим EXEC.

   Зауважте, що позначення в рядку конфігурації змінилось на таке, що відповідає привілейованому режиму EXEC.

   Переконайтеся, що файл конфігурації за замовчуванням на комутаторі порожній, за допомогою команди **show running-config** привілейованого режиму EXEC. Якщо файл конфігурації раніше був збережений, його необхідно видалити. Залежно від моделі комутатора і версії IOS ваша конфігурація може відрізнятись. Однак в конфігурації не повинно бути налаштованих паролів чи IP-адрес. Якщо ваш комутатор має конфігурації, які відрізняються від конфігурацій за замовчуванням, видаліть налаштування і перезавантажте комутатор.

   Примітка: В Додатку А докладно описано кроки для ініціалізації та перезавантаження комутатора.

b. Проаналізуйте файл поточної конфігурації.

   Скільки інтерфейсів FastEthernet має комутатор 2960?

   Скільки інтерфейсів Gigabit Ethernet має комутатор 2960?

   Який діапазон значень показано для ліній vty?

c. Перегляньте файл стартової конфігурації, який зберігається в енергонезалежній пам'яті NVRAM.

   Чому з'являється це повідомлення?

d. Проаналізуйте характеристики SVI для VLAN 1.

Чи присвоєно IP-адресу VLAN 1?

Яку MAC-адресу має SVI? Відповіді можуть відрізнятися.

Цей інтерфейс працює?

e. Вивчіть IP-властивості SVI мережі VLAN 1.

Які вихідні дані ви бачите?

f. Під'єднайте кабель Ethernet від PC-A до порту 6 на комутаторі і перегляньте IP-властивості SVI мережі VLAN 1. Дочекайтеся узгодження параметрів дуплексу і швидкості між комутатором і ПК .

Примітка: Якщо ви використовуєте Netlab, увімкніть інтерфейс F0/6 на S1.

Які вихідні дані ви бачите?

g. Перевірте інформацію про версію Cisco IOS комутатора.

Яка версія Cisco IOS встановлена на комутаторі?

Як називається файл образу системи?

Яка базова MAC-адреса цього комутатора?

h. Вивчіть властивості за замовчуванням інтерфейсу FastEthernet, який використовується PC-A.

```
Switch# show interface f0/6
```

Інтерфейс увімкнений (up) чи вимкнений (down)?

Що потрібно зробити, щоб увімкнути інтерфейс?

Яка MAC-адреса інтерфейсу?

Які налаштування швидкості і дуплексу задано на інтерфейсі?

i. Вивчіть налаштування VLAN за замовчуванням комутатора.

Яке ім'я за замовчуванням вказано для VLAN 1?

Які порти є в мережі VLAN 1?

Чи активна мережа VLAN 1?

До якого типу мереж VLAN належить VLAN за замовчуванням?

j. Перегляньте вміст флеш-пам’яті.

Виконайте одну з наступних команд, щоб переглянути вміст каталогу flash.

```
Switch# show flash
Switch# dir flash:
```

Файли мають розширення, наприклад .bin, в кінці імені файлу. Каталоги не мають розширення файлу.

Як називається файл образу Cisco IOS?

Частина 2: Налаштування базових параметрів мережних пристроїв

У Частині 2 ви налаштовуватимете основні параметри комутатора і ПК.

Крок 1: Налаштуйте основні параметри комутатора.

a. Увійдіть в режим глобальної конфігурації на комутаторі S1, скопіюйте наведену базову конфігурацію і вставте її.

```
no ip domain-lookup
hostname S1
```

```
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
```

b. Призначте IP-адресу інтерфейсу SVI на комутаторі. Це дозволить дистанційно керувати комутатором.

Щоб можна було з PC-A віддалено керувати комутатором S1, необхідно призначити йому IP-адресу. У конфігурації за замовчуванням на комутаторі повинно бути налаштоване керування комутатором через VLAN 1. Однак в базовій конфігурації комутатора не рекомендується назначати VLAN1 в якості керуючої VLAN.

З метою керування використовуйте VLAN 99. Вибір VLAN 99 є довільним і жодним чином не передбачає, що завжди слід використовувати VLAN 99.

Спочатку створіть нову VLAN 99 на комутаторі. Потім налаштуйте IP-адресу 192.168.1.2 з маскою підмережі 255.255.255.0 на внутрішньому віртуальному інтерфейсі (SVI) VLAN 99. Також можна налаштувати адресу IPv6 на інтерфейсі SVI. Використовуйте адреси IPv6, зазначені в таблиці адресації.

Зверніть увагу, що інтерфейс VLAN 99 знаходиться в стані down, незважаючи на те, що ви ввели команду **no shutdown**. Інтерфейс зараз вимкнений, оскільки для VLAN 99 не призначені порти комутатора.

c. Призначте всі користувацькі порти для VLAN 99.

Для встановлення зв'язку між вузлом і комутатором порти, які використовуються вузлом, повинні знаходитися в тій самій VLAN, що і комутатор. Зверніть увагу, що у вищенаведених вихідних даних інтерфейс VLAN 1 вимкнений, оскільки жоден з портів не призначено мережі VLAN 1. Через кілька секунд VLAN 99 перейде в стан up тому, що принаймні один активний порт (F0/6 з під'єднаним PC-A) тепер призначений мережі VLAN 99.

d. Щоб переконатися, що всі порти знаходяться в мережі VLAN 99, виконайте команду **show vlan brief**.

e. Налаштуйте шлюз за замовчуванням на комутаторі S1. Якщо не встановлено шлюз за замовчуванням, комутатором не можна керувати з віддаленої мережі, на шляху до якої є більше одного маршрутизатора. Хоча в цьому завданні не враховується зовнішній IP-шлюз, припустимо, що ви в кінцевому підсумку під’єднаєте LAN до маршрутизатора для зовнішнього доступу. Припускаючи, що інтерфейс LAN на маршрутизаторі має адресу 192.168.1.1, налаштуйте для комутатора шлюз за замовчуванням.

f. Доступ до порту консольної лінії також слід обмежити паролем. Використовуйте **cisco** як пароль для входу в консоль у цьому завданні. Конфігурація за замовчуванням дозволяє всі консольні з'єднання без пароля. Щоб консольні повідомлення не припиняли виконання команд, використовуйте параметр **logging synchronous**.

```
S1(config)# line con 0
S1(config-line)# logging synchronous
```

g. Налаштуйте лінії віртуального терміналу (vty) на комутаторі, щоб дозволити доступ через telnet. Якщо ви не налаштуєте пароль VTY, ви не зможете під'єднатися до комутатора через Telnet.

Для чого потрібна команда **login**?

Крок 2: Налаштуйте IP-адресу на PC-A.

Призначте ПК IP-адресу та маску підмережі згідно з таблицею адресації. Тут описано скорочений варіант даної процедури. Шлюз за замовчуванням не потрібен для цієї топології; однак, ви можете ввести **192.168.1.1** і **fe80::1**, щоб імітувати маршрутизатор, під'єднаний до комутатора S1.

1) Перейдіть до **Панелі керування (Control Panel)**.
2) У розділі Категорія (Category) виберіть **Переглянути стан мережі та завдання (View network status and tasks)**.
3) Натисніть **Змінити налаштування адаптера (Change adapter settings)** на лівій панелі.
4) Натисніть правою кнопкою миші на інтерфейсі **Ethernet** і оберіть пункт **Властивості (Properties)**.
5) Виберіть **Протокол Інтернету версії 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))** та натисніть кнопку **Властивості (Properties)**.
6) Оберіть **Використовувати наступну IP-адресу (Use the following IP address)**, введіть IP-адресу, маску підмережі та шлюз за замовчуванням і натисніть **OK**.
7) Оберіть **Протокол Інтернету версії 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))** і натисніть на кнопку **Властивості (Properties)**.
8) Оберіть **Використовувати наступну адресу IPv6 (Use the following IPv6 address)** і введіть адресу IPv6 та префікс IPv6 і натисніть кнопку **OK**.
9) Натисніть **OK**, щоб закрити вікно Властивості.

Частина 3: Тестування та перевірка зв’язку в мережі

У Частині 3 вам потрібно перевірити та задокументувати конфігурацію комутатора, протестувати наскрізний зв'язок між PC-A і S1, а також перевірити можливість віддаленого керування комутатором.

Крок 1: Відобразіть конфігурацію комутатора.

Використовуйте консольне з'єднання на PC-A для відображення та перевірки конфігурації комутатора. Команда **show run** дозволяє відобразити всю конфігурацію посторінково. Використовуйте клавішу пробілу для гортання сторінок.

a. Зразок конфігурації наведено нижче. Налаштовані вами параметри підсвічуються жовтим кольором. Інші параметри конфігурації - це параметри IOS за замовчуванням.

```
S1# show run
Building configuration...

Current configuration : 2206 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
```

```
enable secret 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
 switchport access vlan 99
!
interface GigabitEthernet0/2
 switchport access vlan 99
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD::2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 15
 password 7 121A0C041104
 login
!
end
```

b. Перевірте налаштування VLAN керування - VLAN 99.

```
S1# show interface vlan 99
```

Яка пропускна здатність цього інтерфейсу?

В якому стані знаходиться VLAN 99?

В якому стані знаходиться канальний протокол?

Крок 2: Протестуйте наскрізне з'єднання за допомогою команди ping.

a. З командного рядка на комп'ютері PC-A за допомогою команди ping перевірте зв'язок, спочатку вказавши адресу PC-A.

```
C:\> ping 192.168.1.10
```

b. З командного рядка на комп'ютері PC-A за допомогою команди ping перевірте зв'язок, вказавши адресу інтерфейсу керування SVI комутатора S1.

```
C:\> ping 192.168.1.2
```

Оскільки PC-A повинен перетворити MAC-адресу S1 за допомогою ARP, час очікування першого пакету може закінчитися. Якщо виконання команди ping і далі невдале, знайдіть та виправіть помилки основних налаштувань пристрою. Перевірте як фізичні кабелі, так і логічну адресацію.

Крок 3: Протестуйте і перевірте віддалене керування комутатором S1.

Тепер ви використовуватимете Telnet для віддаленого доступу до комутатора. У цій лабораторній роботі пристрої PC-A і S1 знаходяться поруч. У корпоративній мережі комутатор може знаходитись в комутаційній шафі на верхньому поверсі, а адміністративний ПК - на першому поверсі. На цьому кроці ви скористаєтесь Telnet для віддаленого доступу до комутатора S1, використовуючи його адресу керування для SVI. Telnet не є захищеним протоколом; однак, ви використаєте його для перевірки віддаленого доступу. Під час сеансу Telnet вся інформація, включаючи паролі та команди, надсилається у вигляді відкритого тексту. У наступних лабораторних роботах ви будете використовувати протокол SSH для віддаленого доступу до мережних пристроїв.

a. Відкрийте Tera Term або іншу програму емуляції терміналу з можливістю Telnet.

b. Виберіть сервер Telnet і вкажіть адресу керування для SVI для під'єднання до S1. Пароль - **cisco**.

c. Після введення пароля **cisco** ви опинитеся в командному рядку користувацького режиму EXEC. Для доступу до привілейованого режиму EXEC введіть команду **enable** і використайте секретний пароль **class**.

d. Збережіть конфігурацію.

e. Для завершення сеансу Telnet введіть **exit**.

Частина 4: Керування таблицею MAC-адрес

У Частині 4 вам потрібно визначити MAC-адресу, яку отримав комутатор, налаштувати статичну MAC-адресу на одному інтерфейсі комутатора, а потім видалити статичну MAC-адресу з цього інтерфейсу.

Крок 1: Запишіть MAC-адресу вузла.

Відкрийте командний рядок на PC-A і введіть команду **ipconfig /all**, щоб визначити та записати адреси 2 рівня (фізичні) мережного адаптера (NIC).

Крок 2: Визначте MAC-адреси, які отримав комутатор.

Відобразіть MAC-адреси за допомогою команди **show mac address-table**.

```
S1# show mac address-table
```

Скільки динамічних адрес?

Скільки всього є MAC-адрес?

Чи відповідає динамічна MAC-адреса MAC-адресі комп'ютера PC-A?

Крок 3: Перелічіть параметри команди show mac address-table.

a. Відобразіть параметри таблиці MAC-адрес.

```
S1# show mac address-table ?
```

Скільки параметрів доступно для команди **show mac address-table**?

b. Введіть команду **show mac address-table dynamic**, щоб відобразити тільки MAC-адреси, які були отримані динамічно.

```
S1# show mac address-table dynamic
```

Скільки динамічних адрес?

c. Перегляньте запис MAC-адреси для комп'ютера PC-A. Формат MAC-адреси для команди - xxxx.xxx.xxxx.

```
S1#show mac address-table address <PC-A MAC here>
```

Крок 4: Налаштуйте статичну MAC-адресу.

a. Очистіть таблицю MAC-адрес.

Щоб видалити наявні MAC-адреси, використовуйте команду привілейованого режиму EXEC **clear mac address-table dynamic**.

```
S1# clear mac address-table dynamic
```

b. Переконайтеся, що таблицю MAC-адрес очищено.

```
S1# show mac address-table
```

Скільки статичних MAC-адрес є в таблиці?

Скільки динамічних адрес?

c. Перевірте таблицю MAC-адрес ще раз.

Більш ніж імовірно, програма, яка запущена на вашому ПК, вже надіслала кадр з мережного адаптера (NIC) до комутатора S1. Перегляньте таблицю MAC-адрес ще раз у привілейованому режимі EXEC, щоб побачити, чи була MAC-адреса комп'ютера PC-A повторно отримана комутатором S1.

```
S1# show mac address-table
```

Скільки динамічних адрес?

Чому це значення змінилося з минулого разу?

Якщо комутатор S1 ще не отримав повторно MAC-адресу для PC-A, пропінгуйте IP-адресу VLAN 99 комутатора з PC-A, а потім повторіть команду **show mac address-table**.

d. Налаштуйте статичну MAC-адресу.

Одним з варіантів вказати, до яких портів може під'єднуватися вузол, є створення статичного зіставлення MAC-адреси вузла з портом.

Налаштуйте статичну MAC-адресу на інтерфейсі F0/6 за допомогою адреси, записаної для PC-A на Кроці 1 Частини 4. MAC-адреса 0050.56BE.6C89 використовується лише в якості прикладу. Вам слід використати MAC-адресу комп'ютера PC-A, яка відрізняється від наведеної тут в якості прикладу.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

e. Перевірте записи таблиці MAC-адрес.

```
S1# show mac address-table
```

Скільки всього MAC-адрес є в таблиці?

Скільки статичних MAC-адрес є в таблиці?

f. Видаліть статичний запис MAC-адреси. Увійдіть в режим глобальної конфігурації і видаліть команду, поставивши **no** перед рядком з командою.

Примітка. MAC-адреса 0050.56BE.6C89 використовується тільки для прикладу. Використовуйте MAC-адресу комп'ютера PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

g. Переконайтеся, що статична MAC-адреса була видалена.

```
S1# show mac address-table
```

Скільки всього статичних MAC-адрес в таблиці?

Питання для самоперевірки

1. Для чого налаштовувати пароль vty на комутаторі?

2. Навіщо змінювати VLAN 1 за замовчуванням на VLAN з іншим номером?

3. Як заборонити надсилання паролів у вигляді відкритого тексту?

4. Навіщо налаштовувати статичну MAC-адресу на інтерфейсі порту?

Додаток A: Ініціалізація та перезавантаження комутатора

a. З консольного режиму комутатора увійдіть до привілейованого режиму EXEC.

```
Switch> enable
Switch#
```

b. Використайте команду **show flash**, щоб визначити, чи були створені мережі VLAN на комутаторі.

```
Switch# show flash
Directory of flash:/

    2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text
    3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text
    4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs
    5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
    6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)
```

c. Якщо файл **vlan.dat** був виявлений у flash, видаліть його.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

d. Вам буде запропоновано перевірити ім'я файлу. Якщо ви ввели ім'я файлу правильно, натисніть Enter; або ви можете змінити ім'я файлу.

   Вам буде запропоновано підтвердити видалення цього файлу. Натисніть Enter, щоб підтвердити.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

e. Скористайтеся командою **erase startup-config** для видалення файлу стартової конфігурації з NVRAM. Вам буде запропоновано видалити файл конфігурації. Натисніть Enter, щоб підтвердити.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

f. Для видалення з пам'яті будь-якої попередньої інформації про конфігурацію необхідно перезавантажити комутатор. Після цього ви отримаєте запит на підтвердження перезавантаження. Натисніть клавішу Enter, щоб продовжити.

```
Switch# reload
Proceed with reload? [confirm]
```

   Примітка: може з'явитися пропозиція зберегти поточну конфігурацію. Відповідайте, ввівши **no**, і натисніть клавішу Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

g. Після перезавантаження комутатора ви побачите пропозицію скористатися діалогом для початкових налаштувань. Відповідайте, ввівши **no**, і натисніть клавішу Enter.

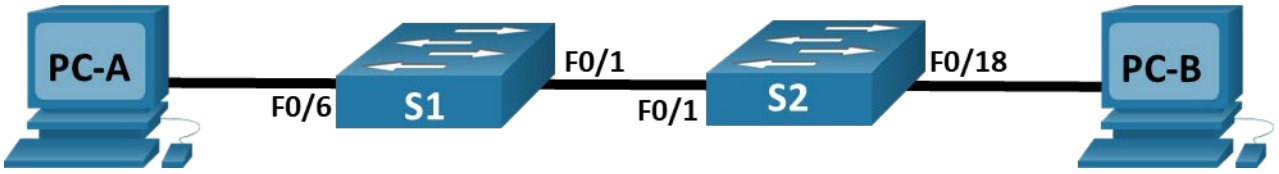
```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Лабораторна робота 2

Тема: Packet Tracer. Налаштування мереж VLAN та магістральних каналів

Лабораторна робота - Налаштування VLAN та транкових каналів

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1

Цілі та задачі

Частина 1. Побудова мережі та налаштування базових параметрів пристрою

Частина 2. Створення VLAN і налаштування належності портів комутатора

Частина 3. Ведення бази даних VLAN та належностей портів до VLAN

Частина 4. Налаштування транкового каналу 802.1Q між комутаторами

Частина 5. Видалення бази даних VLAN

Довідкова інформація / Сценарій

Сучасні комутатори використовують віртуальні локальні мережі (VLANs, Virtual Local Area Networks) для поліпшення продуктивності мережі, розділяючи великі широкомовні домени рівня 2 на менші. Також VLAN можна використовувати як засіб безпеки, встановивши контроль над процесом взаємодії вузлів. Загалом, VLAN спрощують проектування мережі для досягнення цілей організації.

Транкові канали зв'язку використовуються для поєднання VLAN, які створені на багатьох пристроях. Транкові канали надають змогу передавати трафік кількох VLAN по одному фізичному каналу, зберігаючи при цьому ідентифікацію VLAN та сегментацію мережі в цілому.

У цій лабораторій роботі Ви створите VLAN на двох комутаторах мережі, налаштуєте належність портів комутаторів до відповідних VLAN, переконаєтеся, що VLAN працюють належним чином, і також створите транковий канал зв'язку між двома комутаторами, щоб дозволити вузлами однієї VLAN передавати свої дані незалежно від того, до якого комутатора підключений вузол.

Примітка: У лабораторних роботах курсу CCNA використовуються комутатори Cisco Catalyst 2960s з операційною системою Cisco IOS Release 15.2(2) (образ lanbasek9). Також можна використовувати інші моделі маршрутизаторів і комутаторів та інші версії Cisco IOS. Залежно від моделі комутатора та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані у лабораторній роботі. Для правильної ідентифікації інтерфейсів пристроїв скористайтеся таблицею, що наведена у кінці лабораторної роботи.

Примітка: Переконайтесь, що налаштування комутаторів були видалені та комутатори не мають стартових конфігурацій. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- Два комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2), образ lanbasek9 або аналогічний).
- 2 комп'ютери (Windows з термінальним застосунком, наприклад, Tera Term).
- Консольні кабелі для налаштування операційної системи Cisco IOS пристроїв через консольні порти.
- Кабелі Ethernet, що показані в топології мережі.

Інструкції

Частина 1. Створення мережі та налаштування базових параметрів пристрою

У частині 1 лабораторної роботи Ви створите топологію мережі та налаштуєте базові параметри комп'ютерів та комутаторів.

Крок 1. З'єднання пристроїв мережі, відповідно до топології.

Приєднайте пристрої відповідними кабелями, як показано на схемі топології мережі.

Крок 2. Налаштування базових параметрів кожного комутатора.

a. Під'єднайтеся до комутатора за допомогою консольного кабеля і увійдіть до привілейованого режиму EXEC.

b. Перейдіть до режиму глобальної конфігурації.

c. Встановіть назву комутатору.

d. Вимкніть пошук DNS (DNS lookup) на комутаторі для відключення процедури трактування неправильно введених команд як назви вузлів.

e. Встановіть пароль **class** як зашифрований пароль для входу до привілейованого режиму EXEC.

f. Встановіть пароль **cisco** як пароль консольній лінії і активуйте аутентифікацію.

g. Встановіть пароль **cisco** як пароль для входу через віртуальні лінії і активуйте аутентифікацію.

h. Зашифруйте всі паролі, які відображаються у відкритому вигляді.

i. Створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено.

j. Налаштуйте на комутаторі IP-адресу, зазначену в таблиці адресації для VLAN 1.

k. Вимкніть всі інтерфейси, які не будуть використовуватися.

l. Налаштуйте час на комутаторі.

m. Збережіть поточну конфігурацію як стартову конфігурацію.

Крок 3. Налаштування комп'ютерів.

Скористайтеся таблицею адресації для отримання інформації щодо адрес вузлів.

Крок 4. Перевірка зв'язку.

Перевірте можливість зв'язку між комп'ютерами мережі за допомогою команди ping.

Примітка: Можливо, для перевірку зв'язку Вам доведеться відключити брандмауери на Ваших комп'ютерах.

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютерами PC-A та PC-B?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютером PC-A та комутатором S1?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютером PC-B та комутатором S2?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комутаторами S1 та S2?

Якщо Ви відповіли "ні" на всі перераховані вище питання, поясніть чому перевірка зв'язку за допомогою команди ping була невдалою.

Частина 2. Створення VLAN і налаштування належності портів комутатора до VLAN

У частині 2 лабораторної роботи Ви створите чотири VLAN (Management, Operations, Parking_Lot, Native) на обох комутаторах мережі. Також Ви налаштуєте належність інтерфейсів до відповідних VLAN. Для перевірки виконаних Вами налаштувань застосовуйте команду **show vlan**.

Крок 1. Створення VLAN на комутаторах мережі.

a. Створіть VLAN на комутаторі S1.

```
S1(config)# vlan 10
S1 (config-vlan) # name Operations
S1(config-vlan)# vlan 20
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# end
```

b. Створіть ті ж VLAN на комутаторі S2.

c. Виконайте команду **show vlan brief** для перегляду список VLAN на комутаторі S1.

```
S1# show vlan brief

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
                                                Gi0/1, Gi0/2
10 Operations active
20 Parking_Lot active
99 Management active
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddi-default act/unsup
1005 trnet-default act/unsup
```

Якою є VLAN за замовчуванням?

Які порти належать до VLAN за замовчуванням?

Крок 2. Налаштування належності інтерфейсів комутаторів до відповідних VLAN.

a. Налаштувати належність інтерфейсів до VLAN для комутатора S1.

1) Налаштувати належність PC-A до VLAN Operation.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode acces
S1(config-if)# switchport access vlan 10
```

2) Перепризначити IP-адресу комутатора до VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

b. Виконайте команду **show vlan brief** та перевірте, чи коректно встановлено належність інтерфейсів до відповідних VLAN.

c. Виконайте команду **show ip interface brief**.

У якому стані знаходиться VLAN 99? Поясніть.

d. Налаштувати належність PC-B до VLAN Operation на комутаторі S2.

e. Видаліть IP-адресу для VLAN 1 на комутаторі S2.

f. Налаштуйте IP-адресу для VLAN 99 на комутаторі відповідно до даних таблиці адресації.

g. Використайте команду **show vlan brief** для перевірки, чи коректно встановлено належність інтерфейсів до відповідних VLAN .

Чи буде вдалою перевірка зв'язку за допомогою команди ping між комутаторами S1 та S2? Поясніть.

Чи буде вдалою перевірка зв'язку за допомогою команди ping між комп'ютерами PC-A пінг PC-B? Поясніть.

Частина 3. Ведення бази даних VLAN та належностей портів до VLAN

У частині 3 лабораторної роботи Ви зміните належність портів до VLAN та видалите VLAN з бази даних VLAN.

Крок 1. Налаштування належності кількох інтерфейсів до певної VLAN.

a. Налаштуйте належність інтерфейсів F0/11 — 24 до VLAN 99 на комутаторі S1.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# end
```

b. Виконайте команду **show vlan brief**, щоб перевірити налаштування належності до VLAN.

c. Змініть належність інтерфейсів F0/11 та F0/21 так, щоб вони належали до VLAN 10.

d. Переконайтеся, що налаштування належності до VLAN виконано правильно.

Крок 2. Видалення налаштувань належності інтерфейсів до VLAN.

a. Використайте команду **no switchport access vlan**, щоб видалити налаштування належності інтерфейсу F0/24 до VLAN 99.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Переконайтеся, що зміни щодо належності до VLAN було виконано.

До якої VLAN зараз належить інтерфейс F0/24?

Крок 3. Видалення VLAN з бази даних VLAN.

a. Налаштуйте належність інтерфейсу F0/24 до VLAN 30 без виконання команд створення VLAN у режимі конфігурування параметрів бази даних VLAN.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Примітка**: Технології, які нині застосовуються на сучасних комутаторах, не потребуються виконання команди** для додавання нової VLAN до бази даних. У процесі налаштування належності інтерфейсу до невідомої VLAN, ця невідома VLAN буде автоматично створена і додана до бази даних VLAN.

b. Переконайтеся, що нова VLAN відображається у переліку VLAN комутатора.

Яку назву за замовчуванням отримала VLAN 30?

a. Використайте команду **no vlan 30** для видалення VLAN 30 з бази даних VLAN.

```
S1(config)# no vlan 30
S1(config)# end
```

b. Виконайте команду **show vlan brief**. Інтерфейс F0/24 належав до VLAN 30.

Після видалення VLAN 30 з бази даних VLAN, до якої VLAN належатиме порт F0/24? Що відбуватиметься з трафіком, який призначеним вузлові підключеному до F0/24?

c. Виконайте команду **no switchport access vlan** на інтерфейсі F0/24.

d. Виконайте команду **show vlan brief**, щоб перевірити належність порту F0/24 до VLAN.

До якої VLAN належить порт F0/24?

Примітка.**: Перед видаленням VLAN з бази даних VLAN рекомендується змінити належність всіх портів цієї VLAN.**

Чому слід змінювати належність порту до іншої VLAN перед видаленням VLAN з бази даних VLAN?

Частина 2. Налаштування транкового каналу 802.1Q між комутаторами

У частині 4 лабораторної роботи Ви налаштуєте функціонування протоколу DTP (Dynamic Trunking Protocol) на інтерфейсі F0/1 для узгодження режиму транкування каналу зв'язку. Після того, як налаштування буде виконано і перевірено, Ви деактивуєте DTP на інтерфейсі F0/1 і вручну налаштуєте цей інтерфейс як транковий.

Крок 1. Використання протоколу DTP для ініціювання транкування на інтерфейсі F0/1.

Для інтерфейсів комутаторів Cisco Catalyst 2960 режимом протоколу DTP за замовчуванням є режим Dynamic Auto. Це дає змогу інтерфейсу перевести канал зв'язку у транковий режим, якщо сусідній інтерфейс налаштований для функціонування у режимі Trunk або у режимі Dynamic Desirable.

a. Налаштуйте для інтерфейсу F0/1 комутатора S1 режим узгодження параметрів транкового каналу.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Ви повинні отримувати повідомлення про стан каналу на комутаторі S2.

```
S2#
Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

b. Виконайте команду **show vlan brief** на комутаторах S1 і S2. Інтерфейс F0/1 більше не належить VLAN 1. Транкові інтерфейси не відображаються у таблиці VLAN, яка отримана після виконання команди.

c. Виконайте команду **show interfaces trunk** для перегляду транкових інтерфейсів. Зверніть увагу на те, що на комутаторі S1 налаштований режим "Desirable", а на комутаторі S2 - "Auto".

```
S1# show interfaces trunk

S2# show interfaces trunk
```

Примітка: За замовчуванням трафік всіх VLAN дозволено передавати через транковий канал. За допомогою команди **switchport trunk** можна встановлювати лише ті VLAN, трафік яких дозволяється передавати через транковий канал. Для виконання цієї лабораторної роботи збережіть налаштування за замовчуванням, які дозволяють передавати трафік всіх VLAN через інтерфейс F0/1.

d. Переконайтеся, що трафік VLAN передається по транковому каналу через інтерфейс F0/1.

Чи є вдалою перевірка зв'язку за допомогою команди ping між комутаторами S1 та S2?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютерами PC-A та PC-B?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютером PC-A та комутатором S1?

Чи є вдалою перевірка зв'язку за допомогою команди ping між комп'ютером PC-B та комутатором S2?

Якщо ви відповіли "ні" на одне з перерахованих вище питань, поясніть нижче.

Крок 2. Ручне налаштування транкового інтерфейс F0/1.

Команда **switchport mode trunk** використовується для ручного налаштування порту як транкового. Цю команду слід виконувати на обох кінцях каналу.

a. Змініть режим порту F0/1 комутатора для примусового створення транкового каналу. Обов'язково зробіть це на обох комутаторах.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Виконайте команду **show interfaces trunk** для перегляду режимів транкових інтерфейсів. Зверніть увагу на те, що режим змінено з **Desirable** на **on**.

```
S2# show interfaces trunk
```

c. Модифікуйте налаштування транкових інтерфейсів на обох комутаторах, змінивши Native VLAN з VLAN 1 на VLAN 1000.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 1000
```

d. Виконайте команду show interfaces trunk для перегляду режимів транкових інтерфейсів. Зверніть увагу на те, що інформація щодо Native VLAN оновлюється.

```
S2# show interfaces trunk
```

Чому Вам доведеться вручну налаштувати режим транкового інтерфейсу замість використання протоколу DTP?

Чому Ви можете змінити Native VLAN для транкового каналу зв'язку?

Частина 3. Видалення бази даних VLAN

У частині 5 лабораторної роботи Ви видалите базу даних VLAN комутатора. Цю дію виконують у тому випадку, якщо для комутатора необхідно встановити початкові налаштування за замовчуванням.

Крок 1. Визначення, чи існує база даних VLAN.

Виконайте команду **show flash**, щоб визначити, чи наявний файл **vlan.dat** у flash-пам'яті комутатора.

```
S1# show flash:
```

Примітка: Якщо файл vlan.dat, наявний у flash-пам'яті, це не означає, що база даних VLAN містить налаштування за замовчуванням.

Крок 2. Видалення бази даних VLAN.

a. Виконайте команду **delete vlan.dat**, щоб видалити файл vlan.dat з flash-пам'яті і повернути базу даних VLAN до початкових налаштувань за замовчуванням. Вам буде запропоновано двічі підтвердити Ваш намір видалити файл vlan.dat. Обидва рази натисніть клавішу Enter.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

b. Виконайте команду **show flash**, щоб переконатися в тому, що файл vlan.dat був видалений.

```
S1# show flash:
```

Які інші команди потрібно виконати, що відновити налаштування комутатора за замовчуванням?

Питання для самоперевірки

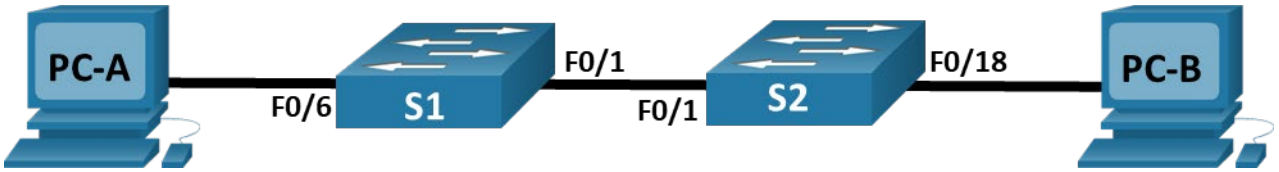
1. Що потрібно для того, щоб надати можливість взаємодії вузлам, що належать до VLAN 10 з вузлами, що належать до VLAN 99?

2. Які основні переваги організація може отримати завдяки ефективному використанню VLAN?

Лабораторна робота 3
Тема: Packet Tracer. Налаштування маршрутизації між мережами VLAN з використанням конфігурації router-on-stick

Лабораторна робота - Впровадження VLAN та транкових каналів

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
S1	VLAN 10	192.168.10.11	255.255.255.0
	VLAN 20	192.168.20.11	255.255.255.0
	VLAN 30	192.168.30.11	255.255.255.0
S2	VLAN 10	192.168.10.12	255.255.255.0
PC-A	NIC	192.168.20.13	255.255.255.0
PC-B	NIC	192.168.30.13	255.255.255.0

Таблиця VLAN

VLAN	Назва VLAN	Належність інтерфейсу
10	Management	S1: VLAN 10 S2: VLAN 10
20	Sales	S1: VLAN 20 та F0/6
30	Operations	S1: VLAN 30 S2: F0/18
999	Parking_Lot	S1: F0/2-5, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
1000	Native	N/A

Цілі та задачі

Частина 1. Створення мережі та налаштування базових параметрів пристрою

Частина 2. Створення VLAN і налаштування належності портів комутатора

Частина 3: Налаштування транкового каналу 802.1Q між комутаторами

Довідкова інформація / Сценарій

Сучасні комутатори використовують віртуальні локальні мережі (VLAN) для поліпшення продуктивності мережі, розділяючи великі широкомовні домени рівня 2 на менші. VLAN вирішують проблеми масштабованості, безпеки та керування мережею. Загалом, VLAN спрощують проектування мережі для досягнення цілей організації. Зв'язок між VLAN вимагає пристрою, що працює на третьому - мережному рівні моделі OSI.

Транкові канали VLAN використовуються для передавання інформації VLAN через множину пристроїв. Транкові канали дозволяють передавати трафік з декількох VLAN по одному каналу, зберігаючи ідентифікацію та сегментацію VLAN незмінними.

У цій лабораторій роботі Ви створите VLAN на двох комутаторах мережі, налаштуєте належність портів комутаторів до відповідних VLAN, переконаєтеся, що VLAN працюють належним чином, і створите транкові канали VLAN між двома комутаторами.

Примітка: Для лабораторних робіт курсу CCNA використовуються комутатори Cisco Catalyst 2960s з операційною системою Cisco IOS Release 15.2(2) (образ lanbasek9). Можна використовувати інші моделі комутаторів та версії Cisco IOS. Залежно від моделі комутатора та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані у лабораторній роботі. Для правильної ідентифікації інтерфейсів пристроїв скористайтеся таблицею, що наведена у кінці лабораторної роботи.

Примітка : Переконайтесь, що налаштування комутаторів були видалені та вони не мають стартових конфігурацій. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- Два комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2), образ lanbasek9 або аналогічний).
- 2 комп'ютери (Windows з термінальним застосунком, наприклад, Tera Term).
- Консольні кабелі для налаштування операційної системи Cisco IOS пристроїв через консольні порти.
- Кабелі Ethernet, що показані в топології мережі

Інструкції

Частина 1. Побудова мережі та налаштування базових параметрів пристроїв

У Частині 1 лабораторної роботи Ви створите топологію мережі та налаштуєте базові параметри комп'ютерів та комутаторів.

Крок 1. З'єднання пристроїв мережі, відповідно до топології.

Приєднайте пристрої відповідними кабелями, як показано на схемі топології мережі.

Крок 2. Налаштування базових параметрів кожного комутатора.

a. Під'єднайтеся до комутатора за допомогою консольного кабеля і увійдіть до привілейованого режиму EXEC.

b. Встановіть назву комутатору.

c. Вимкніть пошук DNS (DNS lookup).

d. Встановіть пароль **class** для входу до привілейованого режиму EXEC.

e. Встановіть пароль **cisco** як пароль для входу через консольне підключення та активуйте аутентифікацію.

f. Встановіть пароль **cisco** як пароль для входу через віртуальні підключення та активуйте аутентифікацію.

g. Зашифруйте всі паролі, які відображаються у відкритому вигляді.

h. Створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено.

i. Збережіть поточну конфігурацію як стартову конфігурацію.

Крок 3. Налаштування комп'ютерів.

Скористайтеся таблицею адресації для отримання інформації щодо адрес вузлів.

Частина 2. Створення VLAN і налаштування належності портів комутатора до VLAN

У частині 2 лабораторної роботи за даними наведеної вище таблиці Ви створите VLAN на двох комутаторах мережі. Також Ви налаштуєте належність інтерфейсів до відповідних VLAN. Команда **show vlan brief** використовується для перевірки параметрів Ваших налаштувань. Виконайте наведені нижче налаштування на кожному комутаторі.

Крок 1. Створення VLAN на двох комутаторах.

a. За даними наведеної вище таблиці на кожному комутаторі створіть і назвіть необхідні VLAN.

b. Налаштуйте інтерфейс управління на кожному комутаторі, використовуючи інформацію про IP-адресу з таблиці адресації.

c. Налаштуйте належність всіх невикористаних інтерфейсів комутаторів до VLAN Parking_Lot, налаштуйте їм статичний режим доступу та адміністративно їх вимкніть.

Крок 2. Налаштування належності інтерфейсів комутаторів до відповідних VLAN.

a. Для використаних портів налаштуйте належність відповідним VLAN (як зазначено у вищенаведеній таблиці VLAN) і налаштуйте їм статичний режим доступу.

b. Переконайтеся, що належність інтерфейсів до відповідних VLAN виконано правильно.

Частина 3. Налаштування транкового каналу 802.1Q між комутаторами

У частині 3 лабораторної роботи Ви вручну налаштуєте інтерфейс F0/1 як транковий інтерфейс.

Крок 1. Ручне налаштування транкового інтерфейс F0/1.

a. Змініть режим порту F0/1 комутатора для примусового створення транкового каналу. Обов'язково зробіть це на обох комутаторах.

b. Налаштуйте VLAN 1000 як Native VLAN на обох комутаторах.

c. Для транкового каналу налаштуйте можливість передачі трафіку лише VLAN 10, 20, 30 та 1000.

d. Виконайте команду **show interfaces trunk** для перевірки транкових портів, Native VLAN та VLAN, трафік яких дозволено передавати через транковий канал.

Крок 2. Перевірка зв'язку.

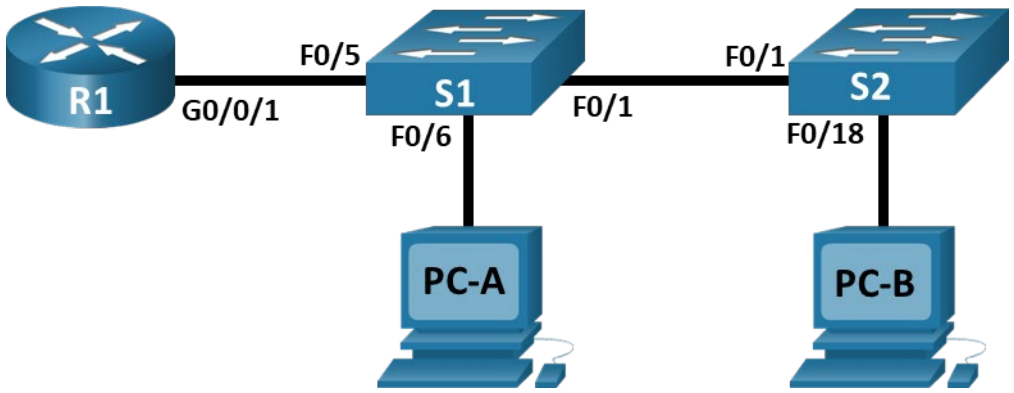
Перевірте можливість передачі трафіку в межах VLAN. Наприклад, PC-A повинен успішно перевіряти зв'язок за допомогою команди ping з VLAN 20 комутатора S1.

Чи була перевірка зв'язку за допомогою команди ping вдалою? Поясніть.

Лабораторна робота 4
Тема: Packet Tracer. Ускладнене завдання маршрутизації між VLAN

Лабораторна робота - Налаштування маршрутизації між VLAN методом Router-on-a-Stick

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0/1.3	192.168.3.1	255.255.255.0	N/A
	G0/0/1.4	192.168.4.1	255.255.255.0	
	G0/0/1.8	N/A	N/A	
S1	VLAN 3	192.168.3.11	255.255.255.0	192.168.3.1
S2	VLAN 3	192.168.3.12	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC-B	NIC	192.168.4.3	255.255.255.0	192.168.4.1

Таблиця VLAN

VLAN	Ім'я	Призначений інтерфейс
3	Management	S1: VLAN 3 S2: VLAN 3 S1: F0/6
4	Operations	S2: F0/18
7	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2

8	Native	N/A

Цілі та задачі

Частина 1: Створення мережі та налаштування базових параметрів пристрою

Частина 2: Створення мереж VLAN і призначення портів комутатора

Частина 3: Налаштування магістрального каналу 802.1Q між комутаторами

Частина 4: Налаштування маршрутизації між VLAN на маршрутизаторі

Частина 5: Перевірка працездатності маршрутизації між VLAN

Довідкова інформація / Сценарій

Сучасні комутатори використовують віртуальні локальні мережі (VLAN) для надання послуг сегментації, які традиційно надаються маршрутизаторами в конфігураціях LAN. VLAN вирішують проблеми масштабованості, безпеки та керування мережею. Загалом, VLAN спрощують проектування мережі для досягнення цілей організації. Для зв'язку між VLAN потрібен пристрій, що працює на рівні 3 моделі OSI. Маршрутизатори в топологіях VLAN забезпечують додаткову безпеку і керування потоками трафіку.

Магістральні канали VLAN використовуються для поширення VLAN на декілька пристроїв. Магістральні канали дозволяють трафіку з декількох VLAN рухатися по одному каналу, зберігаючи ідентифікацію та сегментацію VLAN незмінними. Особливий вид маршрутизації між VLAN, названий «Router-On-A-Stick», використовує магістральний канал від маршрутизатора до комутатора, щоб всі VLAN могли проходити на маршрутизатор.

У цій лабораторній роботі ви створите VLAN на обох комутаторах в топології, призначите VLAN для портів доступу комутатора, переконаєтесь, що VLAN працюють належним чином, створите магістральні канали VLAN між двома комутаторами і між S1 і R1, а також налаштуєте маршрутизацію між VLAN на R1, щоб дозволити вузлам в різних VLAN спілкуватися, незалежно від того, в якій підмережі знаходиться вузол.

Примітка: Маршрутизатори, що використовуються в лабораторних роботах CCNA - це Cisco 4221 з операційною системою Cisco IOS XE Release 16.9.4 (образ universalk9). Комутатори, які використовуються в лабораторних роботах - це Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Також можна використовувати інші моделі маршрутизаторів і комутаторів, а також версії Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані в лабораторних роботах. Зверніться до зведеної таблиці інтерфейсів маршрутизатора, яку наведено у кінці лабораторної роботи, щодо правильних ідентифікаторів інтерфейсів.

Примітка: Переконайтесь, що пам'ять маршрутизаторів та комутаторів була очищена та вони не мають початкових конфігурацій. Якщо ви в цьому не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 1 Маршрутизатор (Cisco 4221 з універсальним образом Cisco IOS XE версії 16.9.4 або сумісний)
- 2 Комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2) (образ lanbasek9 або сумісний)
- 2 ПК (Windows з програмою емуляції терміналу,такою як Tera Term)
- Консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти
- Кабелі Ethernet, вказані на топології

Інструкції

Частина1: Створення мережі та налаштування базових параметрів пристрою

У першій частині лабораторної роботи ви створите топологію мережі та налаштуєте базові параметри вузлів ПК та комутаторів.

Крок1: З'єднайте пристрої у мережу, відповідно до схеми топології.

Приєднайте пристрої необхідними кабелями, як показано на схемі топології.

Крок2: Налаштуйте основні параметри на маршрутизаторі.

a. Утворіть консольне з'єднання із маршрутизатором і увійдіть до привілейованого режиму EXEC.

b. Увійдіть до режиму конфігурації.

c. Призначте маршрутизатору ім’я.

d. Вимкніть пошук DNS, щоб запобігти спробам маршрутизатора перетворити неправильно введені команди на імена вузлів.

e. Призначте **class** як зашифрований пароль привілейованого режиму EXEC.

f. Призначте **cisco** як пароль доступу до консолі і активуйте авторизацію.

g. Призначте **cisco** у як пароль для віртуальних ліній і активуйте авторизацію.

h. Зашифруйте всі відкриті текстові паролі.

i. Створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено.

j. Збережіть поточну конфігурацію у файл стартової конфігурації.

k. Встановіть час на маршрутизаторі.

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку з правильною послідовністю параметрів, необхідних для виконання цієї команди.

Крок3: Налаштуйте базові параметри для кожного комутатора.

a. Під'єднайтесь до комутатора через консольний кабель і увійдіть до привілейованого режиму EXEC.

b. Увійдіть до режиму глобальної конфігурації.

c. Призначте комутатору ім’я.

d. Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби неправильно перекласти введені команди: ніби вони є іменами хостів.

e. Призначте **class** як зашифрований пароль привілейованого режиму EXEC.

f. Призначте **cisco** як пароль на консольній лінії і активуйте авторизацію.

g. Призначте **cisco** у якості паролю для віртуальних ліній і активуйте авторизацію.

h. Зашифруйте всі відкриті текстові паролі.

i. Створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено.

j. Налаштуйте час на комутаторі.

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку з правильною послідовністю параметрів, необхідних для виконання цієї команди.

k. Збережіть поточну конфігурацію як стартову конфігурацію.

Крок4: Налаштуйте вузли PC.

Зверніться до таблиці адресації для визначення адресної інформації вузлів.

Частина2: Створення мереж VLAN і призначення портів комутатора

У частині 2 ви створите VLAN, як зазначено в таблиці вище, на обох комутаторах. Потім ви призначите VLAN для відповідного інтерфейсу. Команда **show vlan** використовується для перевірки ваших налаштувань конфігурації. Виконайте наступні налаштування на кожному комутаторі.

Крок1: Створіть VLAN на обох комутаторах.

a. На обох комутаторах створіть і назвіть VLAN, відповідно до наведеної вгорі таблиці VLAN.

b. Налаштування інтерфейсу керування та шлюзу за замовчуванням на кожному комутаторі, використовуючи відомості про IP-адресу з таблиці адресації.

c. Призначте всі невикористані порти на обох комутаторах у ParkingLot VLAN, налаштуйте їх на статичний режим доступу і адміністративно вимкніть.

Примітка: Команда interface range корисна для виконання цього завдання з якомога меншою кількістю команд.

Крок2: Призначте VLAN відповідним інтерфейсам комутатора.

a. Призначте використовувані порти відповідній VLAN (зазначеній у таблиці VLAN вище) та налаштуйте їх на статичний режим доступу. Обов'язково зробіть це на обох комутаторах.

b. Виконайте команду **show vlan brief** і переконайтеся, що VLAN призначені правильним інтерфейсам.

Частина3: Налаштування магістрального каналу 802.1Q між комутаторами

У частині 3 ви вручну налаштуєте інтерфейс F0/1 як магістральний канал.

Крок1: Вручну налаштуйте магістральний інтерфейс F0/1.

a. Змініть режим порту комутатора на інтерфейсі F0/1 для примусового створення магістрального каналу. Обов'язково зробіть це на обох комутаторах.

b. В рамках конфігурації магістрального каналу встановіть native VLAN за номером 8 на обох комутаторах. Повідомлення про помилки можуть відображатися тимчасово, поки два інтерфейси налаштовано для різних native VLAN.

c. В якості іншої частини конфігурації магістрального каналу вкажіть, що дозволено тільки VLAN 3, 4, і 8 проходити по каналу.

d. Виконайте команду **show interfaces trunk** для перевірки магістральних портів, native VLAN і дозволених VLAN на магістральному каналі.

Крок2: Вручну налаштуйте магістральний інтерфейс S1 F0/5

a. Налаштуйте F0/5 на S1 з тими ж параметрами магістралі, що і F0/1. Це магістральний канал до маршрутизатора.

b. Збережіть поточну конфігурацію у файлі стартової конфігурації.

c. Виконайте команду **show interfaces trunk** для перевірки магістрального каналу.

Чому F0/5 не з'явився в списку магістральних каналів?

Частина4: Налаштування маршрутизації між VLAN на маршрутизаторі

a. Активуйте інтерфейс G0/0/1 на маршрутизаторі.

b. Налаштуйте підінтерфейси для кожної VLAN, як зазначено в таблиці IP-адресації. Всі підінтерфейси використовують інкапсуляцію 802.1Q. Переконайтеся, що підінтерфейс для native VLAN не має IP-адреси. Налаштуйте опис для кожного під-інтерфейсу.

c. Використовуйте команду show ip interface brief для перевірки працездатності під-інтерфейсів.

Частина5: Перевірка працездатності маршрутизації між VLAN

Крок1: Проведіть наступні тести з PC-A. Усі повинні бути успішними.

Примітка: Для успішного використання ping може знадобитися тимчасово відключити брандмауер Windows.

a. Відправте запит ping від PC-A до його шлюзу за замовчуванням.

b. Відправте запит ping dsl PC-A до PC-B.

c. Відправте запит ping від PC-A до S2.

Крок2: Проведіть наступні тести з PC-B.

У командному рядку на PC-B виконайте команду tracert на адресу PC-A.

Які проміжні IP-адреси відображаються в результатах?

Зведена таблиця інтерфейсів маршрутизатора

Модель маршрутизатора	Ethernet-інтерфейс №1	Ethernet Interface №2	Serial Interface №1	Serial Interface №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial0/1/0	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

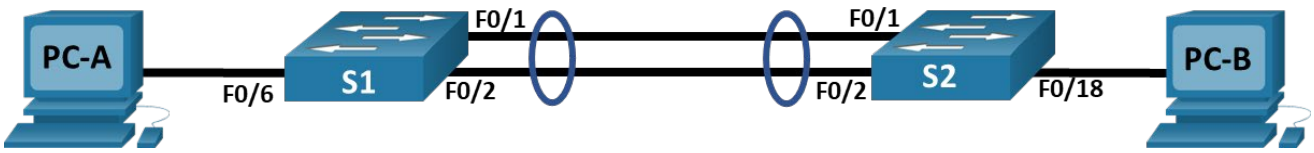
Модель маршрутизатора	Ethernet-інтерфейс №1	Ethernet Interface №2	Serial Interface №1	Serial Interface №2
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial0/1/0	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial0/1/0	Serial 0/1/1 (S0/1/1)

Примітка: Щоб дізнатися, як налаштований маршрутизатор, подивіться на інтерфейси, щоб визначити тип маршрутизатора та скільки інтерфейсів у маршрутизатора. Неможливо ефективно перелічити всі комбінації налаштувань для кожного класу маршрутизаторів. Ця таблиця містить ідентифікатори для можливих комбінацій Ethernet- та Serial-інтерфейсів пристрою. У таблиці немає інших типів інтерфейсів, хоча конкретний маршрутизатор може містити їх. Прикладом може бути інтерфейс ISDN BRI. Рядок у дужках - це загальноприйнята абревіатура, яка може бути використана у командах Cisco IOS при зверненні до інтерфейсу.

Лабораторна робота 5
Тема: Packet Tracer. Налаштування EtherChannel

Лабораторна робота - Впровадження EtherChannel

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
S1	VLAN 10	192.168.10.11	255.255.255.0
S2	VLAN 10	192.168.10.12	255.255.255.0
PC-A	NIC	192.168.20.3	255.255.255.0
PC-B	NIC	192.168.20.4	255.255.255.0

Таблиця VLAN

VLAN	Ім'я	Призначений інтерфейс
10	Management	VLAN 10
20	Clients	S1: F0/6 S2: F0/18
999	Parking_Lot	S1: F0/3-5, F0/7-24, G0/1-2 S2: F0/3-17, F0/19-24, G0/1-2
1000	Native	N/A

Цілі та задачі

Частина 1: Побудова мережі та налаштування базових параметрів пристроїв

Частина 2: Створення мереж VLAN і призначення портів комутатора

Частина 3: Налаштування магістральних каналів 802.1Q між комутаторами

Частина 4: Впровадження та перевірка каналу EtherChannel між комутаторами

Довідкова інформація / Сценарій

Агрегація з'єднань дозволяє створювати логічні канали, які складаються з двох або більше фізичних з'єднань. Це забезпечує збільшену пропускну здатність в порівнянні з використанням лише одного фізичного зв'язку. Агрегація з'єднань також забезпечує резервування, якщо одне зі з'єднань не працює.

У цій лабораторній роботі ви налаштуєте EtherChannel - форму агрегованого каналу, що використовується в комутованих мережах. Ви налаштуєте EtherChannel за допомогою протоколу управління агрегацією з'єднань (LACP).

Примітка: LACP — це протокол агрегації з'єднань, який визначається IEEE 802.3ad, і він не пов'язаний з будь-яким конкретним виробником.

LACP дозволяє комутаторам Cisco керувати каналами Ethernet з комутаторами, які відповідають протоколу 802.3ad. Ви можете налаштувати до 16 портів для формування каналу. Вісім портів знаходяться в активному режимі, а інші вісім знаходяться в режимі очікування. Коли будь-який з активних портів вийде з ладу, порт в режимі очікування стає активним. Режим очікування працює лише для LACP, а не для PAgP.

Примітка: Для лабораторних робіт курсу CCNA використовуються комутатори Cisco Catalyst 2960s з операційною системою Cisco IOS Release 15.2(2) (образ lanbasek9). Можна використовувати інші комутатори та версії Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від показаних у лабораторних роботах.

Примітка: Переконайтесь, що налаштування на комутаторах були видалені та пристрої не мають стартової конфігурації. Якщо ви в цьому не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- Два комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2) образ lanbasek9 або аналогічний)
- 2 ПК (під керуванням Windows з програмою емуляції терміналу,такою як Tera Term)
- Консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти
- Кабелі Ethernet, вказані на топології

Інструкції

Частина1: Створення мережі та налаштування базових параметрів пристрою

У першій частині лабораторної роботи ви створите топологію мережі та налаштуєте базові параметри вузлів ПК та комутаторів.

Крок 1: З'єднайте пристрої у мережу, відповідно до схеми топології.

Приєднайте пристрої необхідними кабелями, як показано на схемі топології.

Крок 2: Налаштуйте базові параметри для кожного комутатора.

a. Призначте комутатору назву.

b. Вимкніть пошук DNS, щоб упередити комутатор від спроби неправильно перекласти введені команди: ніби вони є іменами вузлів.

c. Призначте **class** як зашифрований пароль на привілейований режим EXEC.

d. Призначте **cisco** як пароль на консольній лінії і активуйте авторизацію.

e. Призначте **cisco** як пароль на вхід до віртуальних ліній і активуйте авторизацію.

f. Зашифруйте всі паролі, які відображаються у відкритому вигляді.

g. Створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено.

h. Збережіть поточні налаштування у файлі початкової конфігурації.

i. Встановіть на комутаторі сьогоднішній час і дату.

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку з правильною послідовністю параметрів, необхідних для виконання цієї команди.

j. Збережіть поточну конфігурацію як стартову конфігурацію.

Крок 3: Налаштуйте вузли PC.

Для визначення адресної інформації вузлів зверніться до таблиці адресації.

Частина2: Створення мереж VLAN і призначення портів комутатора

У Частині 2 ви створите VLAN, як зазначено в таблиці вище, на обох комутаторах. Потім ви призначите VLAN відповідному інтерфейсу і перевірите свої налаштування конфігурації. Виконайте нижченаведені налаштування на кожному комутаторі.

Крок 1: Створіть мережі VLAN на обох комутаторах.

a. На обох комутаторах створіть і назвіть VLAN, відповідно до наведеної вгорі таблиці VLAN.

b. Налаштуйте та активуйте інтерфейс керування на кожному комутаторі, використовуючи відомості про IP-адресу з таблиці адресації.

c. Призначте всі невикористані порти на обох комутаторах у VLAN Parking_Lot, налаштуйте їх на статичний режим доступу і адміністративно вимкніть.

Крок 2: Призначте мережі VLAN відповідним інтерфейсам комутатора.

a. Призначте використовувані порти відповідній VLAN (зазначеній у таблиці VLAN вище) та налаштуйте їх на статичний режим доступу.

b. Виконайте команду **show vlan brief** і переконайтеся, що мережі VLAN призначені правильним інтерфейсам.

Частина3: Налаштування магістрального каналу 802.1Q між комутаторами

У Частині 3 ви вручну налаштуєте інтерфейси F0/1 і F0/2 як магістральні інтерфейси 802.1Q.

a. Змініть режим порту комутатора на інтерфейсах для примусового створення магістрального каналу. Використовуйте команду **interface range**, щоб зменшити кількість необхідних команд. Обов'язково зробіть це на обох комутаторах.

b. При налаштуванні магістрального каналу встановіть значення native VLAN у 1000 на обох комутаторах. Тимчасово, поки два інтерфейси налаштовано для різних native VLAN, можуть відображатися повідомлення про помилки.

c. Для магістрального каналу налаштуйте можливість передачі трафіку VLAN 10, 20 та 1000.

d. Введіть команду **show interfaces trunk** для перевірки магістральних портів, Native VLAN та VLAN, для яких дозволено передавати трафік через магістральний канал.

Чому запис Vlans in spanning tree forwarding state and not pruned (Vlan у стані переадресації єднального дерева не відсікаються) відрізняється для F0/1 і F0/2?

Частина4: Впровадження та перевірка каналу EtherChannel між комутаторами

a. Створіть EtherChannel на основі LACP з використанням F0/1 і F0/2 та групи №1, причому обидва так комутатори активно узгоджували протокол EtherChannel. Використовуйте команду **interface range**, щоб зменшити кількість необхідних команд.

b. Після налаштування EtherChannel автоматично створюється віртуальний інтерфейс Port-Channel. Тепер інтерфейс Port-Channel 1 є логічним інтерфейсом згрупованих фізичних портів F0/1 і F0/2. Крім того, Port-Channel буде успадковувати конфігурацію першого фізичного порту, доданого до EtherChannel.

c. Виконайте команду **show interfaces trunk**, щоб перевірити, що магістральний канал все ще на місці.

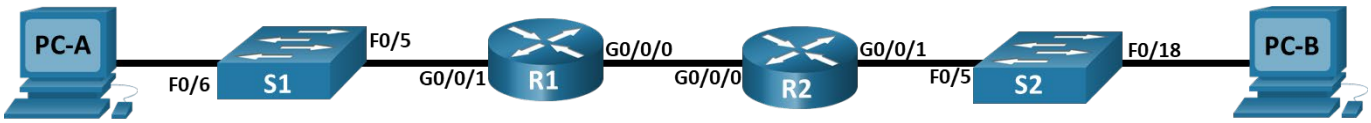
   Що являє собою порт Po1?

d. Скористайтеся командою **show etherchannel summary**, щоб перевірити налаштування EtherChannel.

Лабораторна робота 6
Тема: Packet Tracer. Реалізація DHCPv4

Лабораторна робота - Впровадження DHCPv4

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0/0	10.0.0.1	255.255.255.252	N/A
	G0/0/1	N/A	N/A	
	G0/0/1.100			
	G0/0/1.200			
	G0/0/1.1000	N/A	N/A	
R2	G0/0/0	10.0.0.2	255.255.255.252	N/A
	G0/0/1			
S1	VLAN 200			
S2	VLAN 1			
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Таблиця VLAN

VLAN	Ім'я	Призначений інтерфейс
1	N/A	S2: F0/18
100	Clients	S1: F0/6
200	Management	S1: VLAN 200
999	Parking_Lot	S1: F0/1-4, F0/7-24, G0/1-2
1000	Native	N/A

Цілі та задачі

Частина 1: Створення мережі та налаштування базових параметрів пристрою

Частина 2: Налаштування та перевірка двох DHCPv4-серверів на R1

Частина 3: Налаштування та перевірка ретрансляції DHCP на R2

Довідкова інформація / Сценарій

Протокол динамічної конфігурації вузла (DHCP) - це мережний протокол, який дозволяє адміністраторам мережі керувати та автоматизувати призначення IP-адрес. Без використання DHCP для IPv4 адміністратору довелося би статично призначати та налаштовувати параметри IP-адреси, DNS-серверів та шлюзу за замовчуванням. По мірі збільшення розміру мережі й переміщенні пристроїв з однієї внутрішньої мережі в іншу, статичне налаштування викликає проблеми з адмініструванням.

У запропонованому сценарії компанія збільшилася у розмірах, і мережні адміністратори більше не можуть призначати IP-адреси пристроям статично. Ваше завдання - налаштувати маршрутизатор R1 для призначення IPv4-адрес у двох різних підмережах.

Примітка: У лабораторних роботах CCNA використовуються маршрутизатори Cisco 4221 з операційною системою Cisco IOS XE Release 16.9.4 (образ universalk9) і комутатори Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Також передбачається застосування інших моделей маршрутизаторів і комутаторів, а також версій Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані в лабораторних роботах. Зверніться до зведеної таблиці інтерфейсів маршрутизатора, наведеній у кінці лабораторної роботи, щодо правильних ідентифікаторів інтерфейсів.

Примітка: Переконайтесь, що пам'ять маршрутизаторів і комутаторів була очищена та вони не містять початкових налаштувань. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 2 Маршрутизатори (Cisco 4221 з операційною системою Cisco IOS XE Release 16.9.4 образ universal або аналогічний)
- 2 Комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2) (образ lanbasek9 або сумісний)
- 2 ПК (Windows з програмою емуляції терміналу, такою як Tera Term)
- Консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти
- Кабелі Ethernet подані на топології

Інструкції

Частина 1: Створення мережі та налаштування базових параметрів пристрою

У Частині 1 ви побудуєте топологію мережі та налаштуєте базові параметри вузлів ПК та комутаторів.

Крок 1: Розробіть схему адресації.

Підмережа мережі 192.168.1.0/24 відповідає таким вимогам:

a. Одна підмережа, «Підмережа А», що підтримує 58 вузлів (клієнтська VLAN на R1).

Підмережа А:

Запишіть першу IP-адресу в таблицю адресації для G0/0/1.100 на R1. Запишіть другу IP-адресу в таблицю адресації для S1 VLAN 200 і введіть відповідний шлюз за замовчуванням.

b. Одна підмережа, «Підмережа B», що підтримує 28 вузлів (VLAN керування на R1).

Підмережа B:

Запишіть першу IP-адресу в таблицю адресації для G0/0/1.200 на R1. Запишіть другу IP-адресу в таблицю адресації для S1 (VLAN 1) і введіть відповідний шлюз за замовчуванням.

c. Одна підмережа, «Підмережа C», що підтримує 12 вузлів (клієнтська мережа на R2).

Підмережа C:

Запишіть першу IP-адресу в таблицю адресації для G0/0/1 на R2 .

Крок 2: З'єднайте пристрої у мережу, відповідно до схеми топології.

З’єднайте пристрої необхідними кабелями, як показано на схемі топології.

Крок 3: Налаштуйте основні параметри на кожному маршрутизаторі.

a. Призначте маршрутизатору ім’я пристрою.

b. Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перекласти неправильно введені команди: ніби вони є іменами хостів.

c. Призначте **class** як зашифрований пароль привілейованого режиму EXEC.

d. Призначте **cisco** як пароль доступу до консолі і активуйте авторизацію.

e. Призначте **cisco** як пароль на віртуальні лінії і активуйте авторизацію.

f. Зашифруйте всі паролі, що подаються у відкритому вигляді.

g. Створіть банер, який при зверненні до пристрою попереджатиме про заборону несанкціонованого доступу.

h. Збережіть поточні налаштування до конфігураційного файлу запуску.

i. Встановіть на маршрутизаторі годинник на сьогоднішній час і дату.

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку щодо правильної послідовності параметрів, необхідних для виконання цієї команди.

Крок 4: Налаштуйте маршрутизацію між VLAN на маршрутизаторі R1.

a. Активуйте інтерфейс G0/0/1 на маршрутизаторі.

b. Налаштуйте підінтерфейси для кожної VLAN відповідно до таблиці IP-адресації. Усі підінтерфейси використовують інкапсуляцію 802.1Q і їм призначається перша доступна адреса з розрахованого вами діапазону IP-адрес. Переконайтеся, що підінтерфейс для native VLAN не має IP-адреси. Налаштуйте опис для кожного підінтерфейсу.

c. Перевірте, чи працюють налаштовані підінтерфейси.

Крок 5: Налаштуйте G0/0/1 на R2, а на обох маршрутизаторах - G0/0/0 і статичну маршрутизацію.

a. Налаштуйте на G0/0/1 маршрутизатора R2 першу IP-адресу підмережі C, розраховану вище.

b. Налаштуйте інтерфейс G0/0/0 кожного маршрутизатора використавши параметри наведеної вище таблиці IP-адресації.

c. На кожному маршрутизаторі налаштуйте маршрут за замовчуванням, який би вказував на IP-адресу G0/0/0 сусіднього маршрутизатора.

d. Перевірте чи працює статична маршрутизація пропінгувавши з R1 інтерфейс G0/0/1 на R2.

e. Збережіть поточні налаштування до конфігураційного файлу запуску.

Крок 6: Налаштуйте базові параметри для кожного комутатора.

a. Призначте комутатору ім'я пристрою.

b. Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перекласти неправильно введені команди: ніби вони є іменами хостів.

c. Призначте **class** як зашифрований пароль на привілейований режим EXEC.

d. Призначте **cisco** як пароль на консольній лінії і активуйте авторизацію.

e. Призначте **cisco** як пароль на вхід до віртуальних ліній і активуйте авторизацію.

f. Зашифруйте всі паролі, які відображаються у відкритому вигляді.

g. Створіть банер, який при зверненні до пристрою попереджатиме про заборону несанкціонованого доступу.

h. Збережіть поточні налаштування до конфігураційного файлу запуску.

i. Встановіть на маршрутизаторі годинник на сьогоднішній час і дату.

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку щодо правильної послідовності параметрів, необхідних для виконання цієї команди.

j. Збережіть поточну конфігурацію до конфігураційного файлу запуску.

Крок 7: Створіть VLAN на комутаторі S1.

Примітка: На комутаторі S2 виконуються лише базові налаштування.

a. Створіть і назвіть необхідні VLAN на комутаторі S1 згідно з наведеною вище таблицею.

b. Налаштуйте і активуйте інтерфейс керування на S1 (VLAN 200) використовуючи другу IP-адресу з підмережі, розрахованої раніше. Також встановіть на S1 шлюз за замовчуванням.

c. Налаштуйте і активуйте інтерфейс керування на S2 (VLAN 1) використовуючи другу IP-адресу з підмережі, розрахованої раніше. Також встановіть на S2 шлюз за замовчуванням.

d. Призначте всі невикористані порти на S1 до VLAN Parking_Lot, налаштуйте їх на статичний режим доступу та адміністративно вимкніть. Також вимкніть усі невикористані порти на S2.

Примітка: При виконанні цього завдання команда interface range дозволить суттєво скоротити кількість команд, необхідних для налаштування.

Крок 8: Призначте VLAN відповідним інтерфейсам комутатора.

a. Призначте залучені порти відповідній VLAN (зазначеній у таблиці VLAN вище) та статично налаштуйте їх на роботу в режимі доступу.

b. Переконайтеся, що VLAN призначені відповідним інтерфейсам.

Чому інтерфейс F0/5 вказаний у VLAN 1?

Крок 9: Статично налаштуйте на S1 інтерфейс F0/5 як транк 802.1Q.

a. Для створення магістрального каналу впровадьте на порті комутатора режим транкування.

b. В рамках конфігурації магістрального каналу встановіть native VLAN із номером 1000.

c. Окремо в налаштуваннях надайте дозвіл VLAN 100, 200 і 1000 на передавання даних по магістралі.

d. Збережіть поточну конфігурацію до конфігураційного файлу запуску.

e. Перевірте стан магістрального каналу.

На даному етапі, яку IP-адресу мали би ПК налаштовані для використання DHCP при під'єднані до мережі?

Частина 2: Налаштування та перевірка двох серверів DHCPv4 на R1

У Частині 2 необхідно налаштувати та перевірити сервер DHCPv4 на маршрутизаторі R1. Сервер DHCPv4 обслуговуватиме дві підмережі, Підмережу A і Підмережу C.

Крок 1: Налаштуйте на R1 пули DHCPv4 для двох підтримуваних підмереж. Нижче наведено тільки пул DHCP для підмережі A.

a. Виключіть перші п'ять доступних адрес з кожного пулу адрес.

b. Створіть пул DHCP (Для кожного пулу використайте унікальне ім'я).

c. Вкажіть мережу, яку підтримує цей DHCP-сервер.

d. Встановіть доменне ім'я як ccna-lab.com.

e. Для кожного пулу DHCP налаштуйте відповідний шлюз за замовчуванням.

f. Налаштуйте час оренди на 2 дні 12 годин і 30 хвилин.

g. Далі налаштуйте другий пул DHCPv4, зазначивши R2_Client_LAN як ім'я пулу, обчисліть мережу, маршрутизатор за замовчуванням, і використайте те саме доменне ім'я та час оренди, що і для попереднього пулу DHCP.

Крок 2: Збережіть конфігурацію.

Збережіть поточні налаштування до конфігураційного файлу запуску.

Крок 3: Перевірте налаштування DHCPv4-сервера.

a. Щоб переглянути параметри пулу застосуйте команду **show ip dhcp pool**.

b. Для перевірки призначених DHCP-адрес запустіть на виконання команду **show ip dhcp bindings**.

c. Для перевірки DHCP-повідомлень застосуйте команду **show ip dhcp server statistics**.

Крок 4: Спробуйте отримати IPv6-адресу на PC-A за допомогою DHCP-сервера.

a. Відкрийте вікно командного рядка на PC-A і запустіть на виконання команду **ipconfig/renew**.

b. Після завершення процесу оновлення, скористайтесь командою **ipconfig** для перегляду нової інформації про IP-адресу.

c. Перевірте з'єднання пропінгувавши IP-адресу інтерфейсу G0/0/1 маршрутизатора R1.

Частина 3: Налаштування та перевірка ретрансляції DHCP на R2

У Частині 3, налаштуйте R2 для ретрансляції DHCP-запитів з локальної мережі через інтерфейс G0/0/1 на DHCP-сервер (R1).

Крок 1: Налаштуйте R2 як агента ретрансляції DHCP для локальної мережі на G0/0/1.

a. Застосуйте на G0/0/1 команду **ip helper-address**, вказавши IP-адресу G0/0/0 на R1.

b. Збережіть конфігурацію.

Крок 2: Спробуйте отримати IPv6-адресу на PC-B за допомогою DHCP-сервера.

a. Відкрийте вікно командного рядка на PC-B і запустіть на виконання команду **ipconfig/renew**.

b. Після завершення процесу оновлення, застосуйте команду **ipconfig** для перегляду нової інформації про IP-адресу.

c. Перевірте з’єднання пропінгувавши IP-адресу інтерфейсу G0/0/1 маршрутизатора R1.

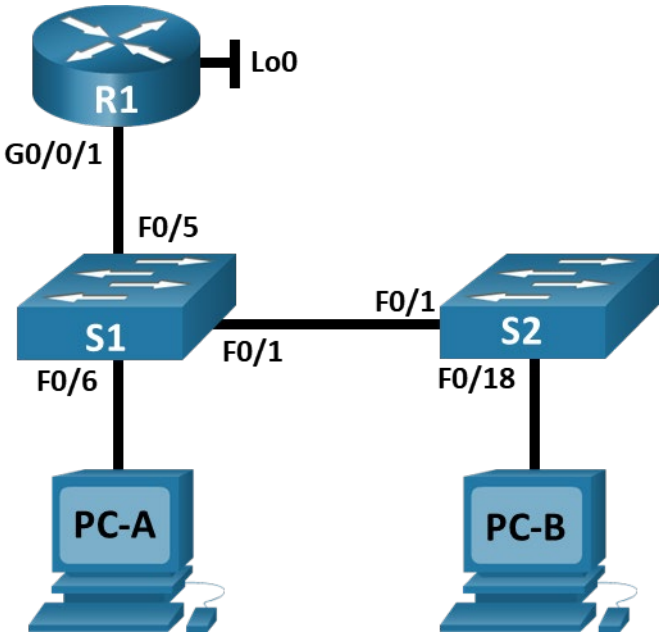
d. Для перевірки прив'язки DHCP на R1 застосуйте команду **show ip dhcp binding**.

e. Для перевірки DHCP-повідомлень маршрутизаторів R1 і R2 скористайтесь командою **show ip dhcp server statistics**.

Лабораторна робота 7
Тема: Packet Tracer. Налаштування безпеки комутатора

Лабораторна робота - Налаштування безпеки на комутаторі

Топологія



Таблиця адресації

Пристрій	Інтерфейс / VLAN	IP-адреса	Маска підмережі
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC - A	NIC	DHCP	255.255.255.0
PC - B	NIC	DHCP	255.255.255.0

Цілі та задачі

Частина 1: Налаштування мережних пристроїв.

- З'єднання пристроїв у мережі.
- Налаштування R1.
- Налаштування і перевірка основних параметрів комутатора.

Частина 2: Налаштування VLAN на комутаторах.

- Налаштування VLAN 10.

- Налаштування SVI для VLAN 10.
- Налаштування VLAN 333 із назвою Native на S1 і S2.
- Налаштування VLAN 999 із назвою ParkingLot на S1 і S2.

Частина 3: Налаштування безпеки на комутаторі.

- Реалізація транкування 802.1Q.
- Налаштування портів доступу.
- Захист і вимкнення невикористаних портів комутатора.
- Документування і запровадження параметрів захисту портів комутатора.
- Уведення відстеження DHCP.
- Реалізація PortFast і BPDU guard.
- Перевірка наскрізного з'єднання.

Довідкова інформація / Сценарій

Це комплексна лабораторна робота, яка охоплює функції безпеки Рівня 2.

Примітка: У практичних лабораторних роботах CCNA використовуються маршрутизатори Cisco 4221 з Cisco IOS XE Release 16.9.3 (образ universalk9) і комутатори Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Також передбачається застосування інших моделей маршрутизаторів і комутаторів, а також версій Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані в лабораторних роботах.

Примітка: Переконайтесь, що налаштування на комутаторах були видалені та пристрої не мають початкової конфігурації запуску. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 1 Маршрутизатор (Cisco 4221 з Cisco IOS XE версія 16.9.3 образ універсальний або аналогічний)
- 2 комутатори (Cisco 2960 з образом операційної системи Cisco IOS Release 15.0(2) lanbasek9 або аналогічним)
- 2 ПК (Windows з програмою емуляції терміналу,такою як Tera Term)
- Консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти
- Кабелі Ethernet, вказані на топології.

Інструкції

Частина 1: Налаштування мережних пристроїв.

Крок 1: З'єднання пристроїв у мережі.

a. З'єднайте пристрої відповідно до схеми топології.

b. Увімкніть пристрої.

Крок 2: Налаштування R1.

a. Застосуйте на R1 наведений нижче сценарій конфігурації.

```
enable
```

```
configure terminal
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 description Link to S1 Port 5
 ip dhcp relay information trusted
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

b. Перевірте поточні налаштування на R1 за допомогою команди:

```
R1# show ip interface brief
```

c. Переконайтеся, що IP-адреса та інтерфейси перебувають у стані up / up (виправте неполадки в разі потреби).

Крок 3: Налаштування і перевірка основних параметрів комутатора.

a. Налаштуйте назви пристроїв для комутаторів S1 і S2.

b. На обох комутаторах вимкніть небажаний пошук DNS.

c. Налаштуйте опис інтерфейсів для портів, які використовуються на S1 і S2.

d. Як шлюз за замовчуванням для VLAN керування на обох комутаторах встановіть 192.168.10.1.

Частина 2: Налаштування VLAN на комутаторах.

Крок 1: Налаштування VLAN 10.

Додайте VLAN 10 до S1 і S2 і назвіть її **Management**.

Крок 2: Налаштування VLAN 10 як SVI.

Налаштуйте на S1 і S2 IP-адресу SVI для VLAN 10 згідно з таблицею адресації. Активуйте SVI-інтерфейси і додайте їх опис.

Крок 3: Налаштування VLAN 333 із назвою Native на S1 і S2.

Крок 4: Налаштування VLAN 999 із назвою ParkingLot на S1 і S2.

Частина 3: Налаштування безпеки на комутаторі.

Крок 1: Реалізація транкування 802.1Q.

a. При запровадженні транкування на F0/1 обох комутаторів як native VLAN налаштуйте VLAN 333.

b. Перевірте налаштування магістралі на обох комутаторах.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999

S2# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999
```

c. Вимкніть узгодження DTP на F0/1 комутаторів S1 і S2.

d. Перегляньте результат налаштування за допомогою команди **show interfaces**.

```
S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off

S2# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

Крок 2: Налаштування портів доступу.

a. На S1 налаштуйте як порти доступу F0/5 і F0/6 і призначте їх до VLAN 10.

b. На S2 налаштуйте F0/18 як порт доступу, що належить до VLAN 10.

Крок 3: Захист і вимкнення невикористаних портів комутатора.

a. На S1 і S2 перемістіть невикористані порти з VLAN 1 до VLAN 999 і вимкніть їх.

b. За допомогою команди **show** переконайтесь, що невикористані порти додано до VLAN 999 і вимкнено.

```
S1# show interfaces status


Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S2         connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
Fa0/4                        disabled     999          auto   auto 10/100BaseTX
Fa0/5     Link to R1         connected    10         a-full  a-100 10/100BaseTX
Fa0/6     Link to PC-A       connected    10         a-full  a-100 10/100BaseTX
Fa0/7                        disabled     999          auto   auto 10/100BaseTX
Fa0/8                        disabled     999          auto   auto 10/100BaseTX
Fa0/9                        disabled     999          auto   auto 10/100BaseTX
Fa0/10                       disabled     999          auto   auto 10/100BaseTX
<output omitted>

S2# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
<output omitted>
Fa0/14                       disabled     999          auto   auto 10/100BaseTX
Fa0/15                       disabled     999          auto   auto 10/100BaseTX
Fa0/16                       disabled     999          auto   auto 10/100BaseTX
Fa0/17                       disabled     999          auto   auto 10/100BaseTX
Fa0/18    Link to PC-B       connected    10         a-full  a-100 10/100BaseTX
Fa0/19                       disabled     999          auto   auto 10/100BaseTX
Fa0/20                       disabled     999          auto   auto 10/100BaseTX
Fa0/21                       disabled     999          auto   auto 10/100BaseTX
Fa0/22                       disabled     999          auto   auto 10/100BaseTX
Fa0/23                       disabled     999          auto   auto 10/100BaseTX
Fa0/24                       disabled     999          auto   auto 10/100BaseTX
Gi0/1                        disabled     999          auto   auto 10/100/1000BaseTX
Gi0/2                        disabled     999          auto   auto 10/100/1000BaseTX
```

Крок 4: Документування і запровадження параметрів захисту портів комутатора.

Інтерфейси F0/6 на S1 і F0/18 на S2 налаштовані як порти доступу. На цьому кроці на них також необхідно налаштувати захист портів

a. Щоб відобразити параметри захисту за замовчуванням для інтерфейсу F0/6 на S1 запустіть на виконання команду **show port-security інтерфейс f0/6.** Запишіть свої відповіді нижче у таблицю.

Налаштування захисту портів за замовчуванням	
Функція	**Параметр за замовчуванням**
Захист портів (Port Security)	
Максимальна кількість MAC-адрес (Maximum MAC Addresses)	
Режим порушення (Violation Mode)	
Час витримки (Aging Time)	
Тип витримки (Aging Type)	
Витримка безпечних статичних адрес (Secure Static Address Aging)	
Клейка MAC-адреса (Sticky MAC Address)	

b. На F0/6 комутатора S1 увімкніть захист портів із такими параметрами:
   - Максимальна кількість MAC-адрес: **3**
   - Тип порушення: **restrict**
   - Час витримки: **60 хв**
   - Тип витримки: **inactivity**

c. Перевірте захист порту F0/6 на S1.

```
S1# show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3411:10
Security Violation Count   : 0
S1# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    0022.5646.3411    SecureDynamic                 Fa0/6       60 (I)
```

```
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

d. Увімкніть захист порту для F0/18 комутатора S2. Налаштуйте автоматичне додавання вивчених на цьому порті MAC-адрес до конфігурації запуску.

e. На F0/18 комутатора S2 налаштуйте такі параметри захисту порту:

- Максимальна кількість MAC-адрес: **2**
- Тип порушення: **Protect**
- Час витримки: **60 хв**

f. Перевірте на S2 захист порту F0/18.

```
S2# show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3413:10
Security Violation Count   : 0

S2# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    0022.5646.3413    SecureSticky                  Fa0/18       -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
Уведення відстеження DHCP.
```

g. На S2 увімкніть і налаштуйте відстеження DHCP (DHCP snooping) на VLAN 10.

h. Налаштуйте магістральний порт комутатора S2 як надійний.

i. На ненадійному порті F0/18 комутатора S2 встановіть обмеження на отримання до п'яти DHCP-пакетів за секунду.

j. Перевірте відстеження DHCP на S2.

```
S2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/18           no         no              5
  Custom circuit-ids:
```

k. У режимі командного рядка на PC-B відпустіть, а потім поновіть IP-адресу.

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

l. Перевірте прив'язку DHCP snooping за допомогою команди **show ip dhcp snooping binding**.

```
S2# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------------
00:50:56:90:D0:8E   192.168.10.11    86213       dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
```

Крок 5: Реалізація PortFast і BPDU guard.

a. Налаштуйте PortFast на всіх портах доступу, які використовуються на обох комутаторах.

b. Увімкніть захист BPDU (BPDU guard) на портах доступу VLAN 10 на S1 і S2, до яких приєднані PC-A і PC-B.

c. Переконайтеся, що BPDU guard і PortFast увімкнені на відповідних портах.

```
S1# show spanning-tree interface f0/6 detail
 Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   <output omitted for brevity>
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
```

```
    Link type is point-to-point by default
    Bpdu guard is enabled
    BPDU: sent 128, received 0
```

Крок 6: Перевірка наскрізного з'єднання.

За допомогою команди ping перевірте наявність з'єднання між усіма пристроями за таблицею IP-адресації. Якщо результат пінгування виявиться неуспішним, можливо на ПК знадобиться вимкнути брандмауер.

Питання для роздумів

1. Стосовно захисту портів на S2, чому при вивченні MAC-адрес із приклеюванням, таймера витримки не відображає час у хвилинах, що залишився?

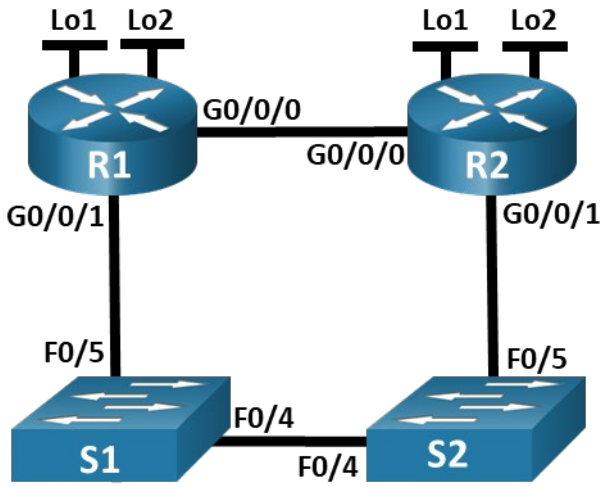
2. Щодо захисту портів на S2, якщо на ньому завантажити налаштування поточної конфігурації, чому PC-B, приєднаний до порту 18, не зможе отримати IP-адресу через DHCP?

3. Стосовно захисту портів, яка різниця між типом витримки абсолютним і за відсутності активності?

Лабораторна робота 8
Тема: Packet Tracer. Налаштування статичних маршрутів та маршрутів по замовчуванню IPv4 та IPv6

Лабораторна робота – Налаштування статичних маршрутів та маршрутів за замовчуванням IPv4 і IPv6

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс
R1	G0/0/0	172.16.1.1 /24
		2001:db8:acad:2::1 /64
		fe80::1
	G0/0/1	192.168.1.1/24
		2001:db8:acad:1::1/64
		fe80::1
	Loopback1	10.1.0.1 /24
		2001:db8:acad:10::1 /64
		fe80::1
	Loopback2	209.165.200.225 /27
		2001:db8:acad:209::1 /64
		fe80::1

Пристрій	Інтерфейс	IP-адреса/Префікс
R2	G0/0/0	172.16.1.2 /24
		2001:db8:acad:2::2 /64
		fe80::2
	G0/0/1	192.168.1.2/24
		2001:db8:acad:1::2 /64
		fe80::2
	Loopback1	10.2.0.1 /24
		2001:db8:acad:11::2 /64
		fe80::2
	Loopback2	209.165.200.193 /27
		2001:db8:acad:210::1 /64
		fe80::2

Цілі та задачі

Частина 1: Побудова мережі та налаштування базових параметрів пристрою

Частина 2: Налаштування та перевірка IP- та IPv6-адресації на R1 і R2

Частина 3: Налаштування та перевірка статичної маршрутизації та маршрутизації за замовчуванням для IPv4 на R1 і R2

Частина 4: Налаштування та перевірка статичної маршрутизації та маршрутизації за замовчуванням для IPv6 на R1 і R2

Довідкова інформація / Сценарій

Маршрутизація статична та за замовчуванням – це найпростіші форми мережної маршрутизації, які налаштовуються вручну. Ці конфігурації фіксовані, тобто не прилаштовуються динамічно до змінних умов мережі. Дійсні маршрути відображаються у таблиці маршрутизації, натомість в разі відмови або втраті актуальності маршрути з неї видаляються. За замовчуванням адміністративна відстань для статичних маршрутів дорівнює 1, проте це значення може налаштовуватися адміністратором. Це дозволяє створити резервний статичний маршрут або маршрут за замовчуванням, який з'являється у таблиці маршрутизації лише в разі відмови маршрутів із меншими адміністративними відстанями, зазвичай згенерованими динамічними протоколами маршрутизації

Примітка: У цій лабораторній роботі ви налаштуєте маршрути статичні, за замовчуванням та змінні за замовчуванням для IPv4 і IPv6, які можуть частково відповідати найкращим практикам забезпечення роботи мережі.

Примітка: У лабораторних роботах CCNA використовуються маршрутизатори Cisco 4221 з операційною системою Cisco IOS XE Release 16.9.4 (образ universalk9) і комутатори Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Передбачається застосування інших моделей маршрутизаторів і комутаторів, а також версій Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані в лабораторних роботах. Зверніться до зведеної таблиці інтерфейсів маршрутизатора, наведеній у кінці лабораторної роботи, щодо правильних ідентифікаторів інтерфейсів.

Примітка: Переконайтесь, що пам'ять маршрутизаторів та комутаторів була очищена і вони не мають початкових налаштувань. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 2 маршрутизатори (Cisco 4221 з операційною системою Cisco IOS XE Release 16.9.4 образ universal або сумісний)
- 2 комутатори (Cisco 2960 з операційною системою Cisco IOS Release 15.2(2) образ lanbasek9 або сумісний)
- 1 ПК (Windows 10 з програмою емуляції терміналу, наприклад, Tera Term)
- Консольні кабелі для налаштування операційної системи Cisco IOS пристроїв через консольні порти.
- Кабелі Ethernet, вказані на топології

Інструкції

Частина 1: Побудова мережі та налаштування базових параметрів пристрою

У першій частині лабораторної роботи ви побудуєте топологію мережі та налаштуєте базові параметри вузлів ПК та комутаторів.

Крок 1: З'єднайте пристрої у мережу відповідно до схеми топології.

З’єднайте пристрої за допомогою кабелів, вказаних на схемі топології.

Крок 2: Налаштуйте основні параметри на кожному маршрутизаторі.

a. Призначте маршрутизатору ім’я.

b. Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перекласти неправильно введені команди, ніби це імена вузлів.

c. Призначте **class** як зашифрований пароль на вхід до привілейованого режиму EXEC.

d. Призначте **cisco** як пароль доступу до консолі й активуйте авторизацію.

e. Призначте **cisco** як пароль для під’єднання до віртуальних ліній і активуйте авторизацію.

f. Зашифруйте всі паролі, що відображаються у відкритому вигляді.

g. Створіть банер, який при зверненні до пристрою попереджатиме про заборону несанкціонованого доступу.

h. Збережіть поточну конфігурацію у конфігураційному файлі запуску.

Крок 3: Налаштуйте базові параметри для кожного комутатора.

a. Призначте комутатору ім’я.

b. Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перекласти неправильно введені команди, ніби це імена вузлів.

c. Призначте **class** як зашифрований пароль на вхід до привілейованого режиму EXEC.

d. Призначте **cisco** як пароль доступу до консолі й активуйте авторизацію.

e. Призначте **cisco** як пароль для під’єднання до віртуальних ліній і активуйте авторизацію.

f. Зашифруйте всі паролі, які відображаються у відкритому вигляді.

g. Створіть банер, який при зверненні до пристрою попереджатиме про заборону несанкціонованого доступу.

h. Вимкніть усі інтерфейси, які не використовуватимуться.

i. Збережіть поточну конфігурацію у конфігураційному файлі запуску.

На цьому етапі при запуску на виконання команди **show cdp neighbors** на R1 або R2 одержується порожній список. Поясніть.

Частина 2: Налаштування та перевірка адресації IPv4 і IPv6 на R1 і R2

У Частині 2 ви налаштуєте та перевірити адреси IPv4 і IPv6 на R1 і R2. Для виконання цього завдання скористайтесь інформацією з таблиці адресації, наведеної вище.

Крок 1: Налаштуйте IP-адрес для обох маршрутизаторів.

a. Увімкніть одноадресну маршрутизацію IPv6 на обох маршрутизаторах.

b. Налаштуйте IP-адресу для всіх інтерфейсів відповідно до таблиці адресації.

Крок 2: Перевірте адресацію.

a. Запустіть на виконання команду для перевірки призначення IPv4 інтерфейсам.

b. Запустіть на виконання команду для перевірки призначення IPv6 інтерфейсам.

Крок 3: Збережіть конфігурацію.

Збережіть поточну конфігурацію у конфігураційному файлі запуску на обох маршрутизаторах.

Частина 3: Налаштування та перевірка статичної маршрутизації та маршрутизації за замовчуванням для IPv4 на R1 і R2

У Частині 3 ви налаштуєте статичну маршрутизацію та маршрутизацію за замовчуванням на R1 та R2 для забезпечення повноцінного з'єднання між маршрутизаторами за допомогою IPv4. Знову ж таки, статична маршрутизація, яка використовується в цьому завданні, призначена не для реалізації найкращих практик, а для оцінювання вашої здатності виконувати необхідні налаштування.

Крок 1: На маршрутизаторі R1 налаштуйте статичний маршрут до мережі Loopback1 маршрутизатора R2 як наступний перехід, використовуючи адресу G0/0/1 R2.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/1 R2 доступний.

b. Налаштуйте статичний маршрут до мережі Loopback1 маршрутизатора R2, використовуючи адресу інтерфейсу G0/0/1 R2.

Крок 2: На маршрутизаторі R1 налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R2.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/0 R2 доступний.

b. Налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R2.

Крок 3: На маршрутизаторі R1 налаштуйте змінний статичний маршрут за замовчуванням з використанням адреси G0/0/1 R2.

Налаштуйте змінний статичний маршрут за замовчуванням на AD = 80 з використанням адреси G0/0/1 R2.

Крок 4: На маршрутизаторі R2 налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R1.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/0 R1 доступний.

b. Налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R1.

Крок 5: Переконайтесь, що маршрути працюють.

a. Скористайтесь командою **show ip route**, щоб переконатися, що таблиця маршрутизації R1 відображає маршрути статичні та за замовчуванням.

b. На маршрутизаторі R1 застосуйте команду **traceroute 10.2.0.1**. Результат повинен показати, що наступний перехід – 192.168.1.2.

c. На маршрутизаторі R1 застосуйте команду **traceroute 209.165.200.193**. Результат повинен показати, що наступний перехід – 172.16.1.2.

d. Застосуйте команду **shutdown** на G0/0/0 R1.

e. Переконайтесь, що змінний статичний маршрут працює. Спочатку застосуйте команду **show ip route static**. Повинні відобразитися два статичні маршрути: маршрут за замовчуванням з AD = 80 та маршрут до мережі 10.2.0.0/24 з AD = 1.

f. Продемонструйте роботу змінного статичного маршруту, застосувавши команду **traceroute 209.165.200.193**. Як наступний перехід у маршруті трасування зазначатиметься 192.168.1.2.

g. Застосуйте команду **shutdown** на G0/0/0 R1.

Частина 4: Налаштування та перевірка статичної маршрутизації та маршрутизації за замовчуванням для IPv6 на R1 і R2

У Частині 4 ви налаштуєте на R1 і R2 статичну маршрутизацію та маршрутизацію за замовчуванням для забезпечення повноцінного з'єднання між маршрутизаторами за допомогою IPv6. Знову ж таки, запропонована статична маршрутизація призначена не для реалізації найкращих практик, а для оцінювання вашої здатності виконувати необхідні налаштування.

Крок 1: На маршрутизаторі R2 налаштуйте статичний маршрут до мережі Loopback1 маршрутизатора R1 як наступний перехід, використовуючи адресу G0/0/1 R1.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/1 R1 доступний.

b. Налаштуйте статичний маршрут до мережі Loopback1 маршрутизатора R1, використовуючи адресу G0/0/1 R1.

Крок 2: На маршрутизаторі R2 налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R1.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/0 R1 доступний.

b. Налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R1.

Крок 3: На маршрутизаторі R2 налаштуйте змінний статичний маршрут за замовчуванням з використанням адреси G0/0/1 R1.

Налаштуйте змінний статичний маршрут за замовчуванням з AD = 80, використавши адресу G0/0/1 R2.

Крок 4: На маршрутизаторі R1 налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R1.

a. Скористайтеся командою **ping**, щоб переконатися, що інтерфейс G0/0/0 R2 доступний.

b. Налаштуйте статичний маршрут за замовчуванням з використанням адреси G0/0/0 R2.

Крок 5: Переконайтесь, що маршрути працюють.

a. Скористайтесь командою **show ipv6 route**, щоб переконатися, що статичний маршрут і маршрут за замовчуванням містяться у таблиці маршрутизації R2.

b. На R2 застосуйте команду **traceroute 2001:db8:acad:10::1**. Результат повинен відобразити адресу наступного переходу 2001:db8:acad:1::1.

c. На R2 застосуйте команду **traceroute 2001:db8:acad:209::1**. Результат повинен відобразити адресу наступного переходу 2001:db8:acad:2::1.

d. Застосуйте команду **shutdown** на G0/0/0 R2.

e. Переконайтесь, що змінний статичний маршрут працює. Спочатку застосуйте команду **show ipv6 route static**. Повинні відобразитися два статичні маршрути: маршрут за замовчуванням з AD = 80 та маршрут до мережі 2001:db8:acad:10::/64 з AD = 1.

f. Нарешті, продемонструйте роботу змінного статичного маршруту, запустивши на виконання команду **traceroute 2001:db8:acad:209::1**. Як наступний перехід у маршруті трасування зазначатиметься 2001:db8:acad:1::1.

Зведена таблиця інтерфейсів маршрутизатора

Модель маршрутизатора	Інтерфейс Ethernet №1	Інтерфейс Ethernet №2	Інтерфейс Serial №1	Інтерфейс Serial №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Примітка: Щоб дізнатись конфігурацію маршрутизатора, подивіться на інтерфейси аби визначити тип маршрутизатора та скільки інтерфейсів він містить. Неможливо ефективно перелічити всі комбінації налаштувань для кожного класу маршрутизаторів. Ця таблиця містить ідентифікатори для можливих комбінацій Ethernet- та Serial-інтерфейсів пристрою. У таблиці немає інших типів інтерфейсів, хоча конкретний маршрутизатор може містити їх. Прикладом може бути інтерфейс ISDN BRI. У дужках – скорочена назва, яка може бути використана у командах Cisco IOS при зверненні до інтерфейсу.