Лабораторна робота №4

Тема: Налаштування вихідних параметрів комутатора в мережевій операційній системі Cisco IOS

Мета роботи: здобути навички налаштування основних параметрів комутатора; здобути навички забезпечення безпеки доступу до інтерфейсу командного рядка (CLI) і портів консолі за допомогою зашифрованих і текстових паролів; вивчити способи конфігурації повідомлень, які будуть адресовані користувачам, котрі виконують вхід в систему комутатора, а також повідомлень, які попереджають користувачів про те, що несанкціонований доступ заборонений.

Теоретичні відомості

Комутатор

Комутатори і маршрутизатори Cisco багато в чому схожі. Вони працюють на аналогічній операційній системі, підтримують схожі структури команд, крім того, у них багато однакових команд. Також, при додаванні цих двох пристроїв до мережі, буде потрібно виконати однакові налаштування.

Однак комутатор Cisco IOS (рис. 4.1) є одним з найпростіших пристроїв, який можна встановити в мережі. Це пов'язано з тим, що комутатор може функціонувати і без додаткової конфігурації.

Рис. 4.1. Комутатор Cisco Catalyst 2960

Крім того, комутатор – один з основних пристроїв, що використовуються для створення невеликої мережі. Після підключення двох ПК до комутатора, між цими комп'ютерами відразу буде встановлено з'єднання.

Далі ми розглянемо створення малої мережі з двох ПК, підключених один до одного через комутатор з початковими налаштуваннями. Початкові параметри – це призначення імені комутатора, обмеження доступу до конфігурації пристрою, настройка банерних повідомлень і збереження конфігурації.

Імена пристроїв

Один з перших кроків при налаштуванні мережевого пристрою – це призначення унікального імені. Імена вузлів відображаються у вікнах інтерфейсу командного рядка (CLI) і

використовуються в різних процесах аутентифікації між пристроями. Їх потрібно використовувати в топологічних схемах.

Імена вузлів налаштовуються на активному мережевому пристрої. Якщо ім'я пристрою не задано, Cisco IOS використовує ім'я, призначене за замовчуванням виробником. Ім'я комутатора Cisco IOS за замовчуванням – «Комутатор».

Уявіть собі, що в мережевій взаємодії беруть участь кілька комутаторів, яким було призначено ім'я за замовчуванням «Комутатор» (як показано на рис. 4.2). Це може створити значні проблеми під час налаштування та обслуговування мережі. Під час доступу до віддаленого пристрою за допомогою протоколу SSH важливо мати підтвердження того, що ви підключені до потрібного пристрою. Якщо у всіх пристроїв залишилися імена за замовчуванням, буде складно визначити, чи підключено потрібний пристрій.

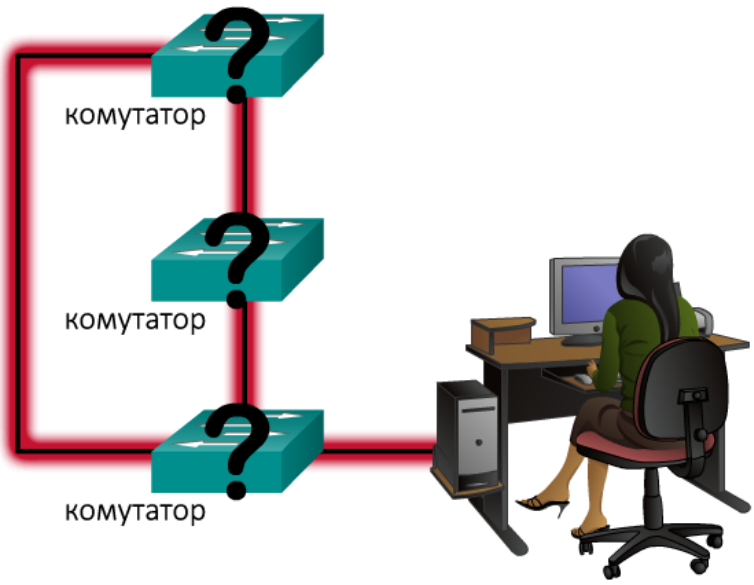

Рис. 4.2. Налаштування базової конфігурації за допомогою Cisco IOS

Якщо розумно призначити імена, буде легше запам'ятовувати мережеві пристрої, обговорювати їх роботу, обслуговувати і розрізняти. Щоб правильно призначити імена, потрібно враховувати угоду про імена, яка поширюється на компанію або місце розташування пристрою. Рекомендується одночасно створювати угоду про імена і схему адресації, щоб не порушити цілісність організації.

Відповідно до посібників по позначенню, імена повинні:

- починатися з літери;
- не містити пробілів;
- закінчуватися на букву або цифру;
- містити тільки букви, цифри і тире;
- містити не більше 64 символів.

В іменах вузлів, що використовуються в пристроях IOS, зберігаються і великі, і малі символи. Тому можна використовувати великі літери. Однак, потрібно відзначити, що цей метод відрізняється від більшості способів призначення імен в Інтернеті, в яких немає відмінностей між великими та малими літерами.

Мережеві адміністратори розпізнають пристрої по локальній мережі або через Інтернет саме за допомогою імен вузлів. Для прикладу візьмемо три комутатора, підключених до мережі, яка охоплює три поверхи. Щоб створити для цих трьох комутаторів угоду імен, потрібно врахувати їх розташування і призначення.

Наприклад, на рис. 4.3 ми назвали три комутатора Ком-Поверх-1, Ком-Поверх-2 і Ком-Поверх-3. Для підтримки цілісності документації, ми зареєстрували їх імена і вказали причини такого найменування. Після укладення угоди про іменування потрібно присвоїти пристроям імена за допомогою інтерфейсу командного рядка (CLI).

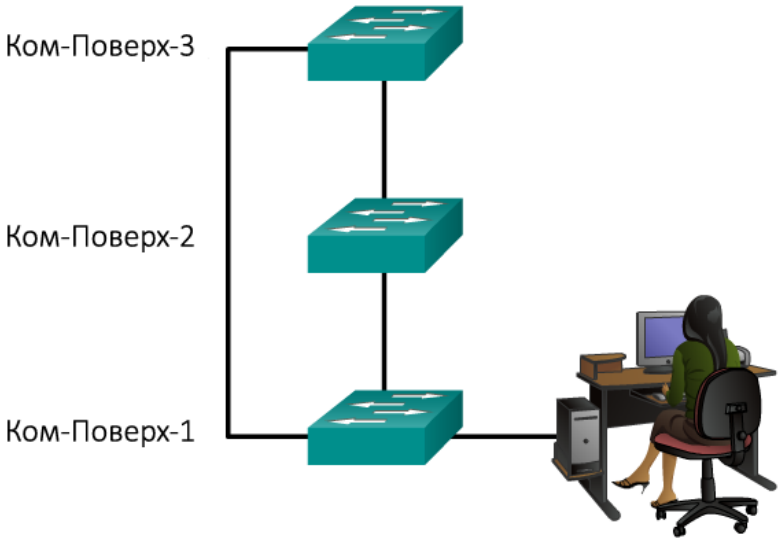

Рис. 4.3. Налаштування імен пристроїв

Налаштування імені вузла IOS

З привілейованого режиму перейдіть в режим глобальної конфігурації за допомогою команди **`configure terminal`**:

```
Switch# configure terminal
```

Після введення команди, командний рядок буде містити наступне:

```
Switch(config)#
```

Як показано на рис. 4.4, в режимі глобальної конфігурації введіть ім'я вузла:

```
Switch(config)# hostname Sw-Floor-1
```

Після введення команди, командний рядок буде містити наступне:

```
Sw-Floor-1(config)#
```

Зверніть увагу, що нове ім'я вузла відображається у вікні запиту. Для виходу з режиму глобальної конфігурації використовуйте команду **`exit`**.

Кожен раз, коли додається або змінюється пристрій, повинна оновлюватися документація. У цій документації пристрою повинні бути присвоєні своє місце розташування, призначення та адреса.

Щоб скасувати дію команди, введіть перед нею ключове слово **no**. Наприклад, щоб видалити ім'я пристрою, потрібно використати наступну команду:

```
Sw-Floor-1(config)# no hostname
```

```
Switch(config)#
```

Зверніть увагу, що команда **no hostname** повернула ім'я комутатора за замовчуванням – «Комутатор».

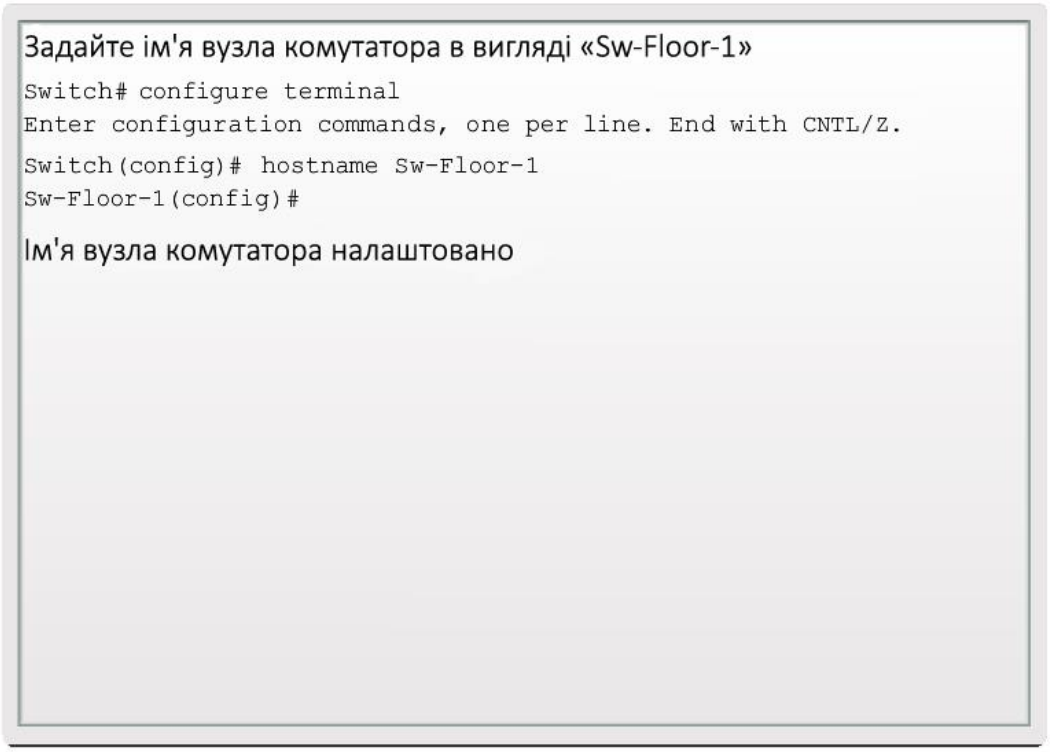

Рис. 4.4. Налаштування імені вузла

Захист доступу до пристроїв

Рекомендується фізично обмежувати доступ до мережевих пристроїв, розміщуючи їх в окремих приміщеннях або в закритих шафах. Проте, паролі залишаються основним засобом захисту від несанкціонованого доступу до мережевих пристроїв. На кожному пристрої, навіть на домашніх маршрутизаторах, повинні бути встановлені паролі для обмеження доступу. Пізніше ми дізнаємося, як посилити захист, налаштувавши запит імені користувача разом з паролем. На даний момент ми розглянемо базові заходи безпеки, використовуючи тільки паролі.

Як зазначалося раніше, для гарантування безпеки пристрій IOS використовує ієрархічні режими. Для посилення захисту IOS може вимагати кілька паролів, щоб надати доступ до різних рівнів ієрархії.

Паролі можуть бути різних типів, серед яких:

- **пароль привілейованого режиму** – обмежує доступ в привілейований режим;
- **секретний пароль** – зашифрований пароль, що обмежує доступ в привілейований режим;
- **пароль консолі** – обмежує доступ до пристроїв через консольне підключення;
- **пароль для VTY** – обмежує доступ до пристроїв через Telnet.

Рекомендується використовувати різні паролі аутентифікації для кожного з рівнів доступу. Незважаючи на те, що вхід в систему з декількома різними паролями незручний, це необхідний захід захисту інфраструктури мережі від несанкціонованого доступу.

Крім того, використовуйте надійні паролі, які складно підібрати. Використання ненадійних паролів або тих, які легко підібрати, представляє серйозну загрозу безпеці в багатьох сферах бізнесу.

При виборі пароля візьміть до уваги наступні основні моменти:

- використовуйте паролі довжиною понад 8 символів;
- використовуйте поєднання великих і малих літер, чисел, спеціальних знаків і/або числових послідовностей;
- на різних пристроях рекомендується використовувати різні паролі;
- не слід використовувати загальновживані слова, такі як «пароль» або «адміністратор», тому що їх легко підібрати.

Примітка. *У більшості лабораторних робіт з даного курсу ми будемо використовувати прості паролі – **cisco** або **class**. Ці паролі ненадійні і їх легко підібрати, тому використовувати їх в робочому середовищі не рекомендується. Ми використовуємо ці паролі лише для зручності роботи в навчальній аудиторії або для демонстрації прикладів.*

Захист доступу до привілейованого режиму

Для захисту доступу до привілейованого режиму використовуйте команду **enable secret** *password*. Застаріла, менш безпечна версія цієї команди – **enable password** *password*. Хоча для настройки аутентифікації перед доступом в привілейований режим підходять обидві ці команди, рекомендується використовувати **enable secret**. Команда **enable secret** забезпечує більш високий рівень безпеки, оскільки пароль зашифрований.

Приклад використання команди для встановлення паролів:

```
Switch(config)# enable secret class
```

Приклад на рис. 4.5 показує, що при першому використанні команди **enable** пароль не потрібен. Далі потрібно ввести команду **enable secret class**, і доступ в привілейований режим буде захищений. Зверніть увагу, що з метою безпеки **пароль при введенні не відображається**.

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Рис. 4.5. Обмеження доступу до пристрою

Захист доступу до користувацького режиму

Консольний порт мережевих пристроїв необхідно захистити як мінімум надійним паролем. Це знижує ймовірність доступу неавторизованих співробітників, які підключають кабель і намагаються отримати доступ до пристрою.

Щоб встановити пароль для консолі рядка в режимі глобальної конфігурації, потрібно ввести наступні команди:

```
Switch(config)# line console 0

Switch(config-line)# password cisco

Switch(config-line)# login
```

У режимі глобальної конфігурації використовується команда **`line console 0`**, щоб увійти в режим конфігурації рядка для консолі. Нуль використовується для позначення першого (а в більшості випадків – єдиного) інтерфейсу консолі.

Друга команда – **`password cisco`** визначає пароль для консолі рядка. Команда **`login`** налаштовує комутатор для аутентифікації при вході в систему. Якщо включена процедура входу і налаштований пароль, користувач консолі повинен буде ввести пароль, щоб отримати доступ до інтерфейсу командного рядка (CLI).

Пароль для VTY

Канали VTY забезпечують доступ до пристроїв Cisco по протоколу Telnet. За замовчуванням багато комутаторів Cisco підтримують до 16 каналів VTY, пронумерованих від 0 до 15. Кількість каналів VTY, що підтримуються на маршрутизаторі Cisco, залежить від типу маршрутизатора і версії IOS. Але найчастіше встановлені п'ять каналів VTY. Ці канали пронумеровані від 0 до 4 за замовчуванням. Пароль потрібно встановити для всіх доступних каналів VTY. Для всіх з'єднань можна встановити один пароль. При цьому часто виникає необхідність встановити унікальний пароль для одного з каналів, щоб забезпечити адміністратору резервний доступ в тому випадку, якщо всі інші з'єднання зайняті.

Команди, які використовуються для призначення пароля каналів VTY:

```
Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line)# login
```

За замовчуванням в IOS вбудована команда **`login`** на каналах VTY. Це запобігає доступу по протоколу Telnet до пристрою без аутентифікації. Якщо помилково була введена команда **`no login`**, через що була знята аутентифікація, по протоколу Telnet, то до мережі можуть приєднатися неавторизовані користувачі. Це являє певну загрозу безпеки. На рис. 4.6 продемонстровано, як здійснюється захист доступу до користувацького режиму на консолі і по каналам Telnet.

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Рис. 4.6. Захист доступу до користувацького режиму на консолі і по каналам Telnet

Шифрування пароля

Ще одна важлива команда, яка захищає пароль під час перегляду файлів конфігурації. Це **service password-encryption**.

Ця команда шифрує паролі під час їх налаштування. Команда **service password-encryption** шифрує всі незашифровані паролі. Шифрування застосовується тільки до паролів в файлі конфігурації, але не до паролів, які відправлені по середовищу передачі даних. Ця команда не дозволяє неавторизованим співробітникам прочитати пароль.

Якщо виконати команди **show running-config** або **show startup-config** до виконання команди **service password-encryption**, то незашифровані паролі будуть видимі в вихідних даних конфігурації. Потім можна виконати команду **service password-encryption**, після чого паролі будуть зашифровані. Після цього шифрування можна буде скасувати. Використавши рис. 4.7 можна відпрацювати введення команди для шифрування пароля.

Банерні повідомлення

Незважаючи на те, що паролі захищають мережу від неавторизованих користувачів, необхідно використовувати повідомлення про те, що лише авторизованим користувачам можна отримати доступ до пристрою. Для цього потрібно додати банер у вихідні дані пристрої.

Банери можуть стати в нагоді під час судового процесу, якщо користувач був звинувачений в недозволеному доступі. У деяких системах правосуддя заборонено судове переслідування або стеження за користувачами без попередження.

Точний зміст або формулювання банера залежать від місцевого законодавства і корпоративної політики. Нижче представлені приклади формулювань, які можуть міститися в таких інформаційних банерах:

- «Доступ до пристрою дозволений тільки для авторизованих користувачів»;
- «Дії можуть відслідковуватися»;
- «Будь-які спроби несанкціонованого використання будуть переслідуватися за законом».

Оскільки банери бачить кожен, хто намагається отримати доступ до пристрою, повідомлення необхідно ретельно сформулювати. Не слід використовувати в формулюванні висловлювання на кшталт «Ласкаво просимо» або щось подібне. Якщо користувач порушує роботу мережі після незаконного проникнення, при наявності вітальних слів складно буде довести злочин.

Введіть команду для шифрування паролів у вигляді незашифрованого тексту

```
Switch(config)#service password-encryption
Switch(config)#exit

Switch# show running-config
!
< вихідні дані приховані >
!
line con 0
 password 7 094F471A1A0A
 login
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
!
!
end

Switch#
```

Шифрування паролів у вигляді незашифрованого тексту виконано

Рис. 4.7. Налаштування шифрування пароля

Створити банери не важко, але їх текст необхідно ретельно продумати. Банер не повинен запрошувати кожного користувача отримати доступ до пристрою. У ньому необхідно вказати, що тільки авторизовані користувачі можуть отримати доступ до пристрою. Крім того, банер може містити розклад відключень системи та інші відомості, які можуть бути корисні іншим користувачам мережі.

IOS надає безліч типів банерів. Щоденне повідомлення – досить поширений банер. Часто використовується для законного повідомлення, так як його бачать всі приєднані термінали.

Налаштуйте щоденне повідомлення за допомогою команди **banner motd** в режимі глобальної конфігурації. Для використання команди **banner motd** необхідні розділові символи, щоб можна було розпізнати зміст банерного повідомлення. Після команди **banner motd** слідують пробіл і розділовий символ. Потім вводиться один чи більше рядків тексту для створення банерного повідомлення. Другий розділовий символ вказує на кінець повідомлення. Розділовим символом може бути будь-який символ, якого немає в даному повідомленні. Тому часто використовуються такі символи, як «#».

Для налаштування щоденного повідомлення в режимі глобальної конфігурації використовуйте наступний синтаксис:

```
Switch(config)# banner motd # message #
```

Після виконання команди банер буде показаний при всіх наступних спробах доступу до пристрою, поки він не буде видалений. На рис. 4.8 показано приклад банера, налаштованого за допомогою розділового символу «#». Зверніть увагу на спосіб відображення банера при отриманні доступу до комутатора.

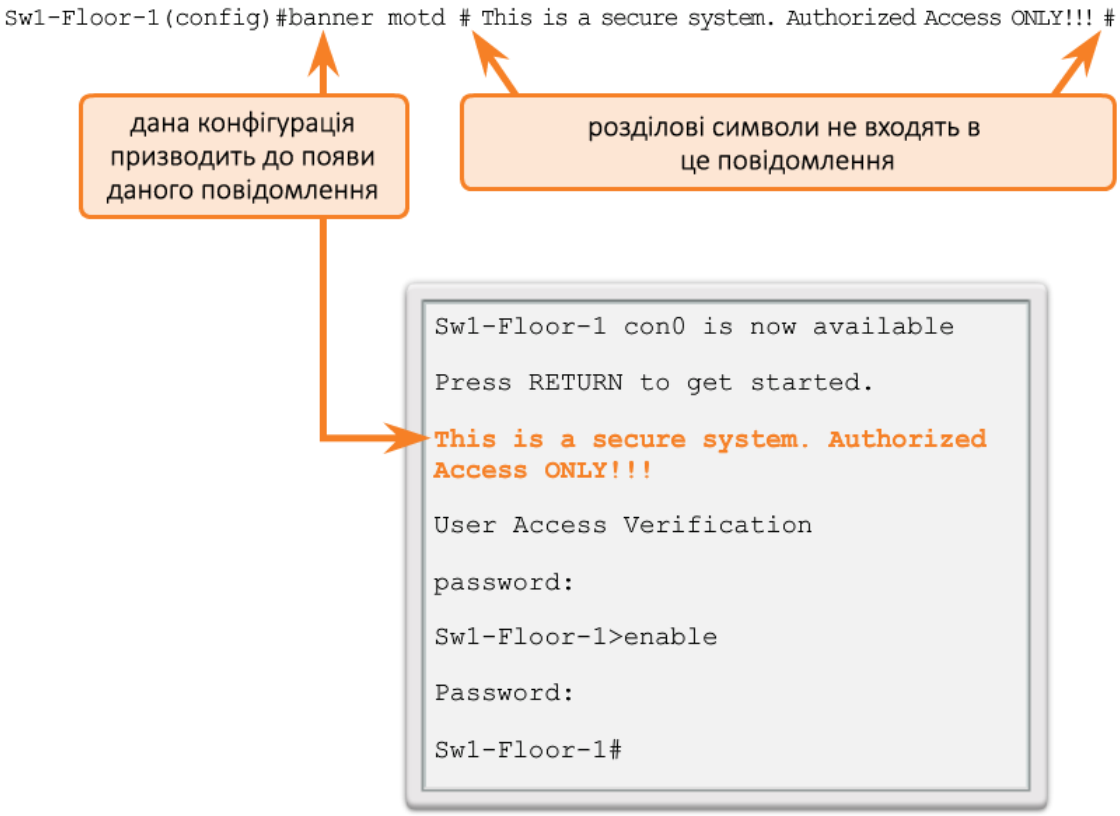

Рис. 4.8. Банер, налаштований за допомогою розділового символу «#»

Файли конфігурації

Файл поточної конфігурації відображає поточну конфігурацію, що функціонує на пристрої Cisco IOS. Він містить команди, які використовуються для визначення принципів роботи пристрою в мережі, як показано на рис. 4.9. Зміни поточної конфігурації негайно впливають на роботу пристрою Cisco.

Файл поточної конфігурації зберігається в робочій пам'яті пристрою або в оперативному запам'ятовуючому пристрої (ОЗП). Це означає, що файл поточної конфігурації тимчасово активний, коли працює пристрій Cisco (підключено живлення). Однак при відключенні живлення пристрою або перезавантаженні пристрою, всі незбережені зміни конфігурації будуть втрачені.

Після внесення змін у файл поточної конфігурації слід розглянути наступні варіанти дій:

- повернути пристрій до початкової конфігурації;
- видалити всі внесені зміни;
- зробити змінену конфігурацію новою початковою конфігурацією.

Файл завантажувальної конфігурації відображає конфігурацію, яка буде застосована на пристрої після перезавантаження. Файл завантажувальної конфігурації зберігається в незалежній пам'яті (NVRAM). Після налаштування мережевого пристрою і зміни поточної конфігурації важливо зберегти ці зміни в файл завантажувальної конфігурації. Це запобігає втратам змін внаслідок збою живлення або випадкового перезавантаження.

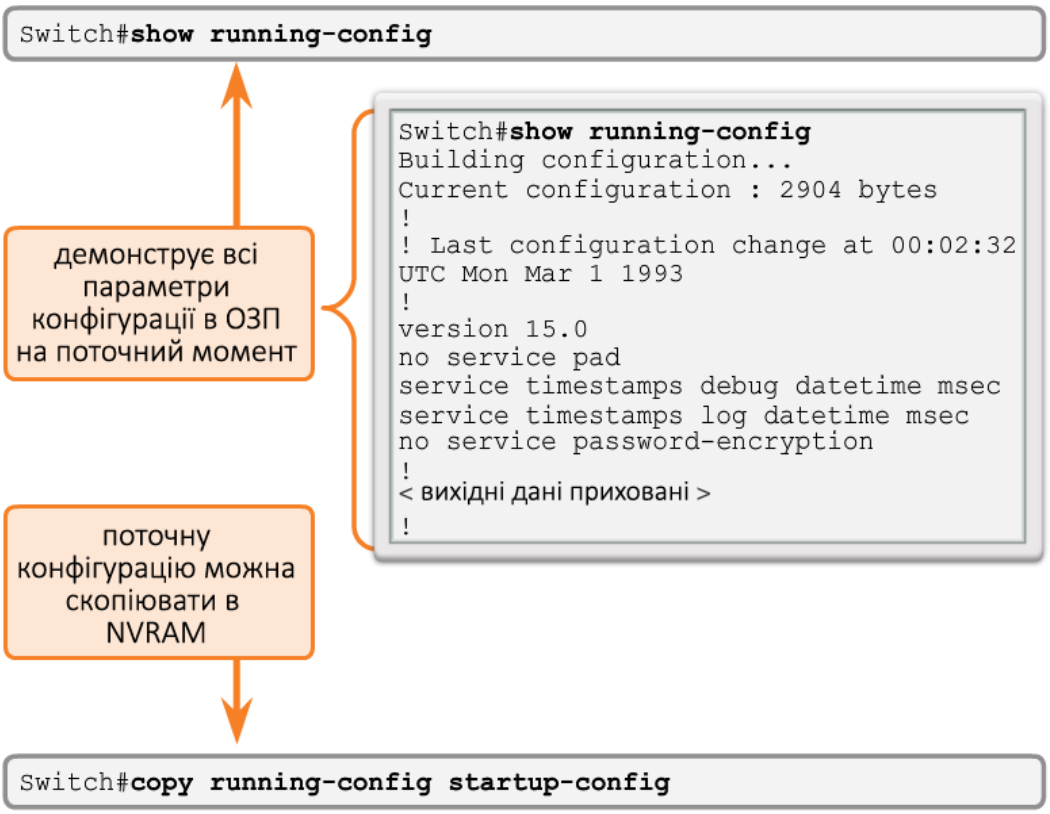

Рис. 4.9. Перегляд файлу поточної конфігурації та збереження файлу поточної конфігурації в файл завантажувальної конфігурації

Перед внесенням змін скористайтеся відповідними командами **show** для перевірки працездатності пристрою. Як показано на рис. 4.9, команду **show running-config** можна використовувати для перегляду файлу поточної конфігурації. Коли зміни перевірені, використовуйте команду **copy running-config startup-config** в командному рядку привілейованого режиму для збереження файлу поточної конфігурації в файл завантажувальної конфігурації:

```
Switch# copy running-config startup-config
```

Після виконання команди, файл поточної конфігурації оновлює файл завантажувальної конфігурації. Якщо зміни, внесені в ході конфігурування не принесли бажаного результату, можливо, потрібно буде відновити попередню конфігурацію пристрою. Якщо ви не перезаписували початкову конфігурацію, поточну конфігурацію можна замінити початковою. Найпростіше це зробити шляхом перезавантаження пристрою і введення команди **reload** в командному рядку привілейованого режиму.

Виконуючи перезавантаження, IOS визначить, що змінена конфігурація не була збережена в файл початкової конфігурації. IOS запросить, чи потрібно зберегти зміни. Для скасування змін введіть **n** або **no**.

Для підтвердження перезавантаження з'явиться додатковий запит. Для підтвердження натисніть **Enter**. Натискання будь-якої іншої клавіші призведе до передчасного завершення даного процесу. Наприклад:

```
Switch# reload

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

```
Proceed with reload? [Confirm]

* Apr 13 01: 34: 15.758:% SYS-5-RELOAD: Reload requested by console.
Reload Reason:

Reload Command.

System Bootstrap, Version 12.3 (8r) T8, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2004 by cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 platform with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled
```

Якщо небажані зміни збережені в файл початкової конфігурації, можливо, знадобиться очистити всі конфігурації. Для цього потрібно видалити початкову конфігурацію і перезапустити пристрій.

Початкову конфігурацію можна видалити за допомогою команди **erase startup-config**. Щоб видалити файл завантажувальної конфігурації, введіть команди **erase NVRAM: startup-config** або **erase startup-config** в командний рядок привілейованого режиму:

```
Switch# erase startup-config
```

Після введення команди з'явиться запит про підтвердження:

```
Erasing the nvram filesystem will remove all configuration files!
Continue? [Confirm]
```

Відповідь за замовчуванням – «Підтверджую». Для підтвердження та видалення файлу завантажувальної конфігурації натисніть клавішу **Enter**. Натискання будь-якої іншої клавіші призведе до передчасного завершення даного процесу.

Увага! *Будьте уважні при використанні команди* **erase***. Цю команду можна використовувати для видалення будь-якого файлу з пристрою. Неправильне використання цієї команди може привести до видалення самої IOS або інших важливих файлів.*

Крім того, на комутаторі необхідно виконати команду **delete vlan.dat** на додаток до команди **erase startup-config**, щоб повернути конфігурацію, «вбудовану» за замовчуванням (відповідну встановленій на підприємстві):

```
Switch# delete vlan.dat
```

```
Delete filename [vlan.dat]?

Delete flash: vlan.dat? [Confirm]

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files!
Continue? [Confirm]

[OK]

Erase of nvram: complete

Switch#
```

Після видалення початкової конфігурації з NVRAM (і видалення файлу vlan.dat з комутатора) перезавантажте пристрій, щоб видалити файл поточної конфігурації з ОЗП. Потім пристрій завантажить файл початкової конфігурації, вбудованої за замовчуванням, в поточну конфігурацію. На рис. 4.10 наведено черговість введення команд для збереження поточної конфігурації з ОЗП в NVRAM, а потім відновлення конфігурації комутатора за замовчуванням.

Завдання

Частина 1: Перевірка конфігурації комутатора за замовчуванням

Крок 1: Вхід в привілейований режим.

У привілейованому режимі доступні всі команди комутатора. Але в зв'язку з тим, що багатьма з привілейованих команд задаються робочі параметри, привілейований доступ повинен бути захищений паролем, щоб уникнути несанкціонованого використання.

До привілейованого набору команд відносяться ті, які містяться в користувацькому режимі, а також команда **configure**, за допомогою якої здійснюється доступ до решти командних режимів.

a. Відкрийте Packet Tracer та додайте **комутатор** (Switch-PT) на робочу область.
b. Клацніть на доданому комутаторі і відкрийте вкладку **CLI**. Натисніть клавішу **Enter**.
c. Перейдіть в привілейований режим, виконавши команду **enable**.

```
Switch> enable
Switch#
```

Зверніть увагу, що змінений в конфігурації рядок буде відображати привілейований режим.

Крок 2: Перегляньте поточну конфігурацію комутатора.

a. Виконайте команду **show running-config**.

```
Switch# show running-config
```

Дайте відповідь на питання «**1.2a.1**»-«**1.2a.5**» у формі **LW №4 CN Quiz**.

Введіть команду в NVRAM для збереження поточної конфігурації, яка зберігається в ОЗП

```
Switch# copy running-config startup-config
```

Тепер в ОЗП і в NVRAM зберігається одна і та ж конфігурація. Для відновлення конфігурації комутатора за замовчуванням необхідно ввести дві команди.
По-перше, введіть команду, яка видалить файл vlan.dat

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

На цьому комутаторі IOS чекає підтвердження імені файлу, а потім підтвердження видалення. Тепер введіть команду для видалення конфігурації, яка зберігається в NVRAM

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

На цьому комутаторі IOS чекає підтвердження команди `erase`. Для завершення процедури відновлення конфігурації за замовчуванням потрібно перезавантажити комутатор

```
Switch# reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with
21039K bytes of memory.
2960-24TT starting...
< вихідні дані приховані >
```

Увійдіть в привілейований режим і відкрийте поточну конфігурацію, яка зберігається в NVRAM

```
Switch> enable


Switch# show startup-config
startup-config is not present
Switch#
```

Тепер конфігурація комутатора за замовчуванням відновлена. Конфігурація комутатора збережена, а потім видалена

Рис. 4.10. Черговість введення команд для збереження поточної конфігурації з ОЗП в NVRAM та відновлення конфігурації комутатора за замовчуванням

Частина 2: Створення базової конфігурації комутатора

Крок 1: Призначення імені комутатору.

Для налаштування параметрів комутатора, можливо, буде потрібно перемикатися між режимами налаштування. Зверніть увагу, як змінюється рядок запрошення при переході по розділах комутатора.

а. Призначте комутатору ім'я **S1**.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
```

```
S1#
```

Крок 2: Безпечний доступ до консолі.

a. Для реалізації 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#
```

Дайте відповідь на питання «**2.2a**» у наступному розділі форми **LW №4 CN Quiz**.

Крок 3: Переконайтеся, що доступ до консолі захищений паролем.

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

```
S1# exit
S1 con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Крок 4: Безпечний доступ в привілейований режим.

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

> **Примітка.** *Символ* 0 *в* **c1$c0** *– це цифра нуль, а не буква «О». Цей пароль не буде надійним, поки ви його не зашифруєте 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 паролем.

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 відноситься до консолі, він був заданий для **line con 0**. Введіть цей пароль, щоб повернутися в користувацький режим.
d. Введіть команду для доступу до привілейованого режиму.
e. Введіть другий пароль, який був заданий для обмеження доступу до привілейованого режиму.
f. Перевірте конфігурацію, вивчивши вміст файлу **running-configuration**:

```
S1# show running-configuration
```

Зверніть увагу, що паролі для консолі і привілейованого режиму відображаються у вигляді звичайного тексту. Це може становити ризик для системи безпеки, якщо за вашими діями спостерігають.

Крок 6: Налаштування зашифрованого пароля для доступу до привілейованого режиму.

Пароль для **enable** потрібно замінити на новий зашифрований пароль за допомогою команди **enable secret**.

a. Встановіть для команди **enable** пароль **itsasecret**.

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

Примітка. *Пароль* **enable secret** *перевизначає пароль* **enable**. *Якщо для комутатора задані обидва паролі, для переходу в привілейований режим потрібно ввести пароль* **enable secret**.

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

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

Примітка. *Команду* **show running-config** *можна скоротити до* **show run**.

Дайте відповідь на питання «**2.7a.1**» і «**2.7a.2**» у формі **LW №4 CN Quiz**.

Крок 8: Шифрування паролів для консолі і привілейованого режиму.

Як було видно на кроці 7, пароль **enable secret** зашифрований, а паролі **enable** і **console** зберігаються у вигляді звичайного тексту.

a. Зашифруйте згадані вище відкриті паролі за допомогою команди **service password-encryption**.

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

Дайте відповідь на питання «**2.8a**» у формі **LW №4 CN Quiz**.

Частина 3: Налаштування банера MOTD

Крок 1: Налаштування повідомлення щоденного банера (MOTD).

a. У набір команд Cisco IOS входить команда, яка дозволяє налаштувати повідомлення, яке буде показуватися всім, хто входить в систему на комутаторі. Це повідомлення називається щоденним банером (MOTD). Текст банера потрібно помістити в подвійні лапки 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#
```

Дайте відповідь на питання «**3.1a.1**» і «**3.1a.2**» у наступному розділі форми **LW №4 CN Quiz**.

Частина 4: Збереження файлів конфігурації в NVRAM

Крок 1: Перевірте правильність конфігурації за допомогою команди «`show run`».

Крок 2: Збережіть файл конфігурації.

a. Ви завершили базове налаштування комутатора. Створіть резервну копію файлу конфігурації в NVRAM і перевірте, щоб внесені зміни не втратились після перезавантаження системи і/або відключення живлення.

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

Дайте відповідь на питання «**4.2a**» у наступному розділі форми **LW №4 CN Quiz**.

Крок 3: Вивчіть початковий файл конфігурації.

a. Дайте відповідь на питання «**4.3a.1**» і «**4.3a.2**» у формі **LW №4 CN Quiz**.

Частина 5: Конфігурація S2

Крок 1. Налаштування конфігурації комутатора S2.

Ви завершили налаштування комутатора **S1**. Тепер додайте ще один **комутатор** (Switch-PT) та налаштуйте для нього наступні параметри (якщо ви не можете згадати необхідні для налаштування команди, поверніться до частин 1-4):

a. Ім'я пристрою: **S2**
b. Захистіть доступ до консолі паролем **`letmein`**.
c. Встановіть для привілейованого режиму пароль **`c1$c0`** і задайте пароль «**`enable secret`**» для **`itsasecret`**.
d. Введіть наступне повідомлення для користувачів, які виконують вхід в систему на комутаторі:

```
Authorized access only. Unauthorized access is prohibited and
violators will be prosecuted to the full extent of the law.
```

e. Зашифруйте всі відкриті паролі.
f. Перевірте правильність конфігурації.
g. Збережіть файл конфігурації, щоб запобігти його втраті в разі відключення живлення комутатора.