Навчально-методична література

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМП'ЮТЕРНІ МЕРЕЖІ

(Модуль 3)

для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»

Тернопіль
2023

Методичні вказівки для виконання лабораторних робіт з курсу «Комп’ютерні мережі». Модуль 3. Для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» /укл. А. Г. Микитишин, О. С. Голотенко. // ТНТУ. – 2023. – 75 с.

Укладачі: Андрій МИКИТИШИН, канд. техн. наук, доц.
Олександр ГОЛОТЕНКО, канд. техн. наук, доц.

Рецензент: Сергій МАРЦЕНКО, канд. техн. наук, доц.

Відповідальний за випуск: Олександр ГОЛОТЕНКО, канд. техн. наук., доц.

Схвалено та рекомендовано до друку:

Протокол кафедри КТ №6 від 07.12.2023 р.

Протокол НМК факультету прикладних інформаційних технологій та електроінженерії №4 від 12.12.2023 р.

Методичні вказівки призначені для проведення лабораторних робіт з дисципліни «Комп'ютерні мережі» для студентів, які навчаються за спеціальністю 151 «Автоматизація та комп’ютерно-інтегровані технології». Викладені матеріали приведені з урахуванням модульної системи навчання, рекомендацій до самостійної роботи і індивідуальних завдань, тем лабораторних занять, тестів, екзаменаційних питань, типової форми та вимог для комплексної перевірки знань з дисципліни.

ЗМІСТ

Лабораторна робота №13.1 Навігація в IOS 4
Лабораторна робота №13.2 Налаштування початкових параметрів комутатора 9
Лабораторна робота №13.3 Налаштування базового з'єднання між комутатором та ПК 15
Лабораторна робота №14.1 Налаштування початкових параметрів маршрутизатора 19
Лабораторна робота №14.2 Налаштування інтерфейсів маршрутизатора 23
Лабораторна робота №14.3 Перевірка зв'язку між безпосередньо під'єднаними мережами 28
Лабораторна робота №15.1 Дослідження реалізації VLAN 31
Лабораторна робота №15.2 Налаштування VLAN 35
Лабораторна робота №15.3 Налаштування транкового каналу 39
Лабораторна робота №16 Налаштування маршрутизації між VLAN 42
Лабораторна робота №17 Дослідження принципів роботи STP для уникнення петель 45
Лабораторна робота №18 Налаштування EtherChannel 47
Лабораторна робота №19.1 Налаштування статичного NAT 54
Лабораторна робота №19.2 Налаштування PAT 56
Лабораторна робота №19.3 Налаштування DHCPv4 59
Лабораторна робота №20 Налаштування статичних маршрутів та маршрутів за замовчуванням IPv4 і IPv6 63
Лабораторна робота №21.1 Налаштування динамічної маршрутизації на базі протоколу RIP 68
Лабораторна робота №21.2 Налаштування OSPFv2 для однієї зони 72

Лабораторна робота №13.1
Навігація в IOS

Цілі та задачі

Частина 1: Основні під'єднання, доступ до CLI та вивчення довідки

Частина 2: Вивчення режимів EXEC Частина 3: Налаштування годинника

Довідкова інформація / Сценарій

При виконанні цього завдання ви отримаєте навички, необхідні для навігації по Cisco IOS, включаючи різні режими доступу користувачів, різні режими конфігурації та деякі загальні команди, що часто використовуються. Ви також отримаєте практичні навички з доступу до контекстної довідки налаштування команди **clock**.

Інструкції

Частина 1: Основні під'єднання, доступ до CLI та вивчення довідки

Крок 1: Під'єднайте PC1 до S1 за допомогою консольного кабеля.

1) Натисніть на піктограму **Connections** (у вигляді блискавки) в лівому нижньому куті вікна Packet Tracer.
2) Оберіть світло-блакитний консольний кабель, натиснувши на нього. Вигляд покажчика миші зміниться на з'єднувач з висячим на ньому кабелем.
3) Натисніть на **PC1**. У вікні відображається опція для під'єднання RS-232. Під'єднайте кабель до порту RS-232.
4) Перетягніть інший кінець під'єднання консолі на комутатор S1 і натисніть до комутатора, щоб відкрити список з'єднань.
5) Виберіть порт **Console**, щоб завершити з'єднання.

Крок 2: Встановіть сеанс роботи через термінал з S1.

1) Натисніть на **PC1** і потім оберіть **Desktop**.
2) Натисніть на піктограму застосунку **Terminal**. Переконайтесь, що налаштування портів за замовчуванням правильні.

Яке значення біт на секунду встановлено?

3) Натисніть **OK**.
4) На екрані, що з’явиться, може відображатися кілька повідомлень. Десь на екрані повинно бути повідомлення **Press RETURN to get started!**. Натисніть клавішу ENTER.

Що відображається на екрані?

Крок 3: Ознайомтеся з довідкою про IOS.

1) IOS може надати допомогу для команд залежно від рівня доступу. Підказка, яка відображається в даний момент, називається **User EXEC**, і пристрій очікує введення команди. Основна форма довідки - набрати в запиті знак питання (?) для відображення списку команд.

S1> **?**

Яка команда починається з літери ‘C’?

2) У запиті введіть **t**, а потім знак питання (?).

S1> **t?**

Які команди відображаються?

У запиті введіть **te**, а потім знак питання (?).

S1> **te?**

Які команди відображаються?

Цей тип довідки називається контекстною довідкою. Вона надає більше інформації по мірі уточнення команд.

Частина 2: Вивчення режимів EXEC

У другій частині цього завдання ви перейдете в привілейований режим EXEC і виконаєте додаткові команди.

Крок 1: Увійдіть у привілейований режим EXEC.

1) У запиті введіть знак питання (?).

S1> **?**

Яка інформація відображається для команди **enable**?

2) Введіть **en** і натисніть кнопку **Tab**.

S1> **en<Tab>**

Яка інформація відображається після натиснення кнопки Tab?

Це називається завершенням команди. Коли вводиться частина команди, клавішу Tab можна використовувати для завершення команди. Якщо введених

символів достатньо, щоб команда була унікальною, як у випадку з командою enable, то відображається частина команди, що залишилася.

Що буде, якщо ви введете **te<Tab>** у рядку?

3) Введіть команду **enable** і натисніть ENTER.

Як змінився рядок?

4) У відповідь на запит введіть знак питання (**?**).

S1# **?**

В користувацькому режимі EXEC з літери ‘C’ починається одна команда.

Скільки команд відображається зараз, коли активований привілейований режим EXEC? (Підказка: ви можете ввести c?, щоб вивести список команд, що починаються з літери ‘C’.)

Крок 2: Увійдіть до режиму глобальної конфігурації

1) У привілейованому режимі EXEC налаштована одна з команд, що починається з літери ‘C’: **configure**. Введіть повну команду або достатню кількість літер команди, щоб зробити її унікальною. Натисніть клавішу <**Tab**> для завершення вводу команди та натисніть ENTER.

S1# **configure**

Яке повідомлення буде відображатись?

2) Натисніть Enter, щоб прийняти параметр за замовчуванням в дужках **[terminal]**.

Як змінився рядок?

3) Це називається режимом глобальної конфігурації. Цей режим буде вивчатись у подальших завданнях та лабораторних роботах. Наразі поверніться до привілейованого режиму EXEC, набравши текст **end**, **exit**, або натисніть **Ctrl-Z**.

S1(config)# **exit**
S1#

Частина 3: Налаштування годинника

Крок 1: Використовуйте команду clock.

1) Використовуйте команду **clock** для подальшого вивчення довідки і синтаксису команд. Введіть **show clock** в запрошенні привілейованого режиму EXEC.

S1# **show clock**

Яка інформація відобразилась? Який рік відображається?

2) Використовуйте контекстну довідку і команду **clock**, щоб встановити поточний час на комутаторі. Введіть команду **clock** і натисніть ENTER.

S1# **clock**<ENTER>

Яка інформація відобразилась?

3) IOS повертає повідомлення **"% Incomplete command**", що вказує на те, що команді **clock** потрібно більше параметрів. У будь-який час, коли Вам потрібна додаткова інформація, можна отримати довідку, ввівши пробіл після команди і знак питання (?).

S1# clock ?

Яка інформація відобразилась?

4) Встановіть годинник за допомогою команди **clock set**. Виконайте команду покроково.

S1# **clock set ?**

Яка інформація відобразилась?

Що було б відображено, якби було введено лише команду clock set, а запит про допомогу не було зроблено за допомогою знака питання?

5) На основі інформації, яка запитується при виконанні команди **clock set** ?, введіть час 3:00 вечора, використовуючи 24-годинний формат, у вигляді 15:00:00. Перевірте, чи потрібно більше параметрів.

S1# **clock set 15:00:00 ?**

У вихідних даних відповідь на запит на додаткову інформацію:

<1-31> Day of the month

MONTH Month of the year

6) Спробуйте встановити дату на 01/31/2035, використовуючи формат, який запитується. Для завершення процесу може знадобитися додатковий запит на допомогу з використанням контекстної довідки. Коли закінчите, виконайте команду show clock , щоб відобразити налаштування годинника. Результат команди повинен відображатися так:

S1# **show clock**
*15:0:4.869 UTC Tue Jan 31 2035

7) Якщо Ваш результат відрізняється, спробуйте виконати наступну команду, щоб отримати вищенаведений результат:

S1# **clock set 15:00:00 31 Jan 2035**

Крок 2: Вивчіть додаткові командні повідомлення.

1) IOS надає різні вихідні дані для неправильних або неповних команд. Продовжуйте використовувати команду **clock**, щоб вивчити інші повідомлення, які можуть зустрітися при використанні IOS.
2) Введіть наступні команди і запишіть результат:

S1# **cl<tab>**
Яка інформація відобразилась?

S1# **clock**
Яка інформація відобразилась?

S1# **clock set 25:00:00**
Яка інформація відобразилась?

S1# **clock set 15:00:00 32**
Яка інформація відобразилась?

Лабораторна робота №13.2

Налаштування початкових параметрів комутатора

Цілі та задачі

Частина 1. Перевірка конфігурації комутатора за замовчуванням

Частина 2. Налаштування базових параметрів комутатора

Частина 3. Налаштування банера MOTD (повідомлення дня)

Частина 4. Збереження файлів конфігурації в NVRAM

Частина 5. Налаштування комутатора S2

Довідкова інформація / Сценарій

У цій практичній роботі ви будете здійснювати базові налаштування комутатора. Ви забезпечите доступ до інтерфейсу командного рядка CLI та консольного порту за допомогою зашифрованих і відкритих паролів. Ви також будете налаштовувати повідомлення для користувачів при авторизації для входу на комутатор. Ці банери також попереджають неавторизованих користувачів про те, що доступ заборонений.

Примітка: У Packet Tracer комутатор Catalyst 2960 за замовчуванням використовує IOS версії 12.2. При необхідності версію IOS можна оновити з файлового сервера в Packet Tracer. Потім комутатор може бути налаштований на завантаження IOS версії 15.0, якщо потрібна ця версія.

Інструкції

Частина 1: Перевірка конфігурації комутатора за замовчуванням

Крок 1: Увійдіть в привілейований режим EXEC.

Ви можете отримати доступ до всіх команд комутатора з привілейованого режиму EXEC. Однак, оскільки багато команд привілейованого режиму налаштовують поточні параметри, привілейований доступ повинен бути захищений паролем, щоб запобігти несанкціонованому використанню.

Набір команд привілейованого режиму EXEC включає в себе команди, доступні в користувацькому режимі EXEC, безліч додаткових команд і команду **configure**, за допомогою якої забезпечується доступ до режимів конфігурації.

a. Натисніть S1 і перейдіть на вкладку CLI (Інтерфейс командного рядка). Натисніть Enter.

b. Увійдіть у привілейований режим EXEC, використовуючи команду **enable**:

   Switch> **enable**

   Switch#

   Зверніть увагу, що змінився вигляд командного рядка, щоб відобразити привілейований режим EXEC.

Крок 2: Дослідіть поточну конфігурацію комутатора.

Введіть команду **show running-config** .

Switch# **show running-config**

Дайте відповідь на наступні запитання

Скільки інтерфейсів Fast Ethernet має комутатор?

Скільки інтерфейсів Gigabit Ethernet має комутатор?

Який діапазон значень показано для ліній vty?

Яка команда відображає поточний вміст енергонезалежної оперативної пам'яті (NVRAM)?

Чому комутатор відповідає повідомленням “startup-config is not present?”

Частина 2: Налаштування основних параметрів комутатора
Крок 1: Призначте комутатору ім’я.

Для налаштування параметрів комутатора може знадобитися переходити між різними режимами конфігурації. Зверніть увагу, як змінюється вигляд командного рядка при переході між режимами командного рядка комутатора.

Switch# **configure terminal**

Switch(config)# **hostname S1**

S1(config)# **exit**

S1#

Крок 2: Забезпечте безпечний доступ до консолі.

Для безпечного доступу до консолі перейдіть в режим config-line і встановіть для консолі пароль **letmein**.

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **line console 0**

S1(config-line)# **password letmein**

S1(config-line)# **login**

S1(config-line)# **exit**

S1(config)# **exit**

%SYS-5-CONFIG_I: Configured from console by

console S1#

Для чого потрібна команда **login**?

Крок 3: Переконайтеся, що доступ до консолі захищений.

Вийдіть з привілейованого режиму, щоб переконатися, що для консольного порту встановлено пароль.

S1# **exit**

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

S1>

Примітка: Якщо комутатор не виводить запит на введення пароля, значить, ви не налаштували параметр **login** на кроці 2.

Крок 4: Забезпечте безпечний доступ до привілейованого режиму.

Встановіть для **enable** пароль **c1$c0**. Цей пароль обмежує доступ до привілейованого режиму.

Примітка: Символ **0** в **c1$c0** - це нуль, а не велика літера «O». Налаштування пароля буде оцінено як виконане успішно тільки після того, як ви зашифруєте його на кроці 8.

S1> **enable**

S1# **configure terminal**

S1(config)# **enable password c1$c0**

S1(config)# **exit**

%SYS-5-CONFIG_I: Configured from console by console S1#

Крок 5: Переконайтеся, що доступ до привілейованого режиму захищений.

a. Виконайте команду **exit** ще раз, щоб вийти з комутатора.

b. Натисніть **<Enter>**, після чого вам буде запропоновано ввести пароль.

   User Access Verification

   Password:

c. Перший пароль - це пароль для консолі, який був заданий для **line con 0**. Введіть цей пароль, щоб повернутися в користувацький режим EXEC.

d. Введіть команду для доступу до привілейованого режиму.

e. Введіть другий пароль, який був заданий для обмеження доступу до привілейованого режиму EXEC.

f. Перевірте конфігурацію, переглянувши вміст файлу running-configuration:

   S1# **show running-config**

Зверніть увагу, що паролі для консолі і привілейованого режиму відображаються у вигляді звичайного тексту. Це може становити загрозу безпеці, якщо хтось підглядає через ваше плече або отримує доступ до файлів конфігурації, що зберігаються в резервному сховищі.

Крок 6: Налаштуйте зашифрований пароль для доступу до привілейованого режиму.

Пароль **Enable password** потрібно замінити на новий зашифрований пароль за допомогою команди **enable secret** . Встановіть з enable secret пароль **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Примітка: Пароль **enable secret** має пріоритет перед паролем **enable**. Якщо для комутатора задані обидва паролі, потрібно ввести пароль **enable secret** для переходу в привілейований режим EXEC.

Крок 7: Переконайтеся в тому, що пароль enable secret додано в файл конфігурації.

Введіть команду **show running-config** ще раз, щоб перевірити, чи налаштовано новий пароль enable secret.

Примітка: Команду **show running-config** можна скоротити до

```
S1# show run
```

Що відображається в якості пароля enable secret?

Чому пароль enable secret відображається не так, як було задано?

Крок 8: Зашифруйте паролі enable і console.

Як було видно на кроці 7, пароль **enable secret** зашифрований, а паролі **enable** та **console** зберігаються у вигляді звичайного тексту. Зашифруйте ці відкриті паролі за допомогою команди **service password-encryption**.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Якщо встановити на комутаторі інші паролі, вони будуть зберігатися в файлі конфігурації у вигляді звичайного тексту чи в зашифрованому вигляді? Поясніть.

Частина 3: Налаштування банера MOTD
Крок 1: Налаштуйте банер MOTD (повідомлення дня).

У набір команд Cisco IOS входить команда, що дозволяє налаштувати повідомлення, яке бачитимуть всі, хто входить в систему на комутаторі. Це повідомлення називається повідомленням дня або банером MOTD (Message Of The Day). Текст банера потрібно обмежити подвійними лапками або використовувати роздільник, відмінний від будь-якого символу в рядку MOTD.

S1# **config t**
S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by
console S1#

Коли буде відображатися цей банер?

Навіщо на всіх комутаторах потрібно налаштувати банер MOTD?

Частина 4: Збереження файлів конфігурації в NVRAM
Крок 1: Перевірте правильність конфігурації за допомогою команди show run.

Збережіть файл конфігурації. Ви завершили основне налаштування комутатора. Тепер зробіть резервну копію файлу поточної конфігурації в NVRAM, щоб переконатися, що внесені зміни не втратяться при перезавантаженні системи або втраті живлення.

S1# **copy running-config startup-config**
Destination filename [startup-config]?**[Enter]**
Building configuration...
[OK]

Яка найкоротша версія команди **copy running-config startup-config**?

Дослідіть файл стартової конфігурації.
Яка команда відображає вміст NVRAM?

Чи всі внесені зміни були записані у файл?

Частина 5: Налаштування комутатора S2

Ви завершили налаштування комутатора S1. Тепер аналогічно налаштуйте комутатор S2. Якщо ви не можете згадати команди, поверніться до частин 1-4.

Налаштуйте для комутатора S2 наступні параметри:

a. Ім'я пристрою: **S2**

b. Захистіть доступ до консолі паролем **letmein**.

c. Встановіть в якості пароля enable password **c1$c0** , а в якості пароля enable secret - **itsasecret**.

d. Налаштуйте відповідне повідомлення для тих, хто під'єднується до комутатора.

e. Зашифруйте всі відкриті паролі.

f. Переконайтесь, що конфігурація правильна.

g. Збережіть файл конфігурації, щоб не втратити її у випадку відключення живлення комутатора.

Лабораторна робота №13.3

Налаштування базового з'єднання між комутатором та ПК

Таблиця адресації

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

Цілі та задачі

Частина 1: Налаштування базової конфігурації на S1 та S2

Частина 2: Конфігурування ПК

Частина 3. Налаштування інтерфейсу керування комутатором

Передумови

У цьому завданні ви спочатку виконаєте базове налаштування комутатора. Потім ви створите основні під'єднання, налаштувавши IP-адреси на комутаторах і ПК. Коли конфігурація IP-адресації буде завершена, ви будете використовувати різні команди **show** для перевірки конфігурації та використовувати команду **ping** для перевірки базового з'єднання між пристроями.

Інструкції

Частина 1: Налаштування базової конфігурації на S1 та S2

Виконайте наступні кроки на S1 і S2.

Крок 1: Налаштуйте ім'я вузла на S1.

a. Натисніть на **S1**, а потім натисніть на вкладку CLI.

b. Введіть потрібну команду, щоб призначити вузлу ім'я S1.

Крок 2: Налаштуйте паролі для консолі і привілейованого режиму EXEC.

a. Використовуйте слово **cisco** для пароля консолі.

b. Використовуйте слово **class** для пароля привілейованого режиму EXEC.

Крок 3: Перевірте конфігурації паролів для S1.

Як можна перевірити, чи обидва паролі були налаштовані правильно?

Крок 4: Налаштуйте банерне повідомлення (MOTD Banner)

Використовуйте відповідний текст банера для запобігання несанкціонованого доступу. Приклад тексту наведено нижче:

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

Крок 5: Збережіть файл конфігурації у NVRAM.

Яку команду необхідно для цього виконати?

Крок 6: Повторіть кроки 1-5 для S2.

Частина 2: Конфігурування ПК

Налаштуйте IP-адреси для PC1 і PC2.

Крок 1: Налаштуйте IP-адреси на обох ПК.

a. Натисніть на PC1 і відкрийте вкладку Desktop (Робочий стіл).

b. Натисніть на IP Configuration (Налаштування IP-адрес). У таблиці адресації вище можна побачити, що для PC1 призначена IP-адреса 192.168.1.1, а маска підмережі - 255.255.255.0. Введіть ці дані для PC1 у вікні IP Configuration (Налаштування IP-адрес).

c. Повторіть кроки 1a і 1b для PC2.

Крок 2: Перевірте під'єднання до комутаторів.

a. Натисніть на PC1. Закрийте вікно IP Configuration, якщо воно все ще відкрите. У вкладці Desktop, натисніть на Command Prompt.

b. Введіть команду **ping** та IP-адресу для S1 і натисніть Enter.

PC> **ping 192.168.1.253**

Чи вдалося виконати команду? Поясніть.

Частина 3: Налаштування інтерфейсу керування комутатором

Налаштуйте IP-адреси для S1 і S2.

Крок 1: Налаштуйте IP-адресу для S1.

Комутатори можна використовувати в режимі «plug&play». Це означає, що вони можуть почати працювати і без попереднього налаштування. Комутатори пересилають дані між портами, використовуючи MAC-адреси.

Якщо це так, для чого тоді потрібно налаштовувати IP-адреси?

Щоб налаштувати IP-адресу на комутаторі S1, використовуйте наступні команди.

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

Навіщо ви вводите команду **no shutdown**?

Крок 2: Налаштуйте IP-адресу для S2.

Використовуючи дані з таблиці адресації, налаштуйте IP-адресу для S2.

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

Використовуйте команду **show ip interface brief** для відображення IP-адрес і стану всіх портів та інтерфейсів комутатора. Для цього можна також використовувати команду **show running-config**.

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

Яка команда використовується для збереження файлу конфігурації з оперативної пам'яті в NVRAM?

Крок 5: Перевірте під'єднання до мережі.

Під'єднання до мережі можна перевірити за допомогою команди **ping**. Дуже важливо, щоб зв'язок існував по всій мережі. У разі збою необхідно усунути несправність. Перевірте зв'язок комутаторів S1 і S2 з комп'ютерами PC1 і PC2.

a. Натисніть на PC1 і відкрийте вкладку Desktop (Робочий стіл).

b. Натисніть на Command Prompt.

c. За допомогою команди ping перевірте доступність IP-адреси комп'ютера PC2.

d. За допомогою команди ping перевірте доступність IP-адреси комутатора S1.

e. За допомогою команди ping перевірте доступність IP-адреси комутатора S2.

Примітка: Ви також можете використовувати команду **ping** в інтерфейсі командного рядка комутатора і на PC2.

Всі перевірки повинні бути успішними. Якщо результат першої перевірки - 80%, повторіть спробу. Тепер результат повинен бути 100%. Пізніше ви дізнаєтесь, чому перша перевірка іноді завершується невдало. Якщо ви не можете пропінгувати будь-який з пристроїв, перевірте конфігурацію на наявність помилок.

Лабораторна робота №14.1
Налаштування початкових параметрів маршрутизатора

Цілі та задачі

Частина 1: Перевірка конфігурації маршрутизатора за замовчуванням

Частина 2: Налаштування та перевірка початкової конфігурації маршрутизатора

Частина 3: Збереження файлу поточної конфігурації

Довідкова інформація

У цьому завданні ви виконаєте базові налаштування маршрутизатора. Ви забезпечите доступ до інтерфейсу командного рядка CLI та консольного порту за допомогою зашифрованих і відкритих паролів. Ви також налаштуєте на маршрутизаторі вхідне повідомлення для користувачів, що авторизуються. Ці банери попереджають неуповноважених користувачів про те, що доступ заборонено. На завершення, ви перевірите та збережете свою поточну конфігурацію.

Інструкції

Частина 1: Перевірка конфігурації маршрутизатора за замовчуванням

Крок 1: Встановіть консольне з'єднання із PCA до R1.

a. Виберіть кабель **Console** із доступних типів з'єднань.
b. Натисніть **PCA** і виберіть **RS 232**.
c. Натисніть **R1** і виберіть **Console**.
d. Натисніть **PCA** > вкладку **Desktop** > **Terminal**.
e. Натисніть **OK** та клавішу **ENTER**. Тепер ви можете налаштовувати **R1**.

Крок 2: Увійдіть в привілейований режим і перевірте поточну конфігурацію.

Ви можете отримати доступ до всіх команд маршрутизатора з привілейованого режиму EXEC. Однак, оскільки багато з них використовуються для налаштування поточних параметрів, привілейований доступ повинен бути захищений паролем, щоб запобігти несанкціонованому використанню.

a. Увійдіть в привілейований режим EXEC, ввівши команду **enable**.

   Router> **enable**

   Router#

   Зауважте, що змінилось позначення в рядку конфігурації на таке, що відображає привілейований режим EXEC.

b. Введіть команду **show running-config**.

Router# **show running-config**

Яке ім'я у маршрутизатора?

Скільки інтерфейсів Fast Ethernet має Router?

Скільки інтерфейсів Gigabit Ethernet має Router?

Скільки послідовних інтерфейсів має маршрутизатор?

Який діапазон значень показано для ліній vty?

c. Відобразіть поточний вміст NVRAM.

Router# **show startup-config**

startup-config is not present

Чому маршрутизатор відповідає повідомленням **startup-config is not present**? Чому відображається таке повідомлення? Чим пояснюється поява цього повідомлення?

Частина 2: Налаштування та перевірка початкових параметрів маршрутизатора

Налаштування параметрів маршрутизатора може потребувати переходу між різними режимами конфігурації. Зверніть увагу, як змінюються позначки командного рядка під час переходу між режимами конфігурації IOS.

Крок 1: Налаштуйте початкові параметри на R1.

Примітка: Якщо у вас виникають труднощі із запам'ятовуванням команд, перегляньте вміст цієї теми. Команди такі ж, як ви налаштували на комутаторі.

a. Налаштуйте **R1** як ім’я хоста.

b. Налаштуйте текст щоденного повідомлення: **Unauthorized access is strictly prohibited.**

c. Зашифруйте всі відкриті паролі.

Використовуйте такі паролі:

1) Для привілейованого режиму EXEC, незашифрований: **cisco**
2) Для привілейованого режиму EXEC, зашифрований: **itsasecret**
3) Для консольного з'єднання: **letmein**

Крок 2: Перевірте початкові налаштування на R1.

a. Перевірте початкові налаштування, переглянувши конфігурацію R1.

Яку команду ви використовуєте?

b. Вийдіть із поточного сеансу налаштування консолі, поки не побачите таке повідомлення:

R1 con0 is now available

Press RETURN to get started.

c. Натисніть клавішу **ENTER**; ви повинні побачити таке повідомлення:

Unauthorized access is strictly prohibited.

User Access Verification

Password:

Чому кожен маршрутизатор повинен мати банер щоденного повідомлення (MOTD, message-of-theday)?

Якщо не пропонується ввести пароль для входу в режим користувача EXEC, яку команду консольної лінії ви забули налаштувати?

d. Введіть паролі, необхідні для повернення до привілейованого режиму EXEC.

Чому команда **enable secret** password дозволить доступ до привілейованого режиму, а команда **enable password** більше не діятиме?

Якщо ви в майбутньому налаштуєте на маршрутизаторі ще якісь паролі, вони відображатимуться у файлі конфігурації у вигляді простого тексту чи у зашифрованому вигляді? Поясніть.

Частина 3: Збереження файлу поточної конфігурації

Крок 1: Збережіть файл конфігурації у NVRAM.

a. Ви налаштували початкові параметри для маршрутизатора **R1**. Тепер зробіть резервну копію файлу поточної конфігурації в NVRAM, щоб переконатися, що внесені зміни не втратяться при перезавантаженні системи або вимкненні живлення.

Яку команду ви ввели, щоб зберегти конфігурацію в NVRAM?

Який найкоротший, однозначний варіант цієї команди?

Яка команда відображає вміст NVRAM?

d. Переконайтеся, що всі налаштовані параметри збережено. Якщо ні, проаналізуйте виведені дані і визначте, які команди не були виконані або були введені неправильно. Ви також можете натиснути кнопку **Check Results** у вікні інструкції.

Крок 2: Додатково: Збережіть файл конфігурації запуску у flash-пам'ять.

Хоча ви дізнаєтесь більше про керування flash-сховищем маршрутизатора в наступних розділах, можливо, вам буде цікаво знати, що в якості додаткової процедури резервного копіювання ви можете зберегти файл початкової конфігурації у flash. За замовчуванням маршрутизатор буде завантажувати стартову конфігурацію з NVRAM, але якщо NVRAM пошкоджена, ви можете відновити конфігурацію запуску, скопіювавши її з flash.

Щоб зберегти конфігурацію запуску у flash, виконайте наступні дії.

a. Перевірте вміст flash за допомогою команди **show flash**:

R1# **show flash**

Скільки файлів зараз зберігається у flash?

Який із цих файлів, на вашу думку, є образом IOS?

Чому, на вашу думку, цей файл є образом IOS?

b. Збережіть файл startup configuration file у flash за допомогою наступних команд:

R1# **copy startup-config flash**

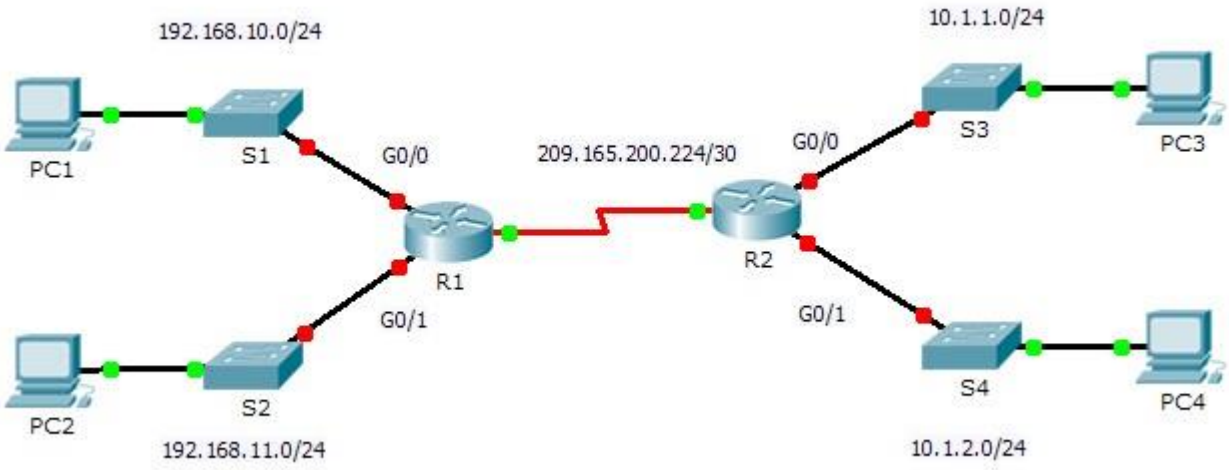
Destination filename [startup-config]

Маршрутизатор пропонує вам записувати файл у flash, використовуючи ім'я в дужках. Якщо відповідь "так", тоді натисніть клавішу **ENTER**; якщо ні - введіть відповідне ім’я та натисніть **ENTER**.

c. Скористайтеся командою **show flash**, щоб переконатися, що файл стартової конфігурації тепер зберігається у flash.

Лабораторна робота №14.2
Налаштування інтерфейсів маршрутизатора

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0	192.168.10.1	255.255.255.0	Недоступно
	G0/1	192.168.11.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	Недоступно
R2	G0/0	10.1.1.1	255.255.255.0	Недоступно
	G0/1	10.1.2.1	255.255.255.0	Недоступно
	S0/0/0	209.165.200.226	255.255.255.252	Недоступно
PC1	Мережевий адаптер	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Мережевий адаптер	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Мережевий адаптер	10.1.1.10	255.255.255.0	10.1.1.1
PC4	Мережевий адаптер	10.1.2.10	255.255.255.0	10.1.2.1

Завдання

Частина 1. Відображення відомостей про маршрутизатор

Частина 2. Налаштування інтерфейсів маршрутизатора

Частина 3. Перевірка конфігурації

Вихідні дані

У цій вправі потрібно використовувати різні команди **show** для відображення поточного стану маршрутизатора. Потім потрібно буде використовувати **Таблицю адресації** для налаштування інтерфейсів Ethernet. На завершення завдання вам треба буде використовувати команди для перевірки та тестування виконаних налаштувань.

Примітка. Маршрутизатори в цій вправі вже частково налаштовані. Деякі з налаштувань не розглянуті докладно, але вони потрібні для того, щоб допомогти вам у використанні команд перевірки.

Частина 1: Відображення відомостей про маршрутизатор

Крок 1: Відображення відомостей про інтерфейс маршрутизатора R1.

Примітка. Виберіть пристрій і відкрийте вкладку **CLI** (Інтерфейс командного рядка) для доступу до командного рядка. Пароль консолі - **cisco**. Пароль привілейованого режиму - **class**.

а) Яка команда виводить статистику по всіх інтерфейсах, налаштованих на маршрутизаторі?

б) Яка команда виводить тільки відомості про інтерфейс Serial0/0/0?

в) Введіть команду, щоб відобразити статистику по інтерфейсу Serial0/0/0 на
маршрутизаторі R1, і дайте відповідь на наступні питання.

1) Яка IP-адреса налаштована на інтерфейсі маршрутизатора **R1**?

2) Яку пропускну здатність має інтерфейс Serial0/0/0?

г) Введіть команду, щоб відобразити статистику по інтерфейсу GigabitEthernet0/0, і дайте відповідь на наступні питання.

1) Яка IP-адреса налаштована на інтерфейсі маршрутизатора **R1**?

2) Яка MAC-адреса інтерфейсу Gigabit Ethernet 0/0?

3) Яку пропускну здатність має інтерфейс Gigabit Ethernet0/0?

Крок 2: Відображення загального списку інтерфейсів маршрутизатора R1.

а) Яка команда виводить коротке зведення по поточних інтерфейсах, їх стан і налаштовані на них IP-адреси?

б) Введіть команду на кожному маршрутизаторі і дайте відповідь на наступні
питання.

1) Скільки послідовних інтерфейсів на маршрутизаторах **R1** і **R2**?

2) Скільки інтерфейсів Ethernet на маршрутизаторах **R1** і **R2**?

3) Чи всі інтерфейси Ethernet на маршрутизаторі **R1** однакові? Якщо відповідь "Ні", поясніть відмінності.

Крок 3: Вивід таблиці маршрутизації на маршрутизаторі R1

а) Яка команда показує вміст таблиці маршрутизації?

б) Виконайте команду виводу таблиці маршрутизації на маршрутизаторі **R1** і
дайте відповідь на наступні питання.

1) Скільки в таблиці підключених маршрутів (мають код C)?

2) Запишіть тип маршрутів представлених у списку та адреси мереж?

3) Яким чином маршрутизатор обробляє пакет, призначений для мережі, яка відсутня в таблиці маршрутизації?

Частина 2: Налаштування інтерфейсів маршрутизатора

Крок 1: Налаштування інтерфейсу Gigabit Ethernet0/0 на маршрутизаторі R1.

а) Виконайте наступні команди і включіть інтерфейс Gigabit Ethernet0/0 на маршрутизаторі **R1**:

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

б) Рекомендується вказати опис для кожного інтерфейсу, що допоможе при документуванні відомостей про мережу. Налаштуйте опис інтерфейсу, вказавши, до якого пристрою він підключений.

R1(config-if)#description LAN connection to S1

в) Марштуризатор **R1** тепер має можливіть надістлати ехо-запит на **PC1**.

R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

Крок 2: Налаштування інших інтерфейсів GigabitEthernet на маршрутизаторах R1 і R2.

а) Використовуючи дані з **Таблиці адресації**, завершіть налаштування інтерфейсів на **R1** і **R2**. Для кожного інтерфейсу виконайте такі дії.

1) Налаштуйте IP-адресу і активуйте інтерфейс. Запишіть команди для налаштувань:

2) Налаштуйте відповідний опис інтерфейсу. Запишіть команди для налаштувань:

б) Перевірте конфігурації інтерфейсів.

Крок 3: Зробіть резервну копію конфігурацій в NVRAM.

Збережіть файли конфігурації на обох маршрутизаторах в NVRAM. Яку команду ви використовували?

Частина 3: Перевірка конфігурації

Крок 1: Перевірте конфігурації інтерфейсів за допомогою відповідних команд.

а) Виконайте команду **show ip interface brief** на маршрутизаторах **R1** і **R2**,

щоб швидко переконатися, що інтерфейси мають правильні IP-адреси і вони активні.

Скільки інтерфейсів налаштовано на маршрутизаторах **R1** і **R2** і мають активний стан (up)?

Яка частина конфігурації інтерфейсу НЕ відображається у виведених даних команди?

За допомогою якої команди можна перевірити цю частину конфігурації?

б) Виконайте команду **show ip route** на маршрутизаторах **R1** і **R2**, щоб переглянути поточні таблиці маршрутизації, і дайте відповідь на наступні питання.

1) Скільки підключених маршрутів (мають код **C**) показано на кожному маршрутизаторі?

2) Скільки маршрутів EIGRP (мають код **D**) показано на кожному маршрутизаторі?

3) Якщо маршрутизатор містить дані про всі маршрути в мережі, тоді кількість безпосередньо підключених маршрутів і динамічно отриманих маршрутів (EIGRP) повинна дорівнювати загальній кількості локальних і глобальних мереж. Скільки локальних і глобальних мереж є в топології?

4) Чи відповідає це число кількості маршрутів C і D, показаних в таблиці маршрутизації?

Примітка. Якщо ви відповіли "Ні", значить, ви налаштували не всі параметри. Переглянете кроки в частині 2.

Крок 2: Перевірка наскрізного підключення через мережу.

Тепер ви повинні бути в змозі відправити ехо-запит на будь-який ПК з будь-якого ПК в мережі. Крім того, ви повинні бути в змозі відправляти ехо-запити на активні інтерфейси маршрутизаторів. Наприклад, такі тести повинні успішно виконатися.

- У командному рядку на комп'ютері **ПК1** відправте ехо-запит на **ПК4**. Запишіть результат виконання команди
- У командному рядку на маршрутизаторі **R2** відправте ехо-запит на **ПК2**.

Запишіть результат виконання команди

Лабораторна робота №14.3

Перевірка зв'язку між безпосередньо під’єднаними мережами

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс	Шлюз за замовчуванням
R1	G0/0/0	172.16.20.1/25	N/A
	G0/0/1	172.16.20.129/25	N/A
	S0/1/0	209.165.200.225/30	N/A
PC1	NIC	172.16.20.10/25	172.16.20.1
PC2	NIC	172.16.20.138/25	172.16.20.129
R2	G0/0/0	2001:db8:c0de:12::1/64	N/A
	G0/0/1	2001:db8:c0de:13::1/64	N/A
	S0/1/1	2001:db8:c0de:11::1/64	N/A
		fe80::2	N/A
PC3	NIC	2001:db8:c0de:12::a/64	fe80::2
PC4	NIC	2001:db8:c0de:13::a/64	fe80::2

Цілі та задачі

- Перевірка зв'язку IPv4 між безпосередньо під'єднаними мережами
- Перевірка зв'язку IPv6 між безпосередньо під'єднаними мережами
- Пошук та усунення проблем зі з'єднанням

Довідкова інформація

Маршрутизатори R1 та R2 мають по дві локальні мережі кожен. Ваше завдання - перевірити адресацію на кожному пристрої та перевірити зв'язок між локальними мережами.

Примітка: Пароль для користувацького режиму EXEC - **cisco**. Пароль для привілейованого режиму EXEC - **class**.

Інструкції

Частина 1: Перевірка зв'язку IPv4 між безпосередньо під'єднаними мережами

Крок 1: Перевірте адреси IPv4 та стан порту на маршрутизаторі R1.

a. Перевірте стан налаштованих інтерфейсів за допомогою фільтрації вихідних даних.
   R1# **show ip interface brief | exclude unassigned**

b. На основі вихідних даних виправіть будь-які проблеми стану порту, які ви бачите.

c. Перевірте відповідність IP-адрес, налаштованих на маршрутизаторі R1, **таблиці адресації**. За необхідності внесіть зміни в адресацію.

d. Застосуйте фільтрацію для відображення таблиці маршрутизації так, щоб вихідні дані починались зі слова **Gateway**.

   Примітка: Терміни, які використовуються для фільтрування вихідних даних, можна скоротити відповідно до тексту, якщо збіг унікальний. Наприклад, Gateway, Gate і Ga матимуть однаковий ефект. A G - не матиме. Фільтрація чутлива до регістру**.**

   R1# **show ip route | begin Gate**

   Яка адреса шлюзу останньої інстанції?

e. Відображення інформації про інтерфейс і фільтр для **Description** або **connected**.

   Примітка: Під час використання декількох пошуків **include** або **exclude** можна виконувати шляхом розділення рядків пошуку символом вертикальної риски(|)

   R1# **show interface | include Desc|conn**

   Який Circuit ID відображається у ваших вихідних даних?

f. Відображення конкретної інформації для інтерфейсу G0/0/0 за допомогою фільтрації для **duplex**.
   Які налаштування дуплексу, швидкості і типу середовища?

Крок 2: Перевірте з’єднання.

PC1 та **PC2** повинні мати можливість пінгувати один одного і **Dual Stack Server**. Якщо ні, перевірте стан інтерфейсів і призначені IP-адреси.

Частина 2: Перевірка зв'язку IPv6 між безпосередньо під'єднаними мережами

Крок 1: Перевірте адреси IPv6 і стан порту на маршрутизаторі R2.

a. Перевірте стан налаштованих інтерфейсів.
   R2# **show ipv6 int brief**
   В якому стані налаштовані інтерфейси?

b. Перевірте відповідність IP-адрес **таблиці адресації** та, за необхідності, внесіть зміни до адресації.

Примітка: При зміні адреси IPv6 необхідно видалити неправильну адресу, оскільки інтерфейс здатний підтримувати кілька мереж IPv6.

R2(config)# **int g0/0/1**
R2 (config-if) # **no ipv6 address 2001:db8:c0de:14::1/64**
Налаштуйте правильну адресу на інтерфейсі.

c. Відобразіть таблицю маршрутизації IPv6.

Примітка: Команди фільтрування не працюють з командами IPv6.

d. Відобразіть всі адреси IPv6, налаштовані на інтерфейсах, шляхом фільтрації вихідних даних **running-config**.

Фільтрація вихідних даних на **R2** для **IPv6** або **інтерфейсу**.
R2# **sh run | include ipv6|interface**
Скільки адрес налаштовано на кожному гігабітному інтерфейсі?

Крок 2: Перевірте з'єднання.

PC3 та **PC4** повинні мати можливість пінгувати один одного і **Dual Stack Server**. Якщо ні, перевірте стан інтерфейсу та призначення адрес IPv6.

Лабораторна робота №15.1

Дослідження реалізації VLAN

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
S1	VLAN 99	172.17.99.31	255.255.255.0	N/A
S2	VLAN 99	172.17.99.32	255.255.255.0	N/A
S3	VLAN 99	172.17.99.33	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1
PC7	NIC	172.17.10.27	255.255.255.0	172.17.10.1
PC8	NIC	172.17.20.28	255.255.255.0	172.17.20.1
PC9	NIC	172.17.30.29	255.255.255.0	172.17.30.1

Цілі та задачі

Частина 1. Вивчення процесу передавання широкомовного трафіку у мережі з налаштованими VLAN.

Частина 2. Вивчення процесу передавання широкомовного трафіку у мережі без налаштованих VLAN.

Довідкова інформація

У цьому завданні Ви проведете дослідження процесів передавання широкомовного трафіку у мережі з налаштованими VLAN та без налаштованих VLAN.

Інструкції

Частина 1. Вивчення процесу передавання широкомовного трафіку у VLAN.

Крок 1. Перевірка зв'язку за допомогою команди ping між комп'ютерами PC1 та PC6.

a. Дочекайтеся, поки всі індикатори засвітяться зеленим кольором. Для пришвидшення процесу натисніть кнопку **Fast Forward Time**, розташовану на нижній панелі інструментів.

b. Перейдіть на вкладку **Simulation** та скористайтеся інструментом **Add Simple PDU**. Спочатку натисніть на піктограмі комп'ютера **PC1**, а потім - на піктограмі комп'ютера **PC6**.

c. Натисніть кнопку **Capture/Forward** для покрокового проходження процесу. Дослідіть передачу ARPзапитів через мережу. Коли з'явиться вікно Buffer Full, натисніть кнопку **View Previous Events**.

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

Подивіться на Simulation Panel і дайте відповідь куди комутатор **S3** надіслав повідомлення після отримання?

При нормальній роботі, коли комутатор отримує широкомовний кадр на одному зі своїх портів, він надсилає цей кадр на решту портів. Зверніть увагу, що комутатор **S2** надсилає ARP-запит до комутатора **S1** з порту F0/1. Також зверніть увагу, що комутатор **S3** надсилає ARP-запит до комп'ютера **PC4** з порту F0/11. Обидва комп'ютери **PC1** та **PC4** належать до VLAN 10. Комп'ютер **PC6** належить до VLAN 30. Оскільки широкомовний трафік передається лише в межах певних VLAN, комп'ютер **PC6** ніколи не отримає ARP-запит від комп'ютера **PC1**. Оскільки комп'ютер **PC4** не є отримувачем повідомлення, він відкидає ARP-запит. Перевірка зв'язку за допомогою команди ping з комп'ютера **PC1** буде невдалою через те, що комп'ютер **PC1** ніколи не отримає ARP-відповідь.

Крок 2. Перевірка зв'язку за допомогою команди ping між комп'ютерами PC1 та PC4.

a. Натисніть кнопку **New** у випадаючому списку Scenario 0. Потім натисніть кнопку **Add Simple PDU** для виконання перевірки зв'язку за допомогою команди ping між комп'ютером **PC1** та комп'ютером **PC4**.

b. Натисніть кнопку **Capture/Forward** для покрокового проходження процесу. Дослідіть передачу ARPзапитів через мережу. Коли з'явиться вікно Buffer Full, натисніть кнопку **View Previous Events**.

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

c. Дослідіть Simulation Panel.

При надходженні повідомлення до комутатора **S1**, чому комутатор також надсилає це повідомлення до комп'ютера **PC7**?

Частина 2. Вивчення процесу передавання широкомовного трафіку у мережі без налаштованих VLAN.

Крок 1. Очистіть конфігурації і видаліть бази даних VLAN на всіх трьох комутаторах.

a. Поверніться до режиму **Realtime**.

b. Видаліть стартові конфігурації на всіх 3 комутаторах.

Яка команда використовується для видалення стартової конфігурації комутатора?
Де на комутаторі зберігається файл з інформацією про VLAN?

c. Видаліть файли з інформацією про VLAN на всіх 3 комутаторах.
Яка команда видаляє файл з інформацією про VLAN?

Крок 2. Перезавантажте комутатори.

Використайте команду привілейованого режиму **reload** для перезавантаження комутаторів. Почекайте, поки всі індикатори засвітяться зеленим кольором. Для пришвидшення процесу натисніть кнопку **Fast Forward Time**, яка розміщена в верхній частині панелі інструментів.

Крок 3. Натисніть кнопку Capture/Forward, щоб надіслати ARP-запити та повідомлення команди ping.

a. Після перезавантаження комутаторів та після того як індикатори каналів зв'язку засвітяться зеленим кольором, мережа готова переслати ваші ARP-повідомлення та ping-повідомлення.
b. Виберіть **Scenario 0** з випадаючої вкладки, щоб повернутися до Scenario 0.
c. У режимі **Simulation** натисніть кнопку **Capture/Forward** для покрокового відстеження процесу. Зверніть увагу на те, що зараз комутатори передають ARP-запити через всі порти, за виключенням тих портів, на яких ці ARP-

запити були отримані. Ця стандартна операція комутатора, є тією операцією, впливаючи на яку, VLAN можуть підвищити продуктивність мережі. Широкомовний трафік передається в межах кожної VLAN. Коли з'явиться вікно **Buffer Full**, натисніть кнопку **View Previous Events**.

Питання для самоперевірки

1. Якщо комп'ютер, що належить VLAN 10, надішле широкомовне повідомлення, які пристрої його отримають?

2. Якщо комп'ютер, що належить VLAN 20, надішле широкомовне повідомлення, які пристрої його отримають?

3. Якщо комп'ютер, що належить VLAN 30, надішле широкомовне повідомлення, які пристрої його отримають?

4. Що відбудеться, коли комп'ютер, що належить до VLAN 10, надішле кадр комп'ютерові, що належить до VLAN 30?

5. Що є доменом колізій на комутаторі з точки зору порту?

6. Що є широкомовними доменами на комутаторі з точки зору порту?

Лабораторна робота №15.2
Налаштування VLAN

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Цілі та задачі

Частина 1. Перегляд налаштувань VLAN за замовчуванням

Частина 2. Налаштування VLAN

Частина 3. Встановлення належності портів до VLAN

Довідкова інформація

VLAN корисні при адмініструванні логічних груп користувачів, дозволяючи їх легко переміщувати, змінювати або додавати. Це завдання фокусується на створенні VLAN, призначенні їм назв та встановленні належності портів доступу до певних VLAN.

Частина 1. Перегляд налаштувань VLAN за замовчуванням

Крок 1. Відображення наявних VLAN.

На комутаторі S1 виконаємо команду, яка відображає всі налаштовані VLAN. За замовчуванням всі інтерфейси комутатора належать до VLAN 1.

Крок 2. Перевірка зв'язку між комп'ютерами однієї мережі.

Зверніть увагу, що кожен комп'ютер може перевірити зв'язок за допомогою команди ping з іншим комп'ютером, який належить ті й же підмережі.

- Комп'ютер PC1 може перевірити зв'язок за допомогою команди ping з комп'ютером PC4
- Комп'ютер PC2 може перевірити зв'язок за допомогою команди ping з комп'ютером PC5

- Комп'ютер PC3 може перевірити зв'язок за допомогою команди ping з комп'ютером PC6

Перевірити зв'язок за допомогою команди ping з вузлами з інших мереж не вдається.
Які переваги використання VLAN у комп'ютерній мережі?

Частина 2. Налаштування VLAN

Крок 1. Створення та іменування VLAN на комутаторі S1.

a. Створіть такі VLAN. Назви VLAN чутливі до регістру і повинні точно відповідати вимогам:

- VLAN 10: Faculty/Staff

S1# (config)# **vlan 10**

S1# (config-vlan)# **name Faculty/Staff**

b. Створіть решту VLAN.

- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native
- VLAN 150: VOICE

Крок 2. Перевірка налаштувань VLAN.

Яка команда відобразить лише ім'я VLAN, її стан та перелік включених до неї портів ?

Крок 3. Створення VLAN на комутаторах S2 та S3.

Використовуйте команди з кроку 1, щоб створити і іменувати відповідні VLAN на комутаторах S2 та S3.

Крок 4. Перевірка налаштувань VLAN.

Частина 3. Встановлення належності портів до VLAN

Крок 1. Встановлення належності активних портів до VLAN на комутаторі S2.

a. Налаштуйте інтерфейси комутатора як порти доступу і встановіть їх належність до VLAN:

- VLAN 10: FastEthernet 0/11

S2(config)# **interface f0/11**

S2(config-if)# **switchport mode acces**

S2(config-if)# **switchport access vlan 10**

b. Встановіть належність решти портів до відповідних VLAN.

- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

Крок 2. Встановлення належності активних портів до VLAN на комутаторі S3.

На комутаторі S3 використовуються такі ж налаштування портів доступу VLAN, що і на комутаторі S2. Налаштуйте інтерфейси комутатора як порти доступу і встановіть їх належність до VLAN:

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

Крок 3. Встановлення належності порту FastEthernet 0/11 до VOICE VLAN на комутаторі S3.

На рисунку показано, що до інтерфейсу FastEthernet 0/11 комутатора S3 підключені IP-телефон Cisco IP Phone0 і комп'ютер PC4. IP-телефон містить вбудований трипортовий комутатор 10/100 Мбіт/с. Один порт телефону має позначення Switch і саме через нього телефон підключений до порту комутатора F0/11. Ще один порт телефону має позначення PC і саме до нього підключається комп'ютер PC4. IPтелефон також має вбудований порт, через який забезпечується доступ до його функцій.

Інтерфейс F0/11 комутатора S3 повинен бути налаштований таким чином, щоб забезпечити передачу трафіку користувача комп'ютера PC4 (VLAN 10) і голосового трафіку IP-телефону (VLAN 150). Також на цьому інтерфейсі необхідно активувати функцію QoS та використання значень класу обслуговування (CoS), призначених IP-телефоном. Підтримка прийнятної якості голосового зв'язку для голосового IPтрафіку вимагає виділення мінімальної пропускної здатності. Наведена нижче команда дозволяє забезпечити мінімальну пропускну здатність на порті комутатора.

S3(config)# **interface f0/11**

S3(config-if)# **mls qos trust cos**

S3(config-if)# **switchport access vlan 150**

Крок 4. Перевірка втрати зв'язку.

Раніше комп'ютери, що мали спільний доступ до однієї мережі, могли успішно перевіряти зв'язок один з одним за допомогою команди ping.

Проаналізуйте результати виведення команди, що виконана на комутаторів **S2** та, використовуючи Ваші знання щодо VLAN, дайте відповіді на питання. Зверніть увагу на налаштування порту Gig0/1.

S2# **show vlan brief**

VLAN Name Status Ports

---- ------------------------------ --------- ------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2

10 Faculty/Staff active Fa0/11

20 Students active Fa0/18

30 Guest(Default) active Fa0/6

99 Management&Native active

150 VOICE active

Спробуйте перевірити зв'язок між комп'ютерами PC1 і PC4 за допомогою команди **ping**.

Хоча для портів доступу було виконано налаштування належності до певних VLAN, чи була перевірка зв'язку успішною? Поясніть.

Що можна зробити для вирішення цієї проблеми?

Лабораторна робота №15.3
Налаштування транкового каналу

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Порт комутатора	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Цілі та задачі

Частина 1. Перевірка VLAN

Частина 2. Налаштування транкових каналів зв'язку

Довідкова інформація

Транкові канали необхідні для передавання інформації певних VLAN між комутаторами. Порт комутатора може бути або портом доступу, або транковим портом. Порти доступу передають трафік тієї VLAN, що якої він належить. За замовчуванням транковий порт є членом всіх VLAN. Тому він передає трафік всіх VLAN. Це завдання фокусується на створенні транкових портів і налаштуванні для них Native VLAN, відмінної від прийнятої за замовчуванням.

Інструкції

Частина 1. Перевірка налаштувань VLAN.

Крок 1. Відображення наявних VLAN.

На комутаторі **S1** виконайте команду, яка відобразить всі налаштовані на ньому VLAN. Всього має бути десять VLAN. Зверніть увагу, що всі 26 портів доступу комутатора належать до VLAN 1.

a. На комутаторах **S2** та **S3** виведіть перелік VLAN та переконайтеся, що всі VLAN налаштовані коректно, також переконайтеся, що порти комутатора належать до відповідних VLAN. Для перевірки скористайтеся даними **таблиці адресації**.

Крок 2. Перевірка втрати зв'язку між комп'ютерами однієї і тієї ж мережі.

За допомогою команди ping перевірте зв'язок між вузлами, що належать до однієї VLAN, але підключені до різних комутаторів. Хоча комп'ютери **PC1** та **PC4** належать до однієї мережі, вони не можуть взаємодіяти один з одним. Це пояснюється тим, що для портів, які з'єднують комутатори, за замовчуванням налаштовано належність до VLAN 1. Для того, щоб забезпечити передавання даних між комп'ютерами однієї мережі та VLAN, необхідно налаштувати транкові канали зв'язку.

Частина 2. Налаштування транкового каналу

Крок 1. Налаштування транкового каналу на комутаторі S1 та налаштування використання VLAN 99 як Native VLAN.

a. Налаштуйте інтерфейси G0/1 і G0/2 комутатора S1 для транкування.

S1(config)# **interface range g0/1 - 2**

S1(config-if)# **switchport mode trunk**

b. Налаштування VLAN 99 як Native VLAN для інтерфейсів G0/1 і G0/2 комутатора **S1**.

S1(config-if)# **switchport trunk native vlan 99**

Транковому портові необхідний певний час для того, щоб стати активним. Ця затримка викликана необхідністю виконання процедур протоколу Spanning Tree Protocol. Для прискорення процесу натисніть кнопку **Fast Forward Time**. Після того, як порти стануть активними, Ви періодично отримуватимете такі syslog-повідомлення:

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).

Ви налаштували VLAN 99 як Native VLAN на комутаторі S1. Однак комутатори S2 і S3 ще використовують VLAN 1 як Native VLAN за замовчування, про що зазначено у syslog-повідомленні.

Хоча Ви маєте невідповідність Native VLAN, перевірка зв'язку за допомогою команди ping між комп'ютерами однієї і тієї ж VLAN вже є успішною. Поясніть.

Крок 2. Перевірка, чи активовано транкування на комутаторах S2 та S3.

Виконайте команду **show interface trunk** на комутаторах **S1** та **S2** для того, щоб пересвідчитися, що протокол DTP успішно узгодив параметри транкових каналів між комутатором S1 та комутаторами S2 та S3. Виведені результати також відображають інформацію про транкові інтерфейси комутаторів S2 і S3. Ви дізнаєтеся більше про протокол DTP при подальшому розгляді курсу.

Яким активним VLAN дозволено передавати свої дані через транковий канал?

Крок 3. Виправлення невідповідності Native VLAN на комутаторах S2 і S3.

a. Налаштуйте VLAN 99 як Native VLAN для відповідних інтерфейсів на комутаторах S2 і S3.
b. Виконайте команду **show interface trunk** для того, що перевірити правильність налаштування Native VLAN.

Крок 4. Перевірка налаштувань на комутаторах S2 та S3.

a. Виконайте команду **show** *interface* **switchport** для того, щоб переконатися, що Native VLAN має номер 99.
b. Використайте команду **show vlan** для відображення інформації щодо налаштованих VLAN.

Чому порт G0/1 комутатора S2 більше не належить до VLAN 1?

Лабораторна робота №16

Налаштування маршрутизації між VLAN

Таблиця адресації

Пристрій	Інтерфейс	Адреса IPv4	Маска підмережі	Шлюз за замовчуванням
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Цілі та задачі

Частина 1: Додавання VLAN на комутаторі

Частина 2: Налаштування підінтерфейсів маршрутизатора

Частина 3: Перевірка з'єднання та маршрутизації між VLAN

Сценарій

У цьому завданні ви налаштуєте VLAN і маршрутизацію між VLAN. А також налаштуєте магістральні інтерфейси і перевірите зв'язок між мережами VLAN.

Інструкції

Частина 1: Додавання VLAN на комутаторі

Крок 1: Створіть VLAN на комутаторі S1.

Створіть VLAN 10 і VLAN 30 на **S1**.

Крок 2: Налаштуйте належність портів до VLAN

a. Налаштуйте інтерфейси F0/6 і F0/11 в якості портів доступу і призначте їм VLAN.
   - Призначте порт, підключений до **PC1** для VLAN 10.
   - Призначте порт, підключений до **PC3** для VLAN 30.

b. Виконайте команду **show vlan brief**, щоб перевірити конфігурацію VLAN.

S1# **show vlan brief**

VLAN Name Status Ports
---- ------------------------------ --------- ------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/7, Fa0/8, Fa0/9
Fa0/10, 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, Gig0/1, Gig0/2
10 VLAN0010 active Fa0/11
30 VLAN0030 active Fa0/6
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

Крок 3: Перевірте з'єднання між PC1 і PC3.

Відправте запит ping з **PC1** на **PC3**.

Чи був ping вдалим? Чому ви отримали такий результат?

Частина 2: Налаштування підінтерфейсів

Крок 1: Налаштуйте підінтерфейси на R1 за допомогою інкапсуляції 802.1Q.

a. Створіть підінтерфейс G0/0.10.

- Встановіть тип інкапсуляції 802.1Q і призначте VLAN 10 для підінтерфейсу.
- Зверніться до **Таблиці адресації** і призначте підінтерфейсу правильну IP-адресу.

R1(config)# **int g0/0.10**
R1(config-subif)# **encapsulation dot1Q 10**
R1(config-subif)# **ip address 172.17.10.1 255.255.255.0**

b. Повторіть це для підінтерфейсу G0/0.30.

Крок 2: Перевірте конфігурацію.

a. Команда **show ip interface brief** застосовується для перевірки конфігурації підінтерфейсу. Обидва підінтерфейси відключені. Підінтерфейси - це віртуальні інтерфейси, пов'язані з фізичним інтерфейсом. Тому для того, щоб включити підінтерфейси, необхідно включити фізичний інтерфейс, з яким вони пов'язані.

b. Увімкніть інтерфейс G0/0. Переконайтеся, що підінтерфейси тепер активні.

Частина 3: Перевірка з'єднання та маршрутизації між VLAN

Крок 1: Відправите запит ping з PC1 до PC3.

Відправте запит ping з **PC1** на **PC3**. Запит ping повинен завершитися помилкою. Поясніть.

Крок 2: Увімкніть магістральний канал.

a. На **S1** вводимо команду **show vlan**.
Яку VLAN призначено для G0/1?

b. Оскільки маршрутизатор був налаштований з декількома підінтерфейсами, призначеними для різних VLAN, порт комутатора, що підключається до маршрутизатора, повинен бути налаштований як магістральний канал. Увімкніть магістральний канал на інтерфейсі G0/1.

Як можна визначити за допомогою команди **show vlan**, що інтерфейс є магістральним каналом?

c. Виконайте команду **show interface trunk**, щоб переконатися, що інтерфейс налаштований як магістральний канал.

Крок 3: Перевірка з'єднання.

Якщо конфігурації правильні, PC1 і PC3 повинні мати можливість відправляти запити ping на свої шлюзи за замовчуванням і один до одного. Які адреси використовують PC1 і PC3 як адреси шлюзу за замовчуванням?

Лабораторна робота №17

Дослідження принципів роботи STP для уникнення петель

Цілі та задачі

Ця лабораторна робота передбачає вивчення станів портів і спостереження за процесом збіжності єднального дерева.

- Описати принципи роботи протоколу Spanning Tree.
- Пояснити, як протокол Spanning Tree запобігає виникненню петель Рівня 2, забезпечуючи резервування у комутованих мережах.

Довідкова інформація / Сценарій

У цьому завданні ви використаєте Packet Tracer для спостереження за роботою протоколу Spanning Tree у простій комутованій мережі з надлишковими шляхами.

Інструкції

Частина 1: Спостереження за формуванням екземпляру єднального дерева

Крок 1: Перевірка з'єднання.

За допомогою команди ping перевірте з'єднання між вузлами PC1 і PC2. Результат перевірки повинен бути успішним.

Крок 2: Перегляд статусу єднального дерева на кожному комутаторі.

Використайте команду **show spanning-tree vlan 1**, щоб зібрати інформацію про стан єднального дерева на кожному комутаторі. Заповніть таблицю. У цьому завданні нам знадобиться інформація лише про гігабітні магістральні порти. Порти Fast Ethernet - це порти доступу, до яких приєднані кінцеві пристрої, і які не належать єднальному дереву на основі магістральних ліній між комутаторами.

Комутатор	Порт	Статус (FWD, BLK...)	Кореневий міст?
S1	G0/1		
	G0/2		
S2	G0/1		
	G0/2		
	G0/1		

S3	G0/2		

На схемі у Packet Tracer індикатор однієї з лінії зв'язку між комутаторами має інший колір.

Як ви думаєте, що означає цей колір індикатора?

Яким шляхом йтимуть кадри від PC1 до PC2?

Чому кадри не проходять через S3?

Чому єднальне дерево перевело цей порт у стан блокування?

Частина 2: Спостереження за збіжністю єднального дерева

Крок 1: Видалення з'єднання між S1 і S2.

a. Відкрийте вікно CLI на комутаторі S3 і запустіть на виконання команду **show spanning-tree vlan 1**. Залиште вікно CLI відкритим.

b. Виберіть інструмент видалення на панелі меню і натисніть на кабелі, що з'єднує S1 і S2.

Крок 2: Відстеження збіжності єднального дерева.

a. Одразу поверніться до режиму командного рядка CLI на комутаторі S3 і застосуйте команду **show spanning-tree vlan 1**.

b. За допомогою клавіші зі стрілкою вгору поверніться до попередньо застосованої команди **show spanning-tree vlan 1** і запустіть її повторно на виконання, допоки індикатор з'єднань не змінить колір із помаранчевого на зелений. Перевірте статус порту G0/2.

Як змінювався стан порту G0/2 під час цього процесу?

Ви простежили за зміною статусів порту, що як елемент єднального дерева, перейшов від стану блокування до переадресації.

c. За допомогою команди ping перевірте досяжність PC2 з PC1. Результат перевірки повинен бути успішним.

Чи є на схемі порти, підсвічені помаранчевим кольором, що було б ознакою того, що порт перебуває у стані spanning-tree, відмінному від переадресації? Поясніть наявність або відсутність таких портів.

Лабораторна робота №18
Налаштування EtherChannel

Мета

Частина 1. Налаштування основних параметрів комутатора

Частина 2: Налаштування EtherChannel за допомогою Cisco PAgP

Частина 3: Налаштування EtherChannel 802.3ad LACP

Частина 4: Налаштування резервного каналу EtherChannel

Довідкова інформація

Щойно встановлено три комутатори. Між комутаторами є надлишкові з'єднання. Відповідно до налаштувань, можна використовувати тільки одне з цих з'єднань, в іншому випадку може виникнути замкнута петля. Однак використання лише одного з'єднання використовує лише половину доступної пропускної здатності. EtherChannel дозволяє об'єднувати до восьми надлишкових з'єднань в одне логічне з'єднання. У цій лабораторній роботі ви налаштуєте протокол агрегації портів (PagP) - протокол Cisco EtherChannel, і протокол управління агрегацією каналів (LACP), який є відкритою стандартною версією EtherChannel IEEE 802.3ad.

Перед початком налаштування ознайомтеся з правилами налаштування EtherChannel і обмеженнями, переліченими в кінці цього завдання.

Таблиця каналів портів

Група каналів	Порти	Протокол
1	S1 F0/21. F0/22 S3 F0/21, F0/22	PagP
2	S1 G0/1, G0/2 S2 G0/1, G0/2	LACP
3	S2 F0/23, F0/24 S3 F0/23, F0/24	Узгоджений LACP

Інструкції

Частина 1: Налаштування основних параметрів комутатора

a. Призначити кожному комутатору назву відповідно до схеми топології.

b. Перед початком налаштування агрегованого каналу між комутаторами перевірте наявну конфігурацію портів, через які з’єднуються комутатори, щоб переконатися, що порти успішно приєднаються до EtherChannels. Команди, що надають інформацію про стан портів комутатора:

S1# **show interfaces | include Ethernet**

S1# **show interface status**

S1# **show interfaces trunk**

c. Налаштуйте всі порти, які необхідні для EtherChannels як статичні магістральні порти.

Примітка: Якщо порти налаштовані з динамічним автоматичним режимом DTP, і ви не встановлюєте режим портів в trunk, з'єднання не утворять магістральний канал і залишаться портами доступу. За замовчуванням на комутаторі 2960 протокол DTP увімкнений і налаштований як dynamic auto. DTP можна відключити на інтерфейсах за допомогою команди **switchport nonegotiate**.

Частина 2: Налаштування EtherChannel за допомогою Cisco PAgP

Примітка: Під час налаштування EtherChannel рекомендується вимкнути фізичні порти, які згруповані на обох пристроях, перш ніж налаштувати їх в групи каналів. В іншому випадку, EtherChannel Misconfig Guard може вимкнути ці порти. Після налаштування EtherChannel порти і агреговані канали можуть бути повторно ввімкнені.

Крок 1: Налаштуйте агрегований канал Port Channel 1.

a. Перший EtherChannel, створений в цьому завданні агрегує порти F0/21 і F0/22 між **S1** і **S3**. Налаштуйте порти на обох комутаторах як статичні магістральні порти.

b. Використовуйте команду **show interfaces trunk**, щоб переконатися, що у вас є активний магістральний канал для цих двох з'єднань, і native VLAN на обох з'єднаннях однакова.

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan
Fa0/21 on 802.1q trunking 1
Fa0/22 on 802.1q trunking 1
G0/1 on 802.1q trunking 1
G0/2 on 802.1q trunking 1

<output omitted>

c. На S1 і S3 додайте порти F0/21 і F0/22 до агрегованого каналу Port Channel 1 командою **channelgroup 1 mode desirable**. Параметр **mode**

desirable дозволяє комутатору активно узгоджувати формування каналу за протоколом PagP. **Примітка:** Інтерфейси повинні бути вимкнені **shutdown**, перш ніж додавати їх до групи каналів.

S1(config)# **interface range f0/21 – 22**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **channel-group 1 mode desirable**

S1(config-if-range)# **no shutdown**

S3(config)# **interface range f0/21 - 22**

S3(config-if-range)# **shutdown**

S3(config-if-range)# **channel-group 1 mode desirable**

S3(config-if-range)# **no shutdown**

Повідомлення «Створення інтерфейсу агрегованого каналу 1» (Creating a port-channel interface Port-channel 1) має з'явитися на обох комутаторах при налаштуванні групи каналів. Це позначення інтерфейсу буде показано як Po1 у виведенні команди.

d. Налаштуйте логічний інтерфейс як магістральний канал, спочатку ввівши команду **interface portchannel** *number*, а потім команду **switchport mode trunk**. Налаштуйте таким чином обидва комутатори.

S1(config)# **interface port-channel 1**

S1(config-if)# **switchport mode trunk**

S3(config)# **interface port-channel 1**

S3(config-if)# **switchport mode trunk**

Крок 2: Перевірте стан агрегованого каналу Port Channel 1.

a. Виконайте команду **show etherchannel summary** на S1 і S3, щоб переконатися, що EtherChannel працює на обох комутаторах. Ця команда відображає тип EtherChannel, порти, які використовуються і їх стан. Виведення команди показано для S1.

S1# **show etherchannel summary**

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling w - waiting to be aggregated d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------
1 Po1 (SU) PagP F0/21 (P) F0/22 (P)

b. Якщо EtherChannel не увімкнувся, вимкніть фізичні інтерфейси на обох кінцях EtherChannel і потім знову увімкніть їх. Команди **show interfaces trunk** і **show spanning-tree** повинні показати агрегований канал як одне логічне з'єднання.

Частина 3: Налаштування EtherChannel 802.3ad LACP

Крок 1: Налаштуйте агрегований канал Port Channel 2.

а. У 2000 році IEEE випустила 802.3ad, який є відкритою версією стандарту EtherChannel. Його зазвичай називають LACP. Використовуючи попередні команди, налаштуйте зв'язок між **S1** і **S2**, використовуючи порти G0/1 і G0/2, як EtherChannel для протоколу LACP. Ви повинні використовувати інший номер агрегованого каналу на **S1**, ніж 1, тому що ви вже використовували це на попередньому кроці. Щоб налаштувати агрегований канал 2 як LACP, використовується команда режиму конфігурації інтерфейсу **channel-group** *2* **mode active**. Активний режим (active) вказує на те, що комутатор активно намагається узгодити це з'єднання як LACP, на відміну від PagP. Конфігурація для комутатора S1 показана нижче.

S1(config)# **interface range g0/1 - 2**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **channel-group 2 mode active**
S1(config-if-range)# **no shutdown**
S1(config-if-range)# **interface port-channel 2**
S1(config-if)# **switchport mode trunk**

Крок 2: Перевірте стан агрегованого каналу Port Channel 2.

Використовуйте команди **show** з частини 1 крок 2, щоб перевірити стан Port Channel 2. Визначте протокол, який використовується для кожного порту.

Частина 4: Налаштування резервного каналу EtherChannel

Крок 1: Налаштуйте агрегований канал Port Channel 3.

Існують різні параметри команди **channel-group** *number* **mode**:

S2(config)# **interface range f0/23 - 24** S2(config-if-range)# **channel-group 3 mode ?**

active Enable LACP unconditionally auto
Enable PAgP only if a PAgP device is detected
desirable Enable PAgP unconditionally on
Enable Etherchannel only
passive Enable LACP only if a LACP device is detected

a. На комутаторі **S2** додайте порти F0/23 і F0/24 до агрегованого каналу Port Channel 3 за допомогою команди **channel-group 3 mode passive**. Параметр **passive** вказує на те, що комутатор повинен використовувати LACP, лише якщо виявлено інший пристрій LACP. Статично налаштуйте Port Channel 3 як магістральний інтерфейс.

S2(config)# **interface range f0/23 - 24**
S2(config-if-range)# **shutdown**
S2(config-if-range)# **channel-group 3 mode passive**
S2(config-if-range)# **no shutdown**
S2(config-if-range)# **interface port-channel 3**
S2(config-if)# **switchport mode trunk**

b. На **S3** додайте порти F0/23 і F0/24 до Port Channel 3 командою **channel-group 3 mode active**. Параметр **active** вказує на те, щоб комутатор використовував LACP безумовно. Статично налаштуйте Port Channel 3 як магістральний інтерфейс.

Крок 2: Перевірте стан агрегованого каналу Port Channel 3.

a. Використовуйте команди **show** з частини 1 крок 2, щоб перевірити стан Port Channel 3. Визначте протокол, який використовується для кожного порту.

b. Створення каналів EtherChannel не перешкоджає виявленню петель комутації протоколом єднального дерева STP. Перегляд стану активних портів єднального дерева на **S1**.

S1# **show spanning-tree active**
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0001.436E.8494
Cost 9

Port 27(Port-channel1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000A.F313.2395
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Po1 Root FWD 9 128.27 Shr
Po2 Altn BLK 3 128.28 Shr

Канал Port Channel 2 не працює, оскільки протокол STP помістив деякі порти в режим блокування. На жаль, ці порти були гігабітними портами. У цій топології ви можете відновити ці порти, налаштувавши **S1** в якості **основного** кореня для VLAN 1. Ви також можете встановити пріоритет **24576**.
S1(config)# **spanning-tree vlan 1 root primary**

або

S1(config)# **spanning-tree vlan 1 priority 24576**

Можливо, доведеться чекати, щоб STP перерахував топологію дерева. При необхідності натисніть клавішу «fast-forward». Використайте команду **show spanning-tree active**, щоб переконатися, що гігабітні порти тепер у стані пересилання.

Рекомендації та обмеження що до налаштування EtherChannel

EtherChannel має деякі конкретні рекомендації, які необхідно дотримуватися, щоб уникнути проблем з конфігурацією.

1) Всі інтерфейси Ethernet підтримують максимум до восьми інтерфейсів для EtherChannel без вимоги, щоб інтерфейси були на одному інтерфейсному модулі.
2) Всі інтерфейси в межах EtherChannel повинні працювати з однаковою швидкістю і дуплексним режимом.
3) Інтерфейси каналів EtherChannel можуть функціонувати як окремі порти доступу VLAN, так і як магістральні канали між комутаторами.
4) Всі інтерфейси рівня 2 в каналі EtherChannel повинні належати одній VLAN або бути налаштовані як магістральні канали.

5) Якщо вони налаштовані як магістральні канали, EtherChannel рівня 2 повинен мати однакову native VLAN і мати однакові дозволені VLAN на обох комутаторах, підключених до магістралі.

6) Під час налаштування з'єднань EtherChannel всі інтерфейси повинні бути вимкнені до початку налаштування EtherChannel. Після завершення налаштування з'єднання можуть бути повторно увімкнені.

7) Після налаштування EtherChannel перевірте, чи всі інтерфейси знаходяться у ввімкненому стані.

8) Можна налаштувати EtherChannel як статичний канал, або використовувати PagP чи LACP для узгодження з'єднання EtherChannel. Спосіб налаштування EtherChannel визначає аргумент команди **channel-group** *number* **mode**. Допустимі значення:

active LACP увімкнений безумовно
passive LACP вмикається, лише якщо підключено інший пристрій із підтримкою LACP.
desirable PagP включений безумовно
auto PagP увімкнено, лише якщо підключено інший пристрій, який підтримує Pagp.
on EtherChannel увімкнено, але без LACP або PagP.

9) Порти LAN можуть утворювати EtherChannel за допомогою PagP, якщо режими сумісні. Сумісними режимами PagP є:

desirable => desirable
desirable => авто
Якщо обидва інтерфейси знаходяться в режимі **auto**, Etherchannel не може утворитися.

10) LAN порти можуть утворювати EtherChannel за допомогою LACP, якщо режими сумісні. Сумісними режимами LACP є:

active => ctive
active => assive
Якщо обидва інтерфейси знаходяться в режимі **passive**, Etherchannel не може утворитися.

11) Номери агрегованого каналу локальні для окремого комутатора. Хоча в цьому завданні показано використання одного і того ж номеру групи каналів на будь-якому кінці підключення EtherChannel, це не є вимогою. Агрегований канал Channel-group 1 (інтерфейс po1) на одному комутаторі може утворювати EtherChannel з Channel-group 5 (інтерфейс po5) на іншому комутаторі.

Лабораторна робота №19.1
Налаштування статичного NAT

Цілі та задачі
Частина 1: Перевірка доступу без використання NAT

Частина 2: Налаштування статичного NAT

Частина 3: Перевірка доступу з використанням NAT

Сценарій

У налаштованих мережах IPv4 клієнти і сервери використовують приватну адресацію. Перед виходом з мережі в Інтернет пакети з приватною адресацією повинні бути трансльовані в пакети з публічною адресацією. Серверам, доступ до яких здійснюється за межами організації, зазвичай призначають як публічну, так і приватну статичну IP-адресу. У цьому завданні ви будете налаштовувати статичний NAT, щоб зовнішні пристрої могли отримати доступ до внутрішнього сервера за його публічною адресою.

Інструкції

Частина 1. Перевірка доступу без використання NAT

Крок 1. Спроба під'єднання до серверу Server1 за допомогою режиму моделювання.

a. Перейдіть до режиму Simulation.

b. З **PC1** або **L1** за допомогою браузера спробуйте під'єднатися до веб-сторінки **Server1** за адресою 172.16.16.1. Продовжуйте натискати кнопку **Capture Forward**, зверніть увагу, що пакети так і не вийдуть за межі інтернет-хмари. Спроби будуть невдалими.

c. Вийдіть з режиму **Simulation**.

d. З **PC1** пропінгуйте інтерфейс S0/0/0 **R1** (209.165.201.2). Перевірка зв'язку за допомогою команди ping повинна бути вдалою.

Крок 2. Перегляд таблиці маршрутизації R1 і початкової конфігурації.

a. Перегляньте конфігурацію запуску маршрутизатора **R1**. Зверніть увагу на відсутність команд, що стосуються NAT. Простий спосіб це підтвердити – виконати таку команду:

R1# show run | include nat

b. Переконайтеся, що таблиця маршрутизації не містить записів, що відповідають IP-адресам мережі для **PC1** і **L1**.

c. Переконайтеся, що NAT не використовується маршрутизатором **R1**.

R1# **show ip nat translations**

Частина 2. Налаштування статичного NAT

Крок 1. Налаштування за допомогою команд для статичного NAT.

Зверніться до топології. Створіть трансляцію статичного NAT для зіставлення внутрішньої адреси **Server1** з його зовнішньою адресою.

R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1

Крок 2. Налаштування інтерфейсів.

a. Налаштуйте інтерфейс **G0/0** як внутрішній інтерфейс.

R1(config)# interface g0/0
R1(config-if)# **ip nat inside**

b. Налаштуйте публічний інтерфейс s0/0/0 як зовнішній інтерфейс.

Частина 3. Перевірка доступу з використанням NAT

Крок 1. Перевірка з'єднання з веб-сторінкою Server1.

a. Відкрийте командний рядок на **PC1** або **L1**, спробуйте пропінгувати публічну адресу для **Server1**. Перевірка зв'язку за допомогою команди ping повинна бути вдалою.

b. Переконайтеся, що як **PC1**, так і **L1** тепер можуть отримати доступ до веб-сторінки **Server1**.

Крок 2. Перегляд трансляцій NAT.

Для перевірки конфігурації статичного NAT на **R1** скористайтеся наведеними нижче командами:

show running-config
show ip nat translations
show ip nat statistics

Лабораторна робота №19.2
Налаштування PAT

Цілі та задачі
Частина 1: Налаштування динамічного NAT з перевантаженням
Частина 2: Перевірка динамічного NAT з реалізацією перевантаження
Частина 3: Налаштування PAT за допомогою інтерфейсу
Частина 4: Перевірка реалізації інтерфейсу PAT

Частина 1. Налаштування динамічного NAT з перевантаженням

Крок 1. Налаштуйте дозволений трафік.

На маршрутизаторі **R1** налаштуйте одне правило для ACL 1, що дозволяє будь-яку адресу, яка належить 172.16.0.0/16.

R1(config)# **access-list 1 permit 172.16.0.0 0.0.255.255**

Крок 2. Налаштуйте пул адрес для NAT.

Налаштуйте на **R1** пулом NAT, який використовує дві доступні адреси в адресному просторі 209.165.200.232/30.

R1(config)# **ip nat pool ANY_POOL_NAME 209.165.200.233 209.165.200.234 netmask 255.255.255.252**

Крок 3. Пов'яжіть ACL 1 із пулом NAT і дозвольте повторне використання адрес.

R1(config)# **ip nat inside source list 1 pool ANY_POOL_NAME overload**

Крок 4. Налаштуйте інтерфейси NAT.

Налаштуйте на інтерфейсах маршрутизатора **R1** відповідні команди для впровадження внутрішніх та зовнішніх NAT-перетворень.

R1(config)# **interface s0/1/0**
R1(config-if)# **ip nat outside**
R1(config-if)# **interface g0/0/0 R1**
R1(config-if)# **ip nat inside**
R1(config-if)# **interface g0/0/1**
R1(config-if)# **ip nat inside**

Частина 2. Перевірка динамічного NAT з реалізацією перевантаження

Крок 1. Зверніться до сервісів через Інтернет.

Із веб-браузера кожного ПК, які використовують **R1** як шлюз (**PC1**, **L1**, **PC2** і **L2**), перейдіть на веб-сторінку **Server1**.

Чи всі з’єднання були вдалими?

Крок 2. Перегляньте трансляції NAT.

Перегляньте трансляції NAT на **R1**.

R1# **show ip nat translations**

Зверніть увагу, що всі чотири пристрої змогли обмінюватися даними, і вони використовують лише одну адресу з пулу. PAT продовжуватиме використовувати ту саму адресу, доки не закінчаться номери портів, пов'язані з трансляцією. Після цього буде використовуватися наступна адреса в пулі. Хоча теоретичним обмеженням буде 65536, оскільки поле номера порту є 16-бітовим числом, на пристрої, ймовірно, закінчиться пам’ять до досягнення цього обмеження.

Частина 3. Налаштування PAT за допомогою інтерфейсу

Крок 1. Налаштуйте дозволений трафік.

На маршрутизаторі **R2** налаштуйте одне правило для ACL 2, що дозволяє будь-яку адресу, яка належить 172.17.0.0/16.

Крок 2. Пов’яжіть ACL 2 з інтерфейсом NAT і дозвольте повторне використання адрес.

Введіть на **R2** команду, яка б для реалізації NAT запровадила використання під'єднаного до Інтернету інтерфейсу та забезпечувала трансляції для всіх внутрішніх пристроїв.

R2(config)# **ip nat inside source list 2 interface s0/1/1 overload**

Крок 3. Налаштуйте інтерфейси NAT.

Налаштуйте інтерфейси маршрутизатора **R2** за допомогою відповідних внутрішніх та зовнішніх команд NAT.

Частина 4. Перевірка реалізації інтерфейсу PAT

Крок 1. Зверніться до сервісів через Інтернет.

Із веб-браузера кожного ПК, які використовують **R2** як свій шлюз (**PC3**, **L3**, **PC4** і **L4**), перейдіть на веб-сторінку **Server1**.

Чи всі звернення були вдалими?

Крок 2. Перегляньте трансляції NAT.

Перегляньте трансляції NAT на маршрутизаторі **R2**.

Крок 3. Порівняйте статистичні дані NAT на R1 і R2.

Порівняйте статистику NAT на двох пристроях.

Чому **R2** не містить жодного динамічного зіставлення?

Лабораторна робота №19.3
Налаштування DHCPv4

Таблиця адресації

Пристрій	Інтерфейс	Адреса IPv4	Маска підмережі	Шлюз за замовчуванням
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	Призначається DHCP	Призначається DHCP	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.0	N/A
PC1	NIC	Призначається DHCP	Призначається DHCP	Призначається DHCP
PC2	NIC	Призначається DHCP	Призначається DHCP	Призначається DHCP
DNS Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Цілі та задачі
Частина 1: Налаштування маршрутизатора як сервера DHCP
Частина 2: Налаштування ретрансляції DHCP
Частина 3: Налаштування маршрутизатора як клієнта DHCP
Частина 4: Перевірка DHCP та з'єднання

Сценарій

Виділений DHCP-сервер добре масштабується і відносно легкий у керуванні, але використання подібного сервера в кожній точці мережі може виявитися занадто витратним. Однак маршрутизатор Cisco можна налаштувати для забезпечення служб DHCP без необхідності виділеного сервера. Як мережний фахівець компанії ви отримали завдання налаштувати маршрутизатор Cisco для виконання функцій сервера DHCP. Також необхідно налаштувати граничний маршрутизатор як клієнта DHCP, щоб він міг отримати IP-адресу від мережі інтернет-провайдера.

Інструкції

Частина 1: Налаштування маршрутизатора як сервера DHCP

Крок 1: Налаштуйте виключення IPv4-адрес.

Адреси, які статично призначені пристроям у мережах і використовуватимуть DHCP, повинні бути виключені з пулів DHCP. Такий підхід дозволяє уникнути помилок, пов'язаних з дублюванням IP-адрес. При цьому IP-адреси LAN-інтерфейсів маршрутизаторів R1 і R3 повинні бути виключені з пулу DHCP. Окрім того, слід виключити дев'ять інших адрес для статичного призначення іншим пристроям, таким як сервери та інтерфейси керування пристроями.

a. Налаштуйте **R2**, щоб виключити перші 10 адрес з локальної мережі маршрутизатора R1.
   R2(config)# **ip dhcp excluded-address 192.168.10.1 192.168.10.10**

b. Налаштуйте **R2**, щоб виключити перші 10 адрес з локальної мережі маршрутизатора R3.

Крок 2: На R2 створіть пул DHCP для локальної мережі маршрутизатора R1.

a. Створіть пул DHCP під назвою **R1-LAN** (з урахуванням регістру).
   R2(config)# **ip dhcp pool R1-LAN**

b. Налаштуйте пул DHCP, який міститиме адресу мережі, шлюз за замовчуванням та IP-адресу DNScервера.
   R2(dhcp-config)# **network 192.168.10.0 255.255.255.0**
   R2(dhcp-config)# default-router 192.168.10.1
   R2(dhcp-config)# dns-server 192.168.20.254

Крок 3: На маршрутизаторі R2 створіть пул DHCP для локальної мережі маршрутизатора R3.

a. Створіть пул DHCP під назвою **R3-LAN** (з урахуванням регістру).

b. Налаштуйте пул DHCP, який міститиме адресу мережі, шлюз за замовчуванням та IP-адресу DNScервера. Зверніться до таблиці адресації.

Частина 2: Налаштування ретрансляції DHCP

Крок 1: Налаштуйте маршрутизатори R1 і R3 як агенти ретрансляції DHCP.

Щоб клієнти DHCP отримували адресу з сервера в іншому сегменті локальної мережі, інтерфейс, до якого під'єднані клієнти, повинен включати допоміжну адресу, що вказує на сервер DHCP. У цьому випадку вузли локальних мереж, під'єднаних до R1 та R3, отримають доступ до сервера DHCP, налаштованому на R2. Як допоміжні адреси використовуються IP-адреси послідовних інтерфейсів R2, які під'єднані до R1 та R3. Трафік DHCP від вузлів локальних мереж маршрутизаторів R1 і R3 перенаправлятиметься за цими адресами та оброблятиметься сервером DHCP, налаштованим на R2. a. Налаштуйте допоміжну адресу для інтерфейсу LAN на R1.

R1(config)# **interface g0/0**
R1(config-if)# **ip helper-address 10.1.1.2**

b. Налаштуйте допоміжну адресу для інтерфейсу LAN на R3.

Крок 2: Налаштуйте вузли для отримання інформації про IP-адресацію за допомогою DHCP.

a. Налаштуйте вузли PC1 і PC2, щоб отримувати IP-адреси через сервер DHCP.
b. Перевірте, чи отримали вузли адреси з правильних пулів DHCP.

Частина 3: Налаштування маршрутизатора як клієнта DHCP

Подібно до того, як PC здатний отримувати IPv4-адресу з сервера, інтерфейс маршрутизатора також має можливість зробити те ж саме. Потрібно налаштувати маршрутизатор **R2** для отримання адресації від інтернет-провайдера.

a. Налаштуйте інтерфейс Gigabit Ethernet 0/1 на маршрутизаторі **R2** для отримання інформації про IPадресацію за допомогою DHCP і активуйте інтерфейс.

R2(config)# **interface g0/1**
R2(config-if)# **ip address dhcp**
R2(config-if)# **no shutdown**

Примітка: Використовуйте функцію **Fast Forward Time** в Packet Tracer, щоб прискорити процес.

b. Використайте команду **show ip interface brief**, щоб перевірити, чи R2 отримав IP-адресу через DHCP.

Частина 4: Перевірка DHCP та з'єднання

Крок 1: Перевірте прив'язки DHCP.

R2# **show ip dhcp binding**

IP address Client-ID/ Lease expiration Type

Hardware address

192.168.10.11 0002.4AA5.1470 -- Automatic

192.168.30.11 0004.9A97.2535 -- Automatic

Крок 2: Перевірте налаштування.

Переконайтеся, що **PC1** і **PC2** тепер можуть відправляти запити ping один одному та іншим пристроям.

Лабораторна робота №20

Налаштування статичних маршрутів та маршрутів за замовчуванням IPv4 і IPv6

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс
Edge_Router	S0/0/0	10.10.10.2/30
		2001:db8:a:1::2/64
	S0/0/1	10.10.10.6/30
		2001:db8:a:2::2/64
	G0/0	192.168.10.17/28
		2001:db8:1:10::1/64
	G0/1	192.168.11.33/27
		2001:db8:1:11::1/64
ISP1	S0/0/0	10.10.10.1/30
		2001:db8:a:1::1/64
	G0/0	198.0.0.1/24
		2001:db8:f:f::1/64
ISP2	S0/0/1	10.10.10.5/30
		2001:db8:a:2::1/64
	G0/0	198.0.0.2/24
		2001:db8:f:f::2/64
PC-A	NIC	192.168.10.19/28
		2001:db8:1:10::19/64
PC-B	NIC	192.168.11.4/27
		2001:db8:1:11::45
Customer Server	NIC	198.0.0.10
		2001:db8:f:f::10

Цілі та задачі

У цьому підсумковому завданні у Packet Tracer ви будете налаштовувати статичні маршрути, маршрути за замовчуванням та змінні статичні маршрути для протоколів IPv4 і IPv6.

- Налаштування статичних та змінних статичних маршрутів за замовчуванням IPv4.
- Налаштування статичних та змінних статичних маршрутів за замовчуванням IPv6.
- Налаштування статичних та змінних статичних маршрутів IPv4 до внутрішньої LAN.
- Налаштування статичних та змінних статичних маршрутів IPv6 до внутрішньої LAN.
- Налаштування статичних маршрутів вузла IPv4.
- Налаштування статичних маршрутів вузла IPv6.

Довідкова інформація / Сценарій

У цьому завданні ви налаштуєте статичні та змінні статичні маршрути за замовчуванням IPv4 і IPv6.

Примітка: Статична маршрутизації, що розглядається в цій лабораторній роботі, використовується виключно для оцінювання вашої здатності налаштовувати різні типи статичних маршрутів. Такий підхід може не відповідати найкращим практикам.

Інструкції

Частина 1: Налаштування статичних і змінних статичних маршрутів за замовчуванням IPv4

Для забезпечення доступу до інтернету користувачів внутрішніх LAN через інтернет-провайдерів мережа PT потребує впровадження статичних маршрутів. Більше того, маршрутизаторам провайдерів (ISP) необхідні статичні маршрути, щоб дістатися до внутрішніх LAN. У цій частині завдання ви налаштуєте статичний маршрут за замовчуванням і змінний маршрут за замовчуванням IPv4 для забезпечення резервних шляхів у мережі.

Крок 1: Налаштування статичного маршруту за замовчуванням IPv4.

На маршрутизаторі Edge_Router налаштуйте **безпосередньо під'єднаний** статичний маршрут за замовчуванням IPv4. Цей основний маршрут за замовчуванням повинен проходити через маршрутизатор **ISP1**.

Крок 2: Налаштування змінного статичного маршруту за замовчуванням IPv4.

На маршрутизаторі Edge_Router налаштуйте **безпосередньо під'єднаний** змінний статичний маршрут за замовчуванням IPv4. Цей маршрут за

замовчуванням повинен проходити через маршрутизатор **ISP2**. Він повинен мати адміністративну відстань **5**.

Частина 2: Налаштування статичних і змінних статичних маршрутів за замовчуванням IPv6

У цій частині завдання ви будете налаштовувати статичні маршрути за замовчуванням IPv6 і змінні статичні маршрути за замовчуванням для IPv6.

Крок 1: Налаштування статичного маршруту за замовчуванням IPv6.

На маршрутизаторі Edge_Router налаштуйте статичний маршрут за замовчуванням **наступного переходу** . Цей основний маршрут за замовчуванням повинен проходити через маршрутизатор **ISP1**.

Крок 2: Налаштування змінного статичного маршруту за замовчуванням IPv6.

На маршрутизаторі Edge_Router налаштуйте змінний статичний маршрут за замовчуванням **наступного переходу** IPv6. Маршрут повинен проходити через маршрутизатор **ISP2**. Використовуйте адміністративну відстань **5**.

Частина 3: Налаштування статичних і змінних статичних маршрутів IPv4 до внутрішніх LAN

У цій частині лабораторної роботи ви налаштуєте статичні та змінні статичні маршрути від маршрутизаторів ISP (інтернет-провайдера) до внутрішніх LAN.

Крок 1: Налаштування статичних маршрутів IPv4 до внутрішніх LAN.

a. На маршрутизаторі ISP1 налаштуйте статичний маршрут **наступного переходу** IPv4 до мережі **LAN 1** через маршрутизатор Edge_Router.

b. На маршрутизаторі ISP1 налаштуйте статичний маршрут **наступного переходу** IPv4 до мережі **LAN 2** через маршрутизатор Edge_Router.

Крок 2: Налаштування змінних статичних маршрутів IPv4 до внутрішніх LAN.

a. На маршрутизаторі ISP1 налаштуйте безпосередньо під'єднаний змінний статичний маршрут до LAN 1 через маршрутизатор ISP2. Використовуйте адміністративну відстань **5**.

b. На маршрутизаторі ISP1 налаштуйте безпосередньо під'єднаний змінний статичний маршрут до LAN 2 через маршрутизатор ISP2. Використовуйте адміністративну відстань **5**.

Частина 4: Налаштування статичних та змінних статичних маршрутів IPv6 до внутрішніх LAN

Крок 1: Налаштування статичних маршрутів IPv6 до внутрішніх LAN.

a. На маршрутизаторі ISP1 налаштуйте статичний маршрут наступного переходу IPv6 до мережі LAN 1 через маршрутизатор Edge_Router.

b. На маршрутизаторі ISP1 налаштуйте статичний маршрут наступного переходу IPv6 до мережі LAN 2

через маршрутизатор Edge_Router.

Крок 2: Налаштування змінних статичних маршрутів IPv6 до внутрішніх LAN.

a. На маршрутизаторі ISP1 налаштуйте змінний статичний маршрут наступного переходу IPv6 до мережі LAN 1 через маршрутизатор ISP2. Використовуйте адміністративну відстань **5**.

b. На маршрутизаторі ISP1 налаштуйте змінний статичний маршрут наступного переходу IPv6 до мережі LAN 2 через маршрутизатор ISP2. Використовуйте адміністративну відстань **5**.

Якщо ви правильно виконали налаштування, вам вдасться пропінгувати веб-сервер з вузлів LAN 1 та LAN 2. Більше того, зв’язок між вузлами LAN і веб-сервером існуватиме навіть у разі відмови каналу, по якому прокладено основний маршрут.

Частина 5: Налаштування маршрутів вузла

Користувачі корпоративної мережі часто звертаються до сервера, який належить важливому клієнту. У цій частині завдання ви налаштуєте статичні маршрути вузла до сервера. Один маршрут буде змінним статичним маршрутом для підтримки резервних з'єднань провайдера (ISP).

Крок 1: Налаштування маршрутів вузла IPv4.

a. На маршрутизаторі Edge_Router налаштуйте **безпосередньо під'єднаний** маршрут вузла IPv4 до сервера користувача – Customer Server.

b. На маршрутизаторі Edge_Router налаштуйте безпосередньо під'єднаний змінний маршрут вузла IPv4 до Customer Server. Використовуйте адміністративну відстань **5**.

Крок 2: Налаштування маршрутів вузла IPv6.

a. На маршрутизаторі Edge_Router налаштуйте маршрут вузла наступного переходу IPv6 до Customer Server через маршрутизатор ISP1.

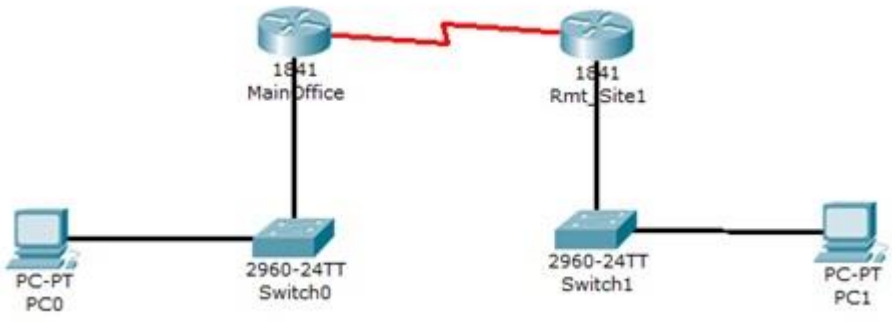
b. На маршрутизаторі Edge_Router налаштуйте безпосередньо під'єднаний змінний маршрут вузла IPv6 до Customer Server через маршрутизатор ISP2. Використовуйте адміністративну відстань **5**.

Лабораторна робота №21.1

Налаштування динамічної маршрутизації на базі протоколу RIP

Мета роботи: Ознайомитись з налаштуванням динамічної маршрутизації на базі протоколу RIP

Вихідні дані.
Невелика компанія розширила свій офіс за рахунок додаткового приміщення в іншій будівлі. Ви повинні налаштувати маршрутизатори таким чином, щоб забезпечити трафік між двома мережами.



Топологія мережі

Крок 1: Налаштування імен вузлів

Задайте ім’я вузла для маршрутизатора головного офісу **MainOffice**

1. Виберіть маршрутизатор головного офісу **MainOffice**.
2. Увійдіть в режим глобальної конфігурації та введіть наступні команди:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MainOffice
MainOffice#copy running-config startup-config
```

Задайте ім’я вузла для маршрутизатора віддаленого відділу **Rmt_Site1**.

1. Виберіть маршрутизатор головного офісу **Rmt_Site1**.
2. Увійдіть в режим глобальної конфігурації та введіть наступні команди:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#hostname Rmt_Site1
Rmt_Site1#copy running-config startup-config
```

Крок 2: Налаштування паролів привілейованого режиму, консолі і віртуального терміналу

Виберіть маршрутизатор головного офісу **MainOffice**.

1. Увійдіть в глобальний режим конфігурації.
2. Задайте пароль з шифруванням привілейованого режиму, пароль консолі та пароль telnet, використовуючи наступні команди:

```
MainOffice#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MainOffice(config)#enable secret cisco123
MainOffice(config)#line console 0
MainOffice(config-line)#password class
MainOffice(config-line)#login
MainOffice(config-line)#exit
MainOffice(config)#line vty 0 4
MainOffice(config-line)#password class
MainOffice(config-line)#login
MainOffice(config-line)# Use the key sequence cntl + z here
%SYS-5-CONFIG_I: Configured from console by console
MainOffice#copy running-config startup-config
```

Виберіть маршрутизатор віддаленого відділу **Rmt_Site1**.

1. Увійдіть в глобальний режим конфігурації.
2. Задайте пароль з шифруванням привілейованого режиму, пароль консолі та пароль telnet, використовуючи аналогічні команди, що використовувались при налаштуванні маршрутизатора **MainOffice.** Збережіть поточну конфігурацію в **startup-config.**

Крок 3: Налаштування інтерфейсів маршрутизатора

Налаштуйте послідовний інтерфейс маршрутизатора головного офісу MainOffice.

1. Виберіть маршрутизатор головного офісу MainOffice.
2. Перейдіть в режим конфігурування та введіть наступні команди:

```
MainOffice#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MainOffice(config)#interface serial0/1/0
```

```
MainOffice(config-if)#ip address 192.168.1.1 255.255.255.252
MainOffice(config-if)#clock rate 64000
MainOffice(config-if)#no shutdown
MainOffice(config-if)#exit
```

Налаштуйте інтерфейс FastEthernet маршрутизатора головного офісу MainOffice.

3. Перейдіть в режим конфігурування та введіть наступні команди:

```
MainOffice(config)#interface fastethernet0/0
MainOffice(config-if)#ip address 192.168.2.1 255.255.255.0
MainOffice(config-if)#no shutdown
MainOffice(config-if)# Use the key sequence cntl + z here
%SYS-5-CONFIG_I: Configured from console by console
MainOffice#copy running-config startup-config
```

Аналогічно налаштуйте Serial0/1/0 та FastEthernet0/0 інтерфейси маршрутизатора **Rmt_Site1**. Слід пам’ятати, що для інтерфейсу Serial0/1/0 маршрутизатора **Rmt_Site1** команду **clock rate** вводити не потрібно.
Збережіть поточну конфігурацію в **startup-config.**

Крок 4: Налаштування протоколу маршрутизації RIP

Налаштуйте протокол RIP версії 2 на маршрутизаторі головного офісу MainOffice.

1. Виберіть маршрутизатор головного офісу **MainOffice**.
2. Перейдіть в режим конфігурування та введіть наступні команди:Увійдіть в режим глобальної конфігурації.

```
MainOffice#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MainOffice(config)#router rip
MainOffice(config-router)#version 2
MainOffice(config-router)#network 192.168.1.0
MainOffice(config-router)#network 192.168.2.0
MainOffice(config-router)# Use the key sequence cntl + z here
%SYS-5-CONFIG_I: Configured from console by console
MainOffice#copy running-config startup-config
```

Аналогічно налаштуйте протокол RIP версії 2 для маршрутизатора віддаленого відділу Rmt_Site1.
Збережіть поточну конфігурацію в **startup-config.**

Крок 5: Перевірка конфігурацій і підключення

1. Перегляньте поточну конфігурацію маршрутизатора головного офісу MainOffice за допомогою команди **show running-config**.
2. Запишіть ім’я вузла, паролі, IP-адресу і конфігурації протоколу маршрутизації.
3. Перегляньте поточну конфігурацію маршрутизатора віддаленого відділу Rmt_Site1 за допомогою команди **show running-config**.
4. Запишіть ім’я вузла, паролі, IP-адресу і конфигурації протоколу маршрутизації.
5. Відправте echo-запит на PC1 із командного рядка PC0:

   PC>ping 192.168.3.3

6. Прослідкуйте мережевий шлях від PC0 до PC1 за допомогою командного рядка PC0:

   PC>tracert 192.168.3.3

7. Виберіть **Check Results.**

Запитання для повторення

1. Які команди використовуються для переходу в режим конфігурації інтерфейсу FastEthernet 0/0 при запуску через запрошення користувацького режиму EXEC?
2. Який інтерфейс необхідно налаштувати командою clock rate? (DCE чи DTE)?
3. Чому команду clock rate не потрібно вводити при конфігуруванні інтерфейсу Serial0/1/0 маршрутизатора **Rmt_Site1**?
4. Які суттєві відмінності між протоколами RIP версії 1 та 2?
5. Які переваги динамічної маршрутизації в порівнянні зі статичною?

Лабораторна робота №21.2

Налаштування OSPFv2 для однієї зони

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
R1	G0/0/0	192.168.10.1	/24
	S0/1/0	10.1.1.1	/30
	S0/1/1	10.1.1.5	/30
R2	G0/0/0	192.168.20.1	/24
	S0/1/0	10.1.1.2	/30
	S0/1/1	10.1.1.9	/30
R3	G0/0/0	192.168.30.1	/24
	S0/1/0	10.1.1.10	/30
	S0/1/1	10.1.1.6	/30
PC1	NIC	192.168.10.10	/24
PC2	NIC	192.168.20.10	/24
PC3	NIC	192.168.30.10	/24

Цілі та задачі

Частина 1: Налаштування ідентифікаторів маршрутизатора

Частина 2: Налаштування мереж для маршрутизації OSPF

Частина 3: Налаштування пасивних інтерфейсів

Частина 4: Перевірка налаштувань OSPF

Довідкова інформація

У цьому завданні ви активуєте маршрутизацію OSPF за допомогою команди network і шаблонних масок, шляхом налаштування маршрутизації OSPF на інтерфейсах і використання команди network з масками з чотирма нулями. Крім того, вам потрібно налаштувати явно ідентифікатори маршрутизаторів і пасивні інтерфейси.

Інструкції

Частина 1. Налаштування ідентифікаторів маршрутизатора

a. Запустіть процес маршрутизації OSPF на всіх трьох маршрутизаторах. Використовуйте ID процесу **10**.
   Router(config)# **router ospf** *process-id*

b. Скористайтесь командою router-id, щоб встановити ID OSPF на трьох маршрутизаторах:
   - R1: **1.1.1.1**
   - R2: **2.2.2.2**
   - R3: **3.3.3.3**

   Використовуйте команду:
   Router(config-router)# **router-id** *rid*

Частина 2. Налаштування мереж для маршрутизації OSPF

Крок 1. Налаштуйте мережі для маршрутизації OSPF за допомогою команди network і шаблонних масок.

Скільки команд потрібно виконати для налаштування OSPF-маршрутизації у всіх мережах, приєднаних до маршрутизатора R1?

Локальна мережа, під'єднана до маршрутизатора R1, має маску /24. Який еквівалент цієї маски в крапково-десятковому форматі?

Відніміть крапково-десяткову маску підмережі від 255.255.255.255. Який Ви отримали результат?

Який крапково-десятковий еквівалент маски підмережі /30?

Відніміть крапково-десяткову маску /30 від 255.255.255.255. Який Ви отримали результат?

a. Налаштуйте процес маршрутизації на R1 за допомогою команди network та шаблонних масок, які потрібні для активації OSPF-маршрутизації у всіх приєднаних мережах. Параметрами команди network повинні бути адреси налаштованих мереж або підмереж.

Router(config-router)# **network** network-address wildcard-mask **area** area-id

b. Використовуючи відображення поточної конфігурації, переконайтеся, що OSPF налаштовано належним чином. У разі виявлення помилки видаліть команду network, використавши **no** перед командою, і переналаштуйте її.

Крок 2. Налаштуйте мережі для маршрутизації OSPF за допомогою IP-адрес інтерфейсів і масок з чотирма нулями.

На маршрутизаторі R2 налаштуйте OSPF, використовуючи команди network з IP-адресами інтерфейсів і масками з чотирма нулями. Синтаксис команди network такий же, як використовувався раніше.

Крок 3. Налаштуйте маршрутизацію OSPF на інтерфейсах маршрутизатора

На маршрутизаторі R3 налаштуйте OSPF на інтерфейсах, де це необхідно.

На яких інтерфейсах маршрутизатора R3 слід налаштувати протокол OSPF?

Налаштуйте кожен інтерфейс, використовуючи наступний синтаксис команди:

Router(config-if)# **ip ospf** *process-id* **area** *area-id*

Частина 3. Налаштування пасивних інтерфейсів

OSPF буде надсилати трафік протоколу з усіх інтерфейсів, що беруть участь в процесі OSPF. На каналах, які не налаштовані для інших мереж, наприклад локальних, цей непотрібний трафік споживає ресурси. Команда passive-interface не дозволить процесу OSPF надсилати зайвий трафік протоколу маршрутизації з інтерфейсів локальної мережі.

Які інтерфейси на R1, R2 і R3 є інтерфейсами локальних мереж?

Налаштуйте процес OSPF на кожному з трьох маршрутизаторів за допомогою команди **passiveinterface**.

Router(config-router)# **passive-interface***interface*

Частина 4. Перевірка налаштувань OSPF

Скористайтесь командами **show** для перевірки налаштувань мережі та пасивних інтерфейсів процесу OSPF на кожному маршрутизаторі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Микитишин А.Г. Комп’ютерні мережі. Книга 1.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 256 с.
2. Микитишин А.Г. Комп’ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.
3. Микитишин А.Г. Телекомунікаційні системи та мережі / Микитишин А.Г., Митник М.М., Стухляк. П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
4. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
5. Буров Є.В. Комп’ютерні мережі. Підручник. Том 1 / Буров Є.В., Митник М.М.; За заг. ред. Пасічника В.В. – Львів: «Магнолія 2006». 2019. – 334 с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
7. ISO/IEC 11801 Information technology – Generic cabling for customer premises – Edition 2. 2.
8. EN 50173– Information Technology – Generic cabling systems.
9. TIA/EIA–568–C Commercial Building Telecommunications Cabling Standard.
10. ISO/IEC TR 14763–2. Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation.
11. ISO/IEC 14763–1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration.
12. Barry J Elliott Designing a structured cabling system to ISO 11801 2nd edition 2002, Published by Wood head Publishing Limited, Abington Hall, Abington Cambridge, England.