МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
"Імітаційне моделювання комп'ютерних мереж"
для студентів спеціальності 123 Комп'ютерна інженерія,
усіх форм навчання

Налаштування комутатора

2024

Методичні вказівки до виконання лабораторних робіт з дисципліни "Імітаційне моделювання комп’ютерних мереж" для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання. Налаштування комутатора / Укл. Г.Г.Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент: М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 7 від 22.03.2024

Затверджено
на засіданні НМК КНТ
Протокол № 8 від 27.03.2024

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА.
Налаштування комутатора Cisco

Мета роботи: ознайомитися: із структурою та налаштуванням керованого комутатора; з основними функціями мережевої операційної системи Cisco IOS та особливостями її застосування на комутаторах; розглянути налаштування основних параметрів комутаторів.

1.1 Теоретичні відомості

Фірма Cisco вже давно займається розробкою і виробництвом комутаторів, додаючи до базового функціоналу комутаторів Ethernet багато нових функцій. Вони реалізували підтримку мережевих протоколів, технологій, архітектур та технологічних рішень. Їх розробки включені до стандарту IEEE 802.3 або є новими стандартами.

Основними складовими комутатора фірми Cisco є центральний процесор (CPU, Central Processing Unit); та блоки: комутації (Switch Fabric); постійної пам'яті (OnBoard ROM, Read-Only Memory); оперативної пам'яті (OnBoard RAM, Random Access Memory типу DRAM, Dynamic RAM або SDRAM, Synchronous DRAM); постійної, перезаписуваної пам'яті (OnBoard Flash); змінної, перезаписуваної пам'яті (Removable Flash); енергонезалежної пам'яті (NVRAM, Non-Volatile Random Access Memory); керування інтерфейсами/портами Ethernet (Port ASICs); фізичного рівня, трансивери Ethernet (Physical Layer Devices); фізичного рівня для формування стеку (Stack Port PHYs) та керування інтерфейсів/портів для підключення робочих станцій керування (Management Interfaces).

Cisco використовує концепцію інтерфейсу командного рядка (CLI) не тільки у комутаторах, а і у своїх маршрутизаторах, а також для більшості пристроїв LAN мереж.

CLI (command-line interface) - це текстовий інтерфейс, у якому користувач, як правило, мережевий інженер, вводить текстову команду та натискає Enter. Натискання клавіші Enter надсилає команду, яка наказує пристрою щось зробити. Пристрій виконує команду, і в деяких випадках, може відповісти повідомленнями про результати виконання команди. Комутатори Cisco Catalyst також підтримують і інші методи моніторингу та налаштування. Наприклад, використати веб-інтерфейс для відкриття веб-браузера при підключенні до веб-сервера, який

працює на комутаторі. Комутаторами також можна керувати та управляти за допомогою програмного забезпечення для керування мережею. Cisco виробляє широкий спектр серій або сімейств комутаторів. Кожна серія комутаторів включає в себе декілька конкретних моделей комутаторів, які мають схожі функції, продуктивність та внутрішні компоненти. На рисунку 1.1 показано фото 10 різних моделей із серії моделей комутаторів 2960-XR від Cisco. Кожна серія комутаторів включає в себе моделі із різноманітними функціями. Наприклад, деякі комутатори мають 48 портів RJ-45 для неекранованої витої пари (UTP) 10/100/1000, - і звеніть увагу, це означає, що порти можуть автоматично погоджувати використання 10BASE-T (10 Мбіт/с), 100BASE-T (100 Мбіт/с) або 1000BASE-T (1 Гбіт/с) Ethernet.

Рис. 1.1. Cisco 2960-XR Catalyst

Зовнішній вигляд комутаторів Cisco серії 2960 наведено на рисунку 1.2. На передній панелі комутатора Cisco розміщуються мережеві інтерфейси/порти, кнопка переключення режимів світлодіодних індикаторів (Mode), світлодіодні індикатори (LEDs), що призначені для відображення стану комутатора в цілому. На задній панелі комутатора Cisco типово розміщуються консольний порт, гніздо для підключення кабелю основного живлення, спеціальний слот для підключення системи резервного живлення та консольний порт.

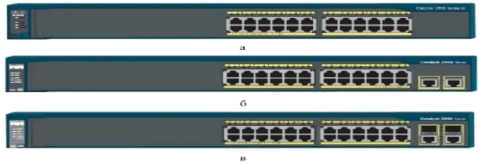

Рис. 1.2. Передня панель комутатора Catalyst 2960: а – модель 2960-24-S; б – модель 2960-24TT-L; в – модель 2960-Plus 24PC-S

Фізичні роз'єми комутатора Cisco називають інтерфейсами або портами з типом і номером інтерфейсу. Тип інтерфейсу, який використовується в командах на комутаторі: Ethernet, Fast Ethernet, Gigabit Ethernet ……. Для інтерфейсів Ethernet, які підтримують роботу на декількох швидкостях, постійна назва інтерфейсу стосується найшвидшої підтримуваної швидкості. Наприклад, інтерфейс 10/100/1000 (тобто інтерфейс, який працює зі швидкістю 10 Мбіт/с, 100 Мбіт/с або 1000 Мбіт/с) має назву Gigabit Ethernet незалежно від того, яка швидкість зараз використовується. Для унікального нумерування кожного окремого інтерфейсу деякі комутатори Catalyst використовують двозначний номер інтерфейсу (x/y), тоді як інші мають тризначний номер (x/y/z). Наприклад, два порти 10/100/1000 на багатьох старих комутаторах Cisco Catalyst мають назву GigabitEthernet 0/0 і GigabitEthernet 0/1, тоді як на новішій серії 2960-XR (рис.1.1) два інтерфейси будуть GigabitEthernet 1/0/1 і GigabitEthernet 1/0/2.

1.2 Підключення до комутатора

Налагодження та керування керованим комутатором може здійснюватися з використанням наступних видів підключень:

- консольне підключення (Console Connection);
- допоміжне підключення (Auxiliary Connection);
- мережеве керуюче підключення (Network Management Connection);
- мережеве підключення (Network Connection).

Як будь-яке інше комп'ютерне обладнання, комутатори Cisco потребують певного програмного забезпечення - операційної системи. У Cisco - це ОС Internetwork Operating System (IOS). Програмне забезпечення Cisco IOS для комутаторів Catalyst реалізує та контролює логіку та функції, які виконуються комутатором Cisco. Окрім керування продуктивністю та поведінкою комутатора, Cisco IOS також визначає інтерфейс для користувачів під назвою CLI. Cisco IOS CLI дозволяє користувачеві використовувати програму емуляції терміналу. Доступ до командного рядка комутатора можна отримати трьома популярними способами: консоль, Telnet і Secure Shell (SSH) (рис.1.3). Два з цих методів (Telnet і SSH), щоб отримати доступ до комутатора, використовують IP-мережу, в якій він знаходиться. Консолью є

фізичний порт, створений спеціально для доступу до CLI. На рисунку показано варіанти.

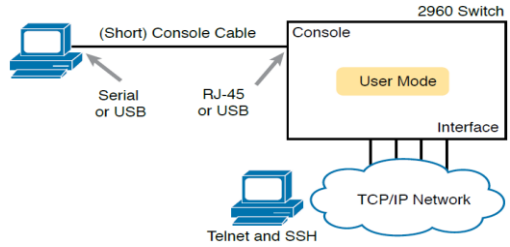

Рис. 1.3. Доступ до командного рядка

Консольне підключення (Console Connection) є прямим підключенням послідовного порта комп'ютера до консольного порта комутатора за допомогою спеціального консольного кабелю (рис. 1.4). Це підключення також позначається як Console Out-of-Band Connection.

З'єднання фізичної консолі використовує три основні компоненти: фізичний консольний порт на комутаторі, фізичний послідовний порт на ПК та кабель, який працює з консоллю та послідовними портами.

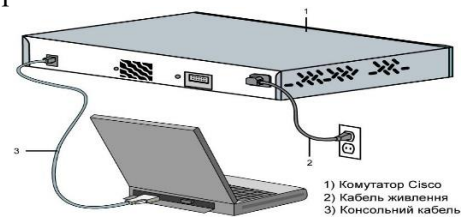

Рис. 1.4. Консольне підключення до комутатора

Основним типом підключення для поточного налагодження, керування та діагностування процесів роботи комутатора є мережеве підключення (Network Connection) – підключення через мережеву інфраструктуру (рис. 1.5), позначається як Network In-Band Connection.

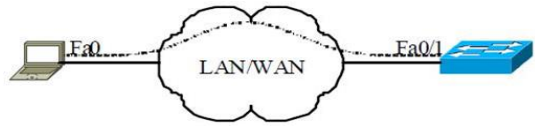

Рис. 1.5. Мережеве підключення до керованого комутатора

У всіх випадках підключень використовуються спеціальні термінальні програмні додатки, що мають засоби забезпечення функціонування як прямих так і мережевих підключень, які використовують протоколи віддаленого доступу. Більшість ПК сьогодні використовують для підключення консолі стандартний кабель USB. Cisco також включає USB-порти як консольні порти в нові маршрутизатори та комутатори. Ви можете використовувати будь-який порт USB на ПК за допомогою кабелю USB, під'єднаного до консольного порту USB на комутаторі або маршрутизаторі, як показано на рисунку 1.6.

Перевага надається порту USB. У разі підключення кабелю до порту USB, порт RJ-45 автоматично відключається, при відключенні кабелю – активується. USB-порти стали звичайними для ПК до того, як Cisco почала широко використовувати USB для консольних портів своїх пристроїв.

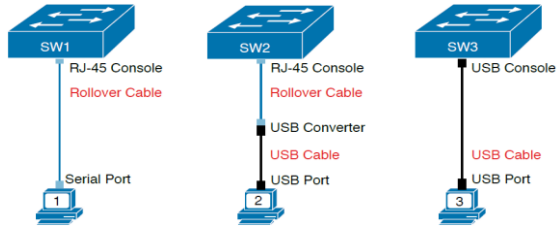

Рис. 1.6. Підключення кабелю до консолі

Тому ви повинні бути готові до використання ПК, який має лише USB-порт, а маршрутизатор або комутатор має старший консольний порт RJ-45 (без порту USB). Центр рисунка 1.6 демонструє цей випадок. Щоб під'єднати комп'ютер до маршрутизатора чи консолі комутатора, потрібен USB-конвертер, який перетворює кабель старої консолі на USB-роз'єм, і кабель UTP. Серія комутаторів 2960-XR, наприклад, підтримує як старіший консольний порт RJ-45, так і консольний порт USB. Рисунок 1.7 вказує на два порти консолі, але для використання застосовується тий чи інший. Зверніть увагу, що консольний USB-порт використовує порт mini-B, а не стандартний прямокутний порт USB типу A, який зустрічається частіше.

Після фізичного підключення комп'ютера до консольного порту на комп'ютері потрібно встановити та налаштувати програмний пакет емулятора терміналу.

Рис. 1.7. Порти консолі

Емулятори терміналу також підтримують TCP/IP, включаючи Telnet і SSH (Secure Shell). Telnet і SSH дозволяють користувачеві підключатися до CLI іншого пристрою, але замість підключення через консольний кабель до консольного порту трафік проходить через ту саму IP-мережу, яку ці мережеві пристрої створюють.

Telnet використовує концепцію клієнта Telnet (програма терміналу) і сервера Telnet (у цьому випадку комутатор).

1.3 Режими роботи комутатора

Керований комутатор Cisco, який працює під керуванням Cisco IOS, має три основних та кілька додаткових командних режими функціонування. Основними режимами є:

– режим користувача (User Mode, User EXEC Mode);

– привілейований режим (Privilege Mode, Privilege EXEC Mode);

– режим глобального конфігурування (Global Configuration Mode).

Додатковими режимами є:

– режим конфігурування інтерфейсу (Interface Configuration Mode);

– режим конфігурування групи інтерфейсів (Interface-range Configuration Mode);

– режим конфігурування лінії (Line Configuration Mode);

– режим конфігурування віртуальної локальної мережі (Config-VLAN Mode);

– режим конфігурування параметрів бази даних віртуальної локальної мережі (VLAN Configuration Mode).

Кожен із режимів надає певні функціональні можливості з діагностування та налагодження роботи комутатора. У кожному режимі

користувачеві надається певний набір команд. Переходи між режимами також здійснюються за допомогою відповідних команд.

1.4 Режими користувача та привілейованого режиму

Усі три розглянуті методи доступу до CLI (консоль, Telnet і SSH) надають користувачу доступ у режимі користувача EXEC. Цей режим дозволяє користувачеві нічого не зламати в процесі налаштувань. В цьому режимі, при введені команди, комутатор виконує команду і відображає результати команди. Також Cisco IOS підтримує більш потужний режим EXEC, який називається режимом ввімкнення (привілейований режим або привілейований режим EXEC). Режим ввімкнення отримав назву від команди enable, що переміщує користувача із режиму користувача в привілейований режим(рис. 1.8) і в ньому можна виконувати привілейовані команди.

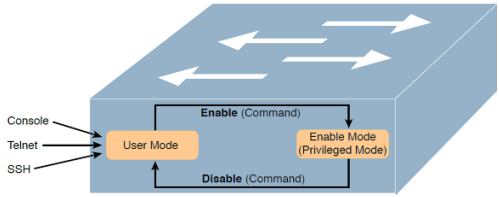

Рис. 1.8. Режим користувача та привілейований режим

Якщо в командному рядку вказано:

– ім’я хоста, за яким стоїть > - то це режим користувача;
– ім'я хоста, після якого йде # - то це привілейований режим.

Приклад демонструє різницю між режимом користувача і привілейованим режимом. У прикладі наведено вихідні дані, які можна побачити у вікні емулятора терміналу, під час підключення з консолі.

Press RETURN to get started.
User Access Verification
Password:
Certskills1>
Certskills1> **reload**
Translating "reload"
% Unknown command or computer name, or unable to find computer address
Certskills1> **enable**
Password:

Certskills1#
Certskills1# **reload**
Proceed with reload? [confirm] y
00:08:42: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command

Користувач в режимі користувача (“Certskills1>”) намагається виконати команду перезавантаження. Команда reload повідомляє комутатору повторно ініціалізувати або перезавантажити Cisco IOS, але IOS дозволяє використовувати цю команду лише в привілейованому режимі. Тому IOS відхиляє команду перезавантаження. Коли користувач переходить у привілейований режим (команда enable EXEC) - IOS вже приймає команду перезавантаження.

Жирний текст це те, що ввів користувач, а нежирний текст – це те, що комутатор надсилає емулятору терміналу. Крім того, введені паролі не відображаються на екрані з міркувань безпеки. І для цього пристрою - попередньо налаштовано ім’я хоста Certskills1, тому командний рядок ліворуч показує це ім’я хоста в кожному рядку.

Далі приклад демонструє додаткові команди конфігурації, які налаштовані перед запитом пароля у першому прикладі. Вихід містить уривок із команди EXEC show running-config, яка містить поточну конфігурацію комутатора.

Certskills1# show running-config
! Output has been formatted to show only the parts relevant to this discussion
hostname Certskills1
!
enable secret love
!
line console 0
login
password faith
! The rest of the output has been omitted
Certskills1#

Перша команда конфігурації - show running-config, встановлює ім’я хоста комутатора як Certskills1.

Далі, рядки із !, є рядками коментарів CLI комутатора. Команда конфігурації enable secret love визначає пароль love, який мають використовувати всі користувачі, щоб перейти у привілейований

режим. Нарешті, останні три рядки налаштовують пароль консолі. Перший рядок (console 0) - команда, яка ідентифікує консоль, що в основному означає «наступні команди застосовуються лише до консолі». Команда входу повідомляє IOS виконати просту перевірку пароля (на консолі). І команда превірки пароля визначає пароль, який користувач консолі має ввести при потребі.

Це простий приклад із типів конфігурації безпеки, яку ви можете налаштувати на комутаторі.

Перелік комбінацій клавіш, які можна використовувати для редагування командного рядка, наведено у таблиці 1.1.

Таблиця 1.1 – Клавіші редагування CLI комутатора

Комбінація клавіш	Виконувані дії
Ctrl+A	Переміщення курсора на початок рядка
Ctrl+B	Переміщення курсора на один символ назад (аналог ←)
Ctrl+D	Переміщення курсора на кінець рядка
Ctrl+E	Переміщення курсора на кінець рядка
Ctrl+F	Переміщення курсора вперед на один символ (аналог →)
Ctrl+K	Видалення всіх символів від позиції курсора до кінця рядка
Ctrl+N	Перехід на наступну в історії сеансу команду (аналог ↓)
Ctrl+P	Перехід на попередню в історії сеансу команду (аналог ↑)
Ctrl+T	Міняє місцями поточний символ і символ ліворуч від курсора
Ctrl+R	Перерисовує або заново виводить поточний рядок
Ctrl+U	Очищення рядка
Ctrl+W	Видалення слова ліворуч від курсора
Ctrl+X	Видалення символів від позиції курсора і до початку рядка
Ctrl+Y	Вставка символів, що видалені останніми
Ctrl+Z	Вихід із поточного режиму і перехід у привілейований режим
Tab	Доповнення поточної команди
Ctrl +^, X	Відміна послідовності. Переривання виконання команди

Після завантаження налагоджений комутатор Cisco перебуває в режимі користувача. Для переходу до привілейованого режиму використовується команда enable. Для повернення – або disable, або exit, або logout. Для переходу до режиму глобального конфігурування використовується команда configure terminal, для виходу – або команда end, або команда exit. Для переходів до інших режимів (конфігурування інтерфейсу/групи інтерфейсів, конфігурування лінії, конфігурування

vlani, тощо) використовуються відповідні команди. Можливе пряме повернення з будь-якого нижчого режиму до привілейованого режим командою end або натисненням комбінації клавіш <Ctrl>+<Z>.

1.5 Команди налагодження та показу

Найпопулярнішою командою Cisco IOS є команда show, яка має багато параметрів. Команда надає інформацію про робочий стан комутатора. Комутатор, у відповідь на команду show, виконує пошук стану та інформацію в повідомленнях, надісланих користувачеві.

Розглянемо результат динамічної команди show mac address-table, наведений у прикладі. Ця команда show, введена в режимі користувача, містить список MAC-адрес в таблиці, яку використовує комутатор для прийняття рішень про пересилання.

```
Certskills1> show mac address-table dynamic
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
31 0200.1111.1111      DYNAMIC          Gi0/1
31 0200.3333.3333      DYNAMIC          Fa0/3
31 1833.9d7b.0e9a      DYNAMIC          Gi0/1
10 1833.9d7b.0e9a      DYNAMIC          Gi0/1
10 30f7.0d29.8561      DYNAMIC          Gi0/1
1   1833.9d7b.0e9a     DYNAMIC          Gi0/1
12 1833.9d7b.0e9a      DYNAMIC          Gi0/1
Total Mac Addresses for this criterion: 7
Certskills1>
```

Команда debug також повідомляє користувача про подробиці роботи комутатора. Однак, поки команда show надає інформацію про стан у конкретний момент часу (як фотографію), то команда debug більш нагадує живу трансляцію відео з камери.

Команда show виводнить діагностичну інформацію про фізичні параметри комутатора, результати налагоджень, результати роботи комутатора, стан комутатора, тощо. Вона є доступною як із режиму користувача, так і з привілейованого режиму.

Залежно від режиму, дана команда може мати різні параметри. Часто команда show із певним параметром вважається окремою командою. Перелік основних команд show та їх призначення наведені у таблиці 1.2.

Таблиця 1.2 – Перелік основних команд show

Команда	Призначення
show version	Виведення технічної інформації про пристрій
show tech-support	Виведення розширеної технічної інформації про пристрій
show flash	Виведення вмісту Flash-пам'яті
show boot	Виведення параметрів завантаження
show processes	Виведення інформації про стан процесів, що запущені в системі
show terminal	Виведення параметрів роботи термінала
show clock	Виведення параметрів системного часу
show history	Виведення історії команд
show running-config	Виведення поточної конфігурації комутатора
show startup-config	Виведення стартової конфігурації комутатора

Важливим питанням налагодження комутатора Cisco є перегляд та збереження його конфігурацій. Як уже зазначалося, для перегляду стартової конфігурації використовується команда show startup-config, а для перегляду поточної конфігурації – команда show running-config. Обов'язковим є збереження налагоджень поточної конфігурації у стартовій. Для цього використовується команда copy running-config startup-config. Існує можливість копіювання конфігурації на зовнішні сервери або із зовнішніх серверів. Це можуть бути традиційні FTP/TFTP або менш уживані SCP чи RCP-сервери.

1.6 Процеси конфігурації

Режим конфігурації є іншим режимом для Cisco CLI, але він подібний до режиму користувача та привілейованого режиму. Однак жодна з команд у режимі користувача чи привілейованому режимі не змінює конфігурацію комутатора.

Режим конфігурації приймає команди конфігурації - команди, які повідомляють комутатору подробиці того, що робити і як це робити.

Рисунок 1.9 ілюструє взаємозв'язки між режимом конфігурації, режимом користувача EXEC і привілейованим режимом EXEC.

Команди, введені в режимі конфігурації, оновлюють активний файл конфігурації. Ці зміни в конфігурації відбуваються негайно щоразу, коли ви натискаєте клавішу Enter у кінці команди. Будьте обережні, коли ви вводите команду конфігурації!

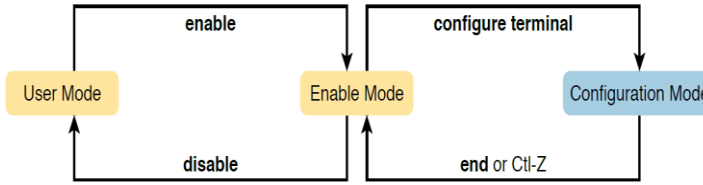

Рис. 1.9. Режим конфігурації

Сам режим конфігурації містить безліч команд. Щоб допомогти організувати конфігурацію, IOS групує деякі типи команд конфігурації.

Найкращий спосіб дізнатися про підрежими конфігурації - це використовувати їх, але спочатку потрібно подивіться на приклади. Наприклад, команда налаштування інтерфейсу є однією з найбільш часто використовуваних команд. Наприклад, користувач CLI може перейти в режим налаштування інтерфейсу, ввівши команду налаштування інтерфейсу FastEthernet 0/1. Запит про допомогу в режимі налаштування інтерфейсу відображає лише команди, які корисні під час налаштування інтерфейсів Ethernet. Команди, які використовуються в цьому контексті, називаються підкомандами або, у цьому конкретному випадку, підкомандами інтерфейсу. Коли ви починаєте роботу з CLI на реальному обладнанні, навігація між режимами може стати природною (рис.1.10).

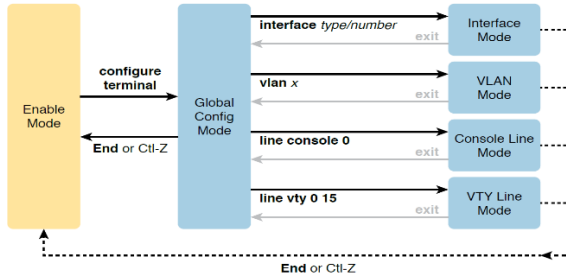

Рис. 1.10. Навігація між режимами

Розглянемо приклад, який показує:

– перехід із режиму включення до режиму глобальної конфігурації за допомогою команди configure terminal EXEC;

– використання команди глобальної конфігурації для налаштування імені комутатора, як Fred;

– перехід із режиму глобальної конфігурації в режим конфігурації рядка (за допомогою команди line console 0);

– встановлення простого пароля консолі (підкоманда password hope);

– перехід із режиму конфігурації консолі в режим конфігурації інтерфейсу (командою interface FastEthernet 0/1);

– встановлення швидкості 100 Мбіт/с для інтерфейсу Fa0/1 (за допомогою підкоманди інтерфейсу speed 100);

– перехід із режиму налаштування інтерфейсу назад до режиму глобального налаштування (командою виходу exit).

```
Switch# configure terminal
Switch(config)# hostname Fred
Fred(config)# line console 0
Fred(config-line)# password hope
Fred(config-line)# interface FastEthernet 0/1
Fred(config-if)# speed 100
Fred(config-if)# exit
Fred(config)#
```

Текст у дужках у командному рядку визначає режим конфігурації. Перший командний рядок після входу в режим конфігурації містить - config, що означає режим глобальної конфігурації. Після команди line console 0 текст розширюється до (config-line), що означає режим конфігурації рядка. Кожного разу, коли командний рядок змінюється в режимі конфігурації, ви переходите до іншого режиму конфігурації.

Конфігурування керованого комутатора Cisco передбачає налагодження: назви, системного годинника, консольного підключення, термінального вікна, часових періодів (тайм-аутів) сеансу, системних повідомлень, безпечного доступу до пристрою, параметрів IP-адресації, тощо.

Назва пристроїв у Cisco IOS використовується:

– для ідентифікації пристрою під час підключення;

– під час розсилки інформації про пристрій іншим пристроям;
– для генерації ключів.

Для зміни імені є команда hostname. Повернення імені за замовчуванням no hostname. За замовчуванням ім'я комутатора Switch.

Налаштування системного часу здійснюється командою clock set, налаштування часового поясу – командою clock timezone. Для активації переходу на літній час застосовується команда clock summertime. Для виведення параметрів часу та дати апаратного годинника у ручному режимі застосовується команда clock read-calendar. Для налаштування апаратного годинника, як джерела мережевого часу застосовується команда clock calendar-valid. Для одноразової ручної синхронізації параметрів часу апаратного годинника з параметрами часу програмного годинника - команда clock update-calendar.

1.7 Захист комутатора

Розглянемо, як налаштувати безпеку входу для комутатора Cisco Catalyst. Захист CLI включає захист доступу до привілейованого режиму, оскільки з цього режиму зловмисник може перезавантажити комутатор або змінити конфігурацію. Захист режиму користувача є також важливим, оскільки зловмисники можуть бачити стан комутатора, дізнаватися про мережу та знаходити нові способи атаки на мережу. Щоб налаштувати спільні паролі для консолі, Telnet і для привілейованого режиму, потрібно налаштувати декілька команд. На рисунку 1.11 показано конфігурацію всіх трьох паролів.

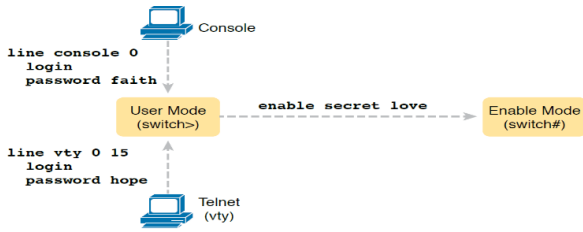

Рис. 1.11. Проста конфігурація захисту паролів

Конфігурація цих трьох паролів не потребує багато роботи. По-перше, конфігурація пароля консолі та vty встановлює пароль на основі контексту: режим консолі (це рядок con 0) і режим конфігурації рядка

vty для пароля Telnet (це рядок vty 0 15). Тоді в режимі консолі та режимі vty, відповідно, дві команди в кожному режимі є такими:

– password password-value: Визначає фактичний пароль, який використовується на консолі або лінії vty;

– login: Вказує IOS увімкнути використання простого спільного пароля (без імені користувача) у цьому рядку (консолі або vty), щоб комутатор запитував у користувача пароль.

Налаштований пароль привілейованого режиму, показаний у правій частині рисунку 1.11, застосовується до всіх користувачів, незалежно від того, чи підключаються вони до режиму користувача через консоль, Telnet чи іншим чином. Команда для налаштування пароля привілейованого режиму є командою глобальної конфігурації: enable secret (увімкнути секретне значення пароля).

Щоб було легше слідкувати за процесом конфігурації можна скористатися контрольним списком конфігурації. Він містить необхідні та додаткові кроки для налаштування потрібних функції. Контрольний список конфігурації для спільних паролів для консолі, Telnet і паролів привілейованого режиму є таким:

Крок 1. Налаштуйте пароль привілейованого режиму за допомогою команди - enable secret.

Крок 2. Налаштуйте пароль консолі.

A. Використовуйте команду line con 0, щоб увійти в режим налаштування консолі.

B. Використовуйте підкоманду password-password-value, щоб установити значення пароля консолі.

C. Використовуйте підкоманду login, щоб увімкнути захист пароля консолі за допомогою простого пароля.

Крок 3. Налаштуйте пароль Telnet (vty).

A. Використовуйте команду line vty 0 15, щоб увійти в режим налаштування vty для всіх 16 ліній vty (пронумерованих від 0 до 15).

B. Використовуйте підкоманду password-password-value, щоб установити значення пароля консолі.

C. Використовуйте підкоманду login, щоб увімкнути захист пароля консолі за допомогою простого пароля.

! Enter global configuration mode, set the enable password, and also

! set the hostname (just because it makes sense to do so)

Switch# configure terminal

```
Switch(config)# enable secret love
! At Step 2 in the checklist, enter console configuration mode, set the
! password value to "faith" and enable simple passwords for the
console.
! The exit command moves the user back to global config mode.
Switch#(config)# line console 0
Switch#(config-line)# password faith
Switch#(config-line)# login
Switch#(config-line)# exit
! The next few lines do basically the same configuration, except it is
! for the vty lines. Telnet users will use "hope" to login.
Switch#(config)# line vty 0 15
Switch#(config-line)# password hope
Switch#(config-line)# login
Switch#(config-line)# end
Switch#
```

У прикладі показано процес конфігурації, як зазначено в контрольному списку конфігурації, разом із встановленням секретного пароля для привілейованого режиму.

Потім результуючу конфігурацію комутатора можна переглянути командою show running-config.

```
Switch# show running-config
!
Building configuration...
Current configuration: 1333 bytes
!
version 12.2
enable secret 5 $1$OwtI$A58c2XgqWyDNeDnv51mNR.
interface FastEthernet0/1
interface FastEthernet0/2
! Several lines have been omitted here - in particular, lines for
! FastEthernet interfaces 0/3 through 0/23.
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
line con 0
password faith
login
```

```
line vty 0 4
password hope
login
line vty 5 15
password hope
login
```

Комутатори Cisco підтримують ще два методи для безпечного входу - використання пари - ім'я користувача/та пароль, замість спільного пароля без імені користувача. Один метод має назву локального і налаштовує пару ім'я користувача/пароль локально, тобто в конфігурації комутатора. Комутатори підтримують цю опцію локального імені користувача/пароля для консолі, для Telnet і навіть для SSH, але не замінюють пароль привілейованого режиму, який використовується для переходу в привілейований режим.

Конфігурація для переходу від використання простих спільних паролів до пар локальне ім'я користувача/і пароль вимагає лише деяких невеликих змін конфігурації, як показано на рисунку 1.12.

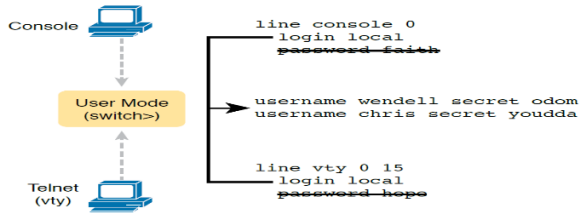

Рис. 1.12. Зміни конфігурації

По-перше, комутатор повинен знати список пар ім'я користувача/пароль. Щоб створити їх - використовуйте команду глобальної конфігурації імені користувача та секретного пароля. Потім, щоб увімкнути цей тип захисту консолі або Telnet, просто ввімкніть цей метод безпчного входу командою, яка означає «використовувати локальний список імен користувачів для входу». Ви також можете використовувати команду no password (навіть не вводячи пароль), щоб очистити будь-які залишкові підкоманди пароля з консолі або режиму vty, оскільки ці команди не потрібні під час використання локальних імен користувачів і паролів. У контрольному списку описано команди для налаштування локального входу за іменем користувача.

Крок 1. Використовуйте команду глобальної конфігурації ім’я користувача та таємний пароль, щоб додати одну або декілька пар ім’я користувача/пароль на локальному комутаторі.

Крок 2. Налаштуйте консоль на використання локально налаштованих пар імені користувача та пароля.

A. Використовуйте команду line con 0, щоб увійти в режим налаштування консолі.

B. Використовуйте підкоманду login local, щоб увімкнути консоль для запиту імені користувача та пароля, перевіряючи їх у списку локальних імен користувачів/паролів.

C. (Необов’язково) Використовуйте підкоманду no password, щоб видалити будь-які наявні прості спільні паролі лише для належного обслуговування файлу конфігурації.

Крок 3. Налаштуйте Telnet (vty) на використання локально налаштованих пар імені користувача та пароля.

A. Використовуйте команду line vty 0 15, щоб увійти в режим налаштування vty для всіх 16 ліній vty (пронумерованих від 0 до 15).

B. Використовуйте підкоманду login local, щоб увімкнути комутатор для запиту імені користувача і пароля для всіх перевірених користувачів Telnet.

C. (Необов’язково) Використовуйте підкоманду no password, щоб видалити будь-які наявні прості спільні паролі лише для належного обслуговування файлу конфігурації.

Коли користувач Telnet підключається до комутатора, налаштованого, як показано на рисунку 1.12, користувачеві спочатку буде запропоновано ввести ім’я користувача, а потім пароль, як показано в прикладі. Пара ім’я користувача/пароль має бути зі списку локальних імен користувачів; інакше вхід буде відхилено.

```
SW2# telnet 10.9.9.19
Trying 10.9.9.19 ... Open
User Access Verification
Username: wendell
Password:
SW1> enable
Password:
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#^Z
```

SW1#

*Mar 1 02:00:56.229: %SYS-5-CONFIG_I: Configured from console by wendell on vty0

(10.9.9.19)

У прикладі значення пароля не відображається як введене, оскільки комутатори Cisco не відображають введений пароль з міркувань безпеки.

У кінці прикладу показано, як користувач входить у режим конфігурації (configure terminal), а потім негайно виходить (^Z). Зверніть увагу, що коли користувач виходить з режиму конфігурації, комутатор створює повідомлення журналу, яке ідентифікує ім'я користувача; зверніть увагу на «wendell» у повідомленні журналу.

1.8 Захист віддаленого доступу за допомогою Secure Shell

Telnet має серйозний недолік: усі дані в сеансі Telnet передаються як відкритий текст, включаючи обмін паролями. Будь-хто може перехопити повідомлення між користувачем і комутатором (атака «людина посередині»), може бачити паролі. SSH шифрує всі дані, що передаються між SSH-клієнтом і сервером, захищаючи дані та паролі.

На рисунку 1.13 показаний приклад конфігурації яка потрібна для підтримки SSH та показано три додаткові команди, необхідні для завершення налаштування SSH на комутаторі.

Рис. 1.13. Зміни конфігурації

IOS використовує три специфічні для SSH команди конфігурації для створення ключів шифрування SSH. Сервер SSH використовує повне доменне ім'я (FQDN) комутатора як вхідні дані для створення цього ключа. Комутатор створює FQDN з імені хоста та імені домену комутатора. Рисунок 1.13 починається з встановлення обох значень (на

випадок, якщо вони ще не налаштовані). Потім третя команда, команда crypto key generate RSA, генерує ключі шифрування SSH. У прикладі показано налаштування команд наведених на рисунку 1.13, із ключем шифрування.

```
SW1# configure terminal
!
SW1(config)# hostname SW1
SW1(config)# ip domain-name example.com
SW1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
SW1(config)#
!
SW1(config)# ip ssh version 2
!
SW1(config)# line vty 0 15
SW1(config-line)# login local
SW1(config-line)# exit
!
SW1(config)# username wendell password odom
SW1(config)# username chris password youdaman
SW1(config)# ^Z
SW1#
```

В цьому прикладі команда crypto key запитує у користувача модуль ключа; також можна додати параметр модулю - значення ключа (1024), щоб додати цей параметр до команди. Дві ключові команди надають деяку інформацію про стан SSH на комутаторі. По-перше, команда show ip ssh відображає інформацію про стан самого сервера SSH. Команда show ssh надає інформацію про кожного SSH-клієнта, підключеного до комутатора. У прикладі показано сесії кожного з користувачів wendell, підключених до комутатора.

```
SW1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
SW1# show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes126-cbc hmac-sha1 Session started wendell
0 2.0 OUT aes126-cbc hmac-sha1 Session started wendell
%No SSHv1 server connections running.
```

1.9 Використання IPv4 для віддаленого доступу

Щоб надати доступ до комутатора через Telnet або SSH і дозволити іншим протоколам керування на основі IP (наприклад, Simple Network Management Protocol або SNMP) працювати належним чином, комутатору потрібна IP-адреса. Вона не має нічого спільного з тим, як Ethernet передає кадри, а потрібна тільки для управління. Для комутатора потрібні такі ж параметри IP, як і для ПК з одним інтерфейсом Ethernet. Щоб призначати IP-адресу керування, комутатор використовує концепцію, яка називається комутованим віртуальним інтерфейсом (SVI), або інтерфейсом VLAN, який діє як мережевий адаптер комутатора. Тоді параметри комутатора виглядають як хост, де конфігурація комутатора використовує IP-параметри, наприклад IP-адресу для інтерфейсу VLAN, як показано на рисунку 1.14.

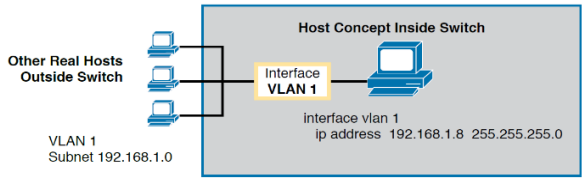

Рис. 1.14. IP-параметри

Використовуючи інтерфейс VLAN 1 для конфігурації IP, комутатор може надсилати та отримувати кадри на будь-якому з портів у VLAN 1. У комутаторі Cisco за замовчуванням усі порти призначено VLAN 1. У більшості мереж на комутаторах налаштовують багато VLAN-ів, тому мережевому інженеру не потрібно налаштовувати IP-адресу керування саме на інтерфейсі VLAN 1. Тоді конфігурація включає інтерфейс VLAN конкретно для цього номера VLAN із відповідною IP-адресою.

Наприклад, на рисунку 1.15 показано комутатор рівня 2 з деякими фізичними портами у двох VLAN (VLAN 1 і 2) та підмережі, які використовуються в цих VLAN. Інженер вибирає будь-який інтерфейс:

- інтерфейс VLAN 1 з IP-адресою в підмережі 192.168.1.0;
- інтерфейс VLAN 2 з IP-адресою в підмережі 192.168.2.0.

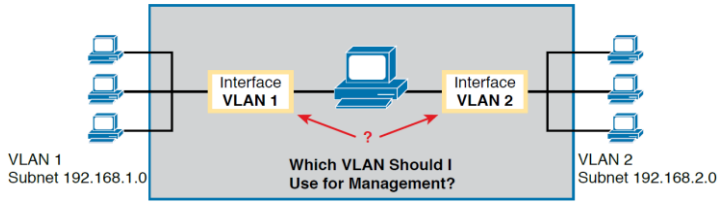

Рис. 1.15. Вибір VLAN для налаштування

1.10 Завдання. Налаштування параметрів комутатора

Метою є налаштування основних параметрів комутатора, забезпечення безпеки доступу до інтерфейсу командного рядка (CLI) та портів консолі за допомогою зашифрованих та текстових паролів, а також вивчення способів конфігурації повідомлень, що адресовані користувачам та входять до системи комутатора.

В середовищі Cisco Packet Tracer зробіть проект локальної мережі (рис. 1.16), звернувши увагу на вибір моделі комутатора, мережевих модулів та адаптерів, а також мережевих з'єднань.

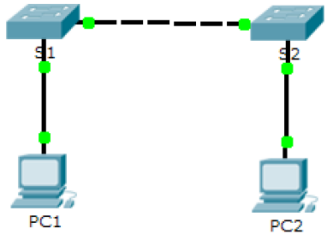

Рисунок 1.16 – Модель мережі

1.11 Створення базової конфігурації комутатора

1. Виконайте вхід до привілейованого режиму враховуючи, що привілейованими командами задаються робочі параметри. До привілейованого набору команд відносяться ті, які містяться в режимі користувача, а також команда configure, за допомогою якої виконується доступ до інших командних режимів:

– клацніть S1 і відкрийте вкладку CLI. Натисніть клавішу ENTER;

– перейдіть до привілейованого режиму, виконавши команду enable.

Switch> **enable**

Switch#

Зверніть увагу, що змінений у конфігурації рядок відображатиме привілейований режим.

2. Перегляньте поточну конфігурацію комутатора, виконавши команду show running-config.

Switch # **show running-config**

3. Призначьте комутатору ім'я, враховуючи, що можливо, для налаштування параметрів комутатора потрібно перемикатися між режимами налаштування. Зверніть увагу, як змінюється рядок запрошення під час переходу до розділів комутатора.

Switch# **configure terminal**

Switch(config)# **hostname S1**

S1(config)# **exit**

S1#

4. Для забезпечення безпечного доступу до консолі перейдіть в режим config-line та 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#

5. Вийдіть із 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, то ви не налаштували параметр login на кроці 4.

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

Примітка. Символ 0 у c1$c0 - це цифра нуль, а не літера «O». Цей пароль не буде дійсним, поки ви не зашифруєте його на кроці 10.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

7. Переконайтеся, що доступ до привілейованого режиму захищений паролем, для цього:

– виконайте команду exit ще раз, щоб вийти з комутатора;

– натисніть клавішу <ВВЕДЕННЯ>, після чого вам буде запропоновано ввести пароль:

User Access Verification
Password:

– перший пароль відноситься до консолі, який був заданий для **line con 0**. Введіть цей пароль, щоб повернутися в режим користувача;

– ведіть команду, щоб отримати доступ до привілейованого режиму;

– введіть другий пароль для обмеження доступу до привілейованого режиму;

– перевірте конфігурацію, вивчивши вміст файлу running-configuration:

S1# **show running-configuration**

Зверніть увагу, що паролі для консолі та привілейованого режиму відображаються у вигляді звичайного тексту. Це може становити ризик для системи безпеки.

8. Пароль для enable потрібно замінити на новий зашифрований пароль за допомогою команди **enable secret**. 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 задано обидва паролі, для переходу в привілейований режим потрібно ввести пароль enable secret.

9. Переконайтеся, що пароль "**enable secret**" додано до конфігураційного файлу. Для цього введіть команду show running-config ще раз, щоб перевірити новий пароль enable secret.

Примітка. Команду show running-config можна скоротити до

S1 # show run

10.Ви бачите, що пароль **enable secret** зашифрований, а паролі enable і console зберігаються як звичайний текст. Тому зашифруємо ці відкриті паролі за допомогою команди **service password-encryption**.

S1# **config t**

S1(config)# **service password-encryption**

S1(config)# **exit**

11.У наборі команд Cisco IOS є команда, яка дозволяє налаштувати повідомлення, яке побачать всі, хто входить у систему на комутаторі. Це повідомлення називається щоденним банером (MOTD). Текст банера береться в подвійні лапки або використовує 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#

12.Для збереження файлів конфігурації в NVRAM, спочатку перевірте правильність конфігурації за допомогою команди **show run**. Потім збережіть конфігураційний файл, виконавши резервне копіювання файлу конфігурації в NVRAM і перевірте, щоб зміни не втратилися після перезавантаження системи та вимкнення живлення.

S1# **copy running-config startup-config**

Destination filename [startup-config]?**[Enter]**

Building configuration...

[OK]

13.Ви завершили налаштування комутатора S1. Тепер налаштуйте комутатор S2. Якщо ви не можете згадати команди, поверніться до початку. Налаштуйте для комутатора S2 такі параметри:

– ім'я пристрою: S2;

– захистіть доступ до консолі паролем letmein;

– встановіть для привілейованого режиму пароль c1$c0 і введіть пароль "enable secret" для itsasecret;

– введіть наступне повідомлення для користувачів, які входять до системи на комутаторі: Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law;

– зашифруйте всі відкриті паролі;

– перевірте правильність конфігурації;

– збережіть файл конфігурації, щоб запобігти його втраті у разі вимкнення живлення комутатора.

1.12 Зміст звіту

– хід роботи;

– основна працююча схема мережі;

– відповіді на контрольні питання.

1.13 Контрольні питання

1. Яка команда відображає поточний вміст NVRAM?
2. Чому комутатор відповідає повідомленням startup-config is not present?
3. Навіщо потрібна команда login?
4. Що відображається під час виведення пароля enable secret?
5. Чому пароль enable secret відображається не так, як пароль?
6. Якщо встановити на комутаторі інші паролі, вони зберігатимуться у файлі конфігурації у вигляді звичайного тексту чи зашифрованому вигляді? Поясніть, чому?
7. Якою є найкоротша версія команди copy running-config startup-config?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
3. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 1. 2024. 30 с.
4. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 2. 2024. 30 с.
5. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 3. 2024. 30 с.
6. Киричек Г.Г. Лабораторні роботи з імітаційного моделювання комп'ютерних мереж. Розрахунки працездатності мереж. Розробка структурних схем. 2023. 30 с.
7. Киричек Г.Г. Лабораторні роботи з імітаційного моделювання комп'ютерних мереж. Моделювання мереж із застосуванням динамічної конфігурації кінцевих вузлів та простих методів безпеки. 2023. 30 с.
8. Киричек Г.Г. Конспект лекцій з дисципліни Комп'ютерні мережі. 2024. 58 с.
9. Киричек Г.Г. Проходження тестування з дисципліни Комп'ютерні мережі. Частина 1. 2024. 30 с.
10. Киричек Г.Г. Проходження тестування з дисципліни Комп'ютерні мережі. Частина 2. 2024. 30 с.
11. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
12. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.
13. Tulloch M., Team WS Introducing Windows Server 2012 R2. - Microsoft press, 2013.
14. Krause J. Mastering Windows Server 2016. - Packt Publishing Ltd, 2016.
15. IT Блог Тараса Кучинского. Знайомство з програмою "Cisco packet tracer". URL: https://kychinskiy.blogspot.com/2017/12/cisco-packet-tracer.html.