Вступ до мереж

Тема2. Базові налаштування комутатора і кінцевого пристрою

2.01. Чому варто вивчити цей розділ?

Ласкаво просимо до базового налаштування комутатора та кінцевого пристрою!

В рамках вашої кар'єри в мережах, можливо, доведеться налаштовувати нову мережу або підтримувати і оновлювати існуючу. У будь-якому випадку ви налаштуєте комутатори та кінцеві пристрої таким чином, щоб вони були захищеними та ефективно працювали на основі ваших вимог.

Вихідні пристрої, комутатори і кінцеві пристрої мають деяку загальну конфігурацію. Але для вашої конкретної мережі комутатори та кінцеві пристрої вимагають вашої конкретної інформації та інструкцій. У цьому розділі ви дізнаєтесь, як отримати доступ до мережних пристроїв Cisco IOS. Ви вивчите основні команди конфігурації та використовуватимете їх для налаштування та перевірки пристрою Cisco IOS та кінцевого пристрою з IP-адресою.

Звичайно, є ще багато можливостей для мережного адміністрування, але нічого з цього не може статися без попереднього налаштування комутаторів та кінцевих пристроїв. Давайте розпочнемо!

2.02. Що нового я дізнаюсь у цьому розділі?

Заголовок розділу: Базові налаштування комутатора та кінцевого пристрою

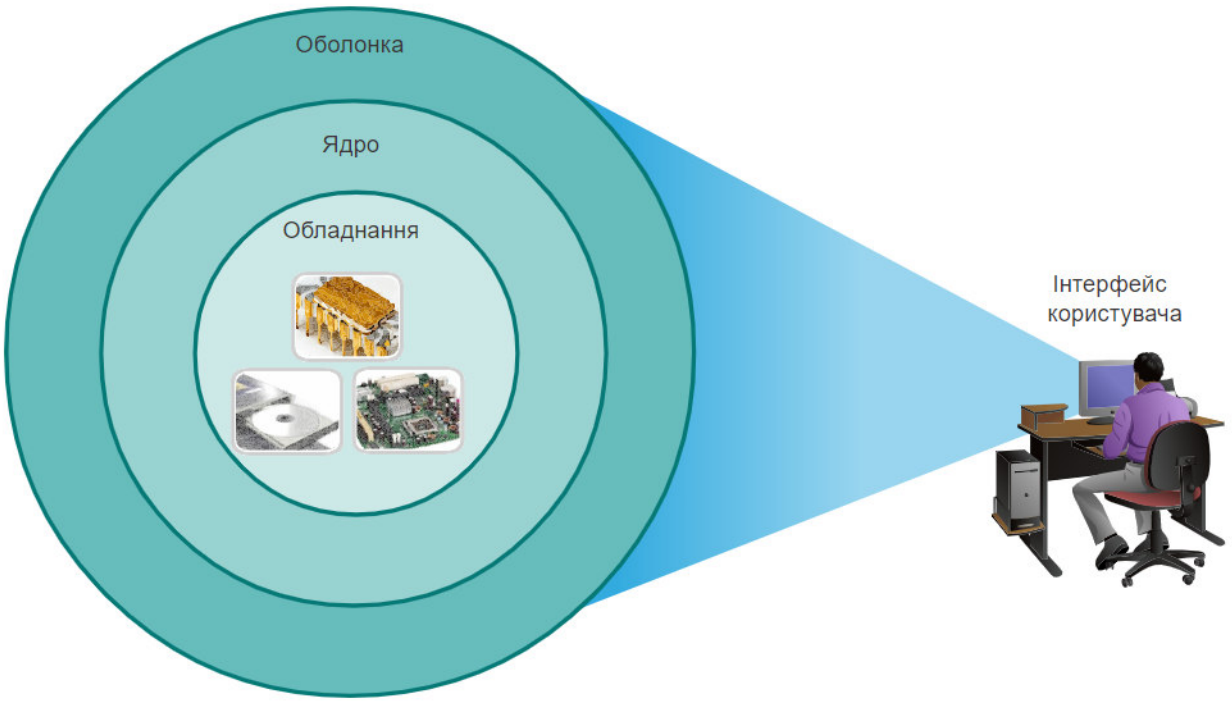
Мета розділу: Виконання початкових налаштувань, зокрема, встановлення паролів, IP-адресації і параметрів шлюзу за замовчуванням, на мережному комутаторі та кінцевих пристроях.

Назва теми	Мета вивчення теми
2.1. Доступ до Cisco IOS	Пояснити, як отримати доступ до пристрою під керуванням Cisco IOS з метою налаштування.
2.2. Навігація в IOS	Пояснити, як орієнтуватися у Cisco IOS для конфігурування мережних пристроїв.
2.3. Структура команд	Описати структуру команд програмного забезпечення Cisco IOS.
2.4. Базові налаштування пристрою	Виконати налаштування пристрою під керуванням Cisco IOS за допомогою CLI.
2.5. Зберігання налаштувань	Використання команд IOS для зберігання поточних налаштувань.
2.6. Порти і адреси	Пояснити, як пристрої взаємодіють у мережному середовищі.
2.7. Налаштування IP-адресації	Налаштування IP-адреси на кінцевому пристрої.
2.8. Перевірка з'єднання	Виконати перевірку з'єднання двох кінцевих пристроїв.

2.1. Доступ до Cisco IOS

2.1.1. Операційні системи

Усі кінцеві пристрої та мережні пристрої потребують операційної системи (ОС). Як показано на рисунку, частина ОС, яка взаємодіє безпосередньо з комп'ютерним обладнанням, називається ядром. Частина, яка взаємодіє з програмами та користувачем, називається оболонка. Користувач може взаємодіяти з оболонкою за допомогою інтерфейсу командного рядка (command-line interface, CLI) або графічного інтерфейсу користувача (graphical user interface, GUI).



- **Оболонка** - призначений для користувача інтерфейс, що дозволяє користувачам робити конкретні запити з комп'ютера. Ці запити можна робити або через інтерфейси CLI або GUI.
- **Ядро** - частина операційної системи, що забезпечує взаємодію апаратних засобів і програмного забезпечення комп'ютера, розподіл системних ресурсів та інше.
- **Обладнання** - електронні та інші "фізичні" компоненти комп'ютера.

Під час використання CLI користувач взаємодіє безпосередньо з системою в текстовому середовищі, вводячи команди на клавіатурі в командному рядку, як показано в прикладі. Система виконує команду, часто надаючи вихідні дані у текстовому вигляді. Для роботи CLI потрібно дуже мало накладних витрат. Однак користувач повинен мати знання про базову структуру команд для керування системою.

```
analyst@secOps ~]$ ls
```

```
Desktop Downloads lab.support.files second_drive
```

```
[analyst@secOps ~]$
```

2.1.2. Графічний інтерфейс користувача

Графічний інтерфейс користувача (GUI), такий як у ОС Windows, macOS, Linux KDE, Apple iOS або Android, дозволяє користувачеві взаємодіяти з системою, використовуючи середовище графічних значків, меню та вікон. Приклад GUI, який зображено на рисунку, більш зручний для

користувачів та вимагає менших знань базової структури команд для керування системою. З цієї причини більшість користувачів використовують GUI.

Проте, GUI не завжди може забезпечити всі функції, які доступні при використанні CLI. Крім того, в GUI часто виникають помилки, аварійні збої або інтерфейс просто не працює належним чином. Тому до мережних пристроїв, як правило, звертаються через CLI. CLI менш ресурсомісткий і дуже стабільний у порівнянні з GUI.

Сімейство мережних операційних систем, що використовуються на багатьох пристроях Cisco, називається **Cisco Internetwork Operating System (IOS)**. Cisco IOS використовується на багатьох маршрутизаторах і комутаторах Cisco незалежно від типу або розміру пристрою. Кожен тип маршрутизатора або комутатора використовує свою версію Cisco IOS. Інші операційні системи Cisco включають IOS XE, IOS XR та NX-OS.

Примітка: Операційну систему на домашніх маршрутизаторах зазвичай називають мікропрограмним забезпеченням (*firmware*). Найпоширеніший метод налаштування домашнього маршрутизатора - це використання GUI на базі веб-браузера.

2.1.3. Призначення ОС

Мережні операційні системи схожі на операційну систему ПК. Через GUI операційна система ПК дозволяє користувачеві виконати такі задачі:

- Використовувати мишу для вибору та запуску програм.
- Вводити текст та текстові команди.
- Переглядати результат на моніторі.

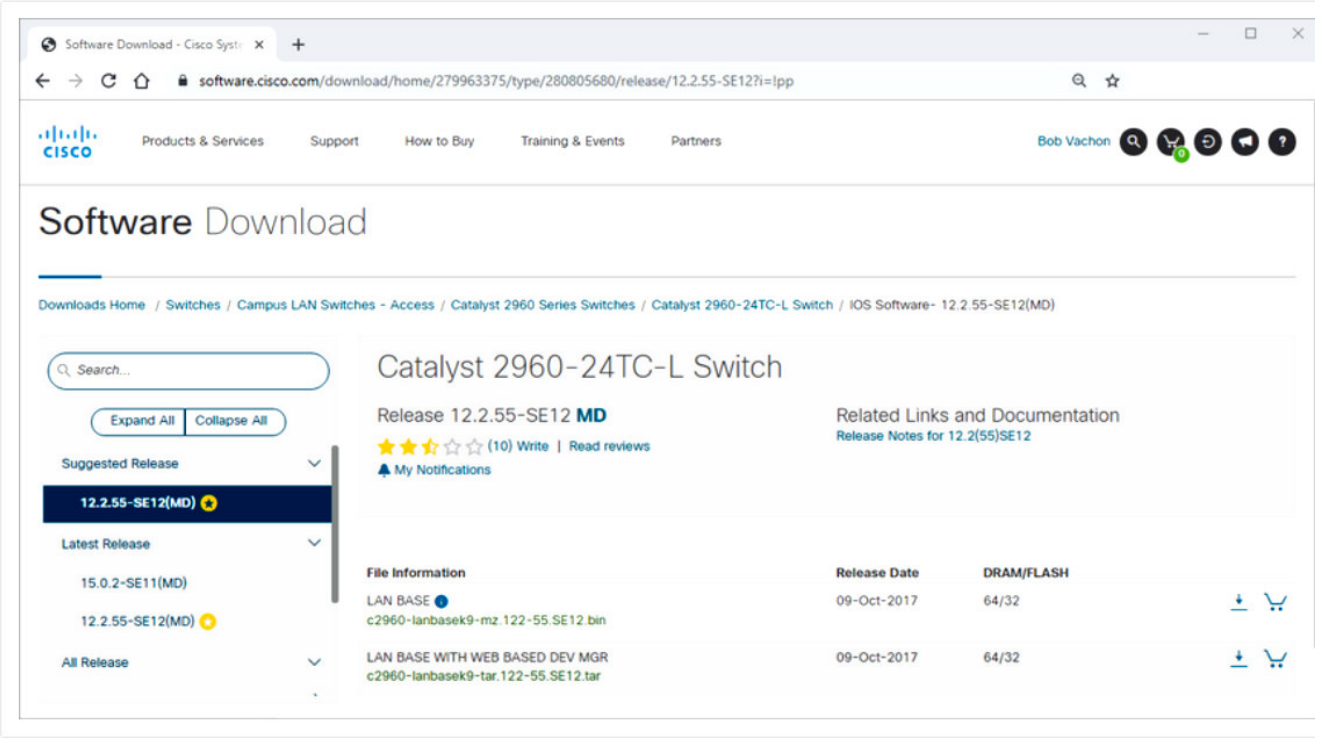
Мережна операційна система на основі CLI (наприклад, Cisco IOS на комутаторі або маршрутизаторі) дозволяє мережному спеціалісту:

- Використовувати клавіатуру для запуску мережних програм на базі CLI.
- Використовувати клавіатуру для введення тексту та текстових команд.
- Переглядати результат на моніторі.

Мережні пристрої Cisco працюють під керуванням певних версій Cisco IOS. Версія IOS залежить від типу пристрою, який використовується, та необхідних функцій. Хоча всі пристрої поставляються зі стандартною IOS і набором функцій за замовчуванням, можна оновити версію або набір функцій IOS, щоб отримати додаткові можливості.

На рисунку відображається перелік версій програмного забезпечення IOS для комутатора Cisco Catalyst 2960.

Приклад завантаження програмного забезпечення Cisco



2.1.4. *Методи доступу*

Комутатор буде пересилати трафік за замовчуванням і його не потрібно чітко налаштовувати для роботи. Наприклад, два налаштовані вузли, які під'єднані до одного і того ж нового комутатора, зможуть спілкуватися.

Незалежно від поведінки нового комутатора за замовчуванням, всі комутатори повинні бути налаштовані і захищені.

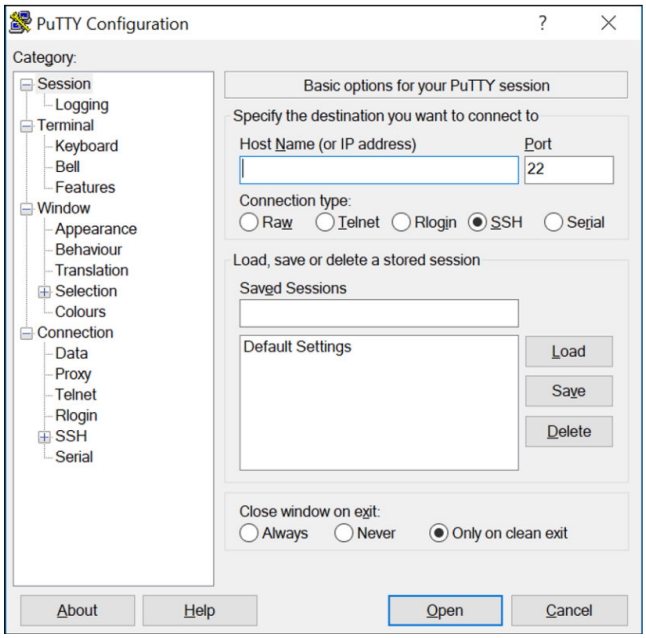
Заголовок таблиці	
Метод	**Опис**
Консоль	Це фізичний порт керування, який забезпечує позасмуговий доступ до пристрою Cisco. Позасмуговий доступ здійснюється через виділений адміністративний канал, який використовується для технічного обслуговування пристрою. Перевага використання консольного порту полягає в тому, що доступ до пристрію є, навіть якщо не налаштовано жодних мережних служб, наприклад, під час початкового налаштування пристрою. Для під'єднання до консолі потрібні програмне забезпечення для емуляції терміналу та спеціальний консольний кабель для під'єднання до пристрою.
Протокол Secure Shell (SSH)	SSH - це вбудований і рекомендований метод дистанційного встановлення захищеного CLI-з'єднання через віртуальний інтерфейс через мережу. На відміну від консольного з'єднання, SSH-з'єднання вимагають активних мережних служб на пристрої, включаючи активний інтерфейс з налаштованою адресою. Більшість версій Cisco IOS включають SSH-сервер та SSH-клієнт, які можна використовувати для встановлення сеансів SSH з іншими пристроями.

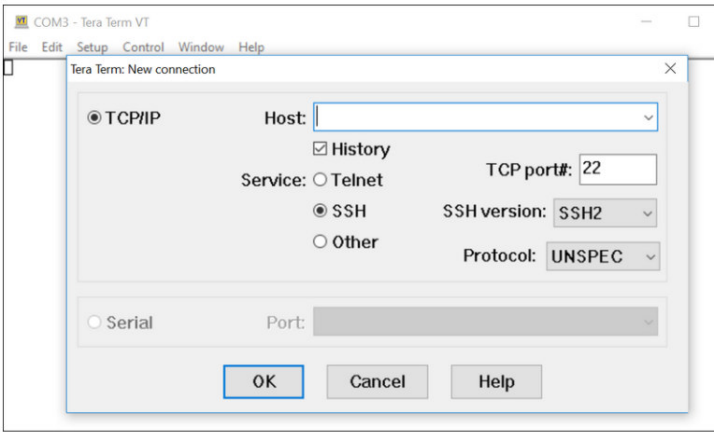
Заголовок таблиці	
Метод	**Опис**
Telnet	Telnet - це незахищений, вбудований метод дистанційного встановлення сеансу CLI через віртуальний інтерфейс через мережу. На відміну від SSH, Telnet не забезпечує захищене, зашифроване з'єднання і його слід використовувати лише в лабораторних умовах. Ідентифікація користувача, паролі та команди надсилаються через мережу у вигляді простого тексту. Найкраща практика - використовувати SSH замість Telnet. Cisco IOS включає як сервер Telnet, так і клієнт Telnet.

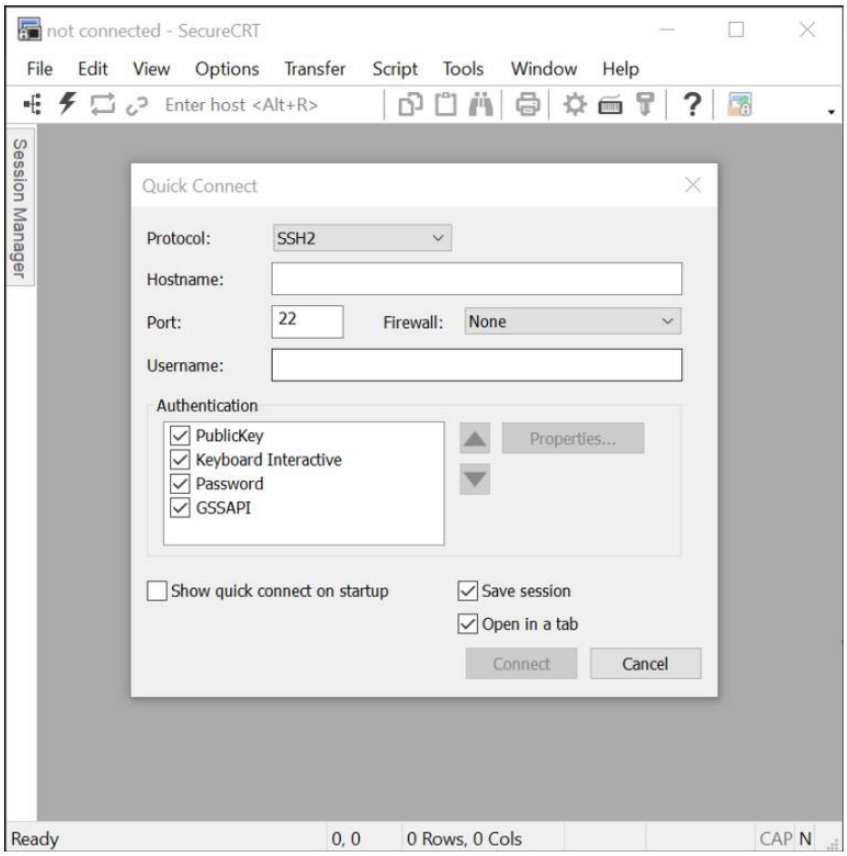
Примітка: Деякі пристрої, такі як маршрутизатори, можуть також підтримувати застарілий допоміжний порт, який використовувався для дистанційного встановлення сеансу CLI через телефонний зв’язок за допомогою модему. Подібно консольному з'єднанню, порт AUX також позасмуговий і не вимагає налаштування або доступності мережних служб.

2.1.5. *Програми емуляції терміналу*

Існує кілька програм емуляції терміналів, які можна використовувати для під'єднання до мережного пристрою або через послідовне з'єднання через консольний порт, або через з'єднання SSH/Telnet. Ці програми дозволяють підвищити вашу продуктивність, регулюючи розміри вікон, змінюючи розміри шрифту та змінюючи кольорові схеми.






not connected - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
Session Manager
Quick Connect
Protocol: SSH2
Hostname:
Port: 22
Firewall: None
Username:
Authentication
PublicKey
Keyboard Interactive
Password
GSSAPI
Properties...
Show quick connect on startup
Save session
Open in a tab
Connect
Cancel
Ready
0, 0
0 Rows, 0 Cols
CAP N

2.1.6. *Питання для самоперевірки - Доступ до Cisco IOS*

1. Який метод доступу був би найбільш відповідним, якби ви були в приміщенні з обладнанням з новим комутатором, який потрібно налаштувати?

   - ◯ Консоль
   - ◯ Telnet/SSH
   - ◯ Aux

2. Який метод доступу був би найбільш відповідним, якщо ваш менеджер подав вам спеціальний кабель і наказав вам використовувати його для налаштування комутатора?

   - ◯ Консоль
   - ◯ Telnet/SSH
   - ◯ Aux

3. Який метод доступу був би найбільш відповідним вбудованим доступом до IOS через мережне з'єднання?

   - ◯ Консоль
   - ◯ Telnet/SSH
   - ◯ Aux

4. Який метод доступу буде найбільш відповідним, якщо ви зателефонуєте своєму менеджеру і скажете йому, що ви не можете отримати доступ до маршрутизатора в іншому місті через Інтернет, і він надасть вам інформацію для доступу до маршрутизатора через телефонне з'єднання?

   - ◯ Консоль
   - ◯ Telnet/SSH
   - ◯ Aux

1. Який метод доступу був би найбільш відповідним, якби ви були в приміщенні з обладнанням з новим комутатором, який потрібно налаштувати?

Правильно!

- (●) Консоль
- ( ) Telnet/SSH
- ( ) Aux

2. Який метод доступу був би найбільш відповідним, якщо ваш менеджер подав вам спеціальний кабель і наказав вам використовувати його для налаштування комутатора?

Правильно!

- (●) Консоль
- ( ) Telnet/SSH
- ( ) Aux

3. Який метод доступу був би найбільш відповідним вбудованим доступом до IOS через мережне з'єднання?

Правильно!

- ( ) Консоль
- (●) Telnet/SSH
- ( ) Aux

4. Який метод доступу буде найбільш відповідним, якщо ви зателефонуєте своєму менеджеру і скажете йому, що ви не можете отримати доступ до маршрутизатора в іншому місті через Інтернет, і він надасть вам інформацію для доступу до маршрутизатора через телефонне з'єднання?

Правильно!

- ( ) Консоль
- ( ) Telnet/SSH
- (●) Aux

2.2. Навігація в IOS

2.2.1 Основні командні режими

У попередній темі ви дізналися, що всі мережні пристрої потребують ОС і що їх можна налаштувати за допомогою CLI або GUI. Використання CLI може надати адміністратору мережі більш точний контроль та гнучкість, ніж використання GUI. У цій темі обговорюється використання CLI для навігації в Cisco IOS.

З міркувань безпеки Cisco IOS використовує два окремих командних режими для доступу до адміністративних функцій:

- **Користувацький режим EXEC (User EXEC)** - цей режим має обмежені можливості, але корисний для основних операцій. В користувацькому режимі доступне лише обмежене число основних команд моніторингу та неможливо виконувати будь-які команди, які можуть змінити конфігурацію самого пристрою. Користувацький режим EXEC ідентифікується за допомогою запиту CLI, який закінчується символом >.
- **Привілейований режим EXEC (Privileged EXEC)** - для виконання команд конфігурації адміністратор мережі повинен отримати доступ до привілейованого режиму EXEC. Режими конфігурації більш високого рівня, як, наприклад, режим глобальної конфігурації, можуть бути доступні лише з привілейованого режиму EXEC. Привілейований режим EXEC може бути визначений підказкою, що закінчується символом # .

У таблиці узагальнено два режими та відображаються підказки CLI за замовчуванням комутатора та маршрутизатора Cisco.

Командний режим	Опис	Командний рядок пристрою за замовчуванням
Користувацький режим EXEC	Забезпечує доступ до обмеженої кількості базових команд моніторингу. Цей режим часто називають режимом “лише для перегляду" .	Switch> Router>
Привілейований режим EXEC	Цей режим дозволяє отримати доступ до всіх команд і функцій. Користувач може використовувати будь-які команди моніторингу, а також має доступ до всіх конфігурацій і команд керування.	Switch# Router#

2.2.2. Режим конфігурації та підрежими конфігурації

Для налаштування пристрою користувач повинен перейти у режим глобальної конфігурації.

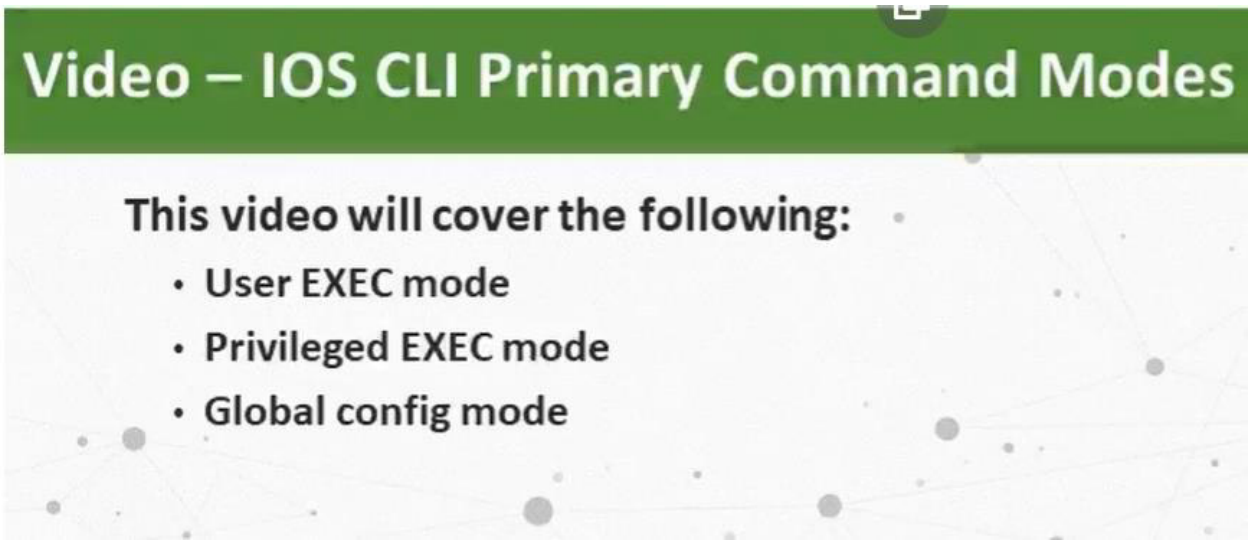
У режимі глобальної конфігурації вносяться зміни конфігурації CLI, які впливають на роботу пристрою в цілому. Режим глобальної конфігурації ідентифікується підказкою, що закінчується (config)# після імені пристрою, наприклад **Switch(config)#**.

Перед тим, як перейти в інші спеціалізовані режими конфігурації, потрібно увійти в режим глобальної конфігурації З режиму глобальної конфігурації користувач може перейти в різні підрежими конфігурації. Кожен з цих режимів дозволяє конфігурувати певну частину або функцію пристрою IOS. Два поширених підрежими конфігурації:

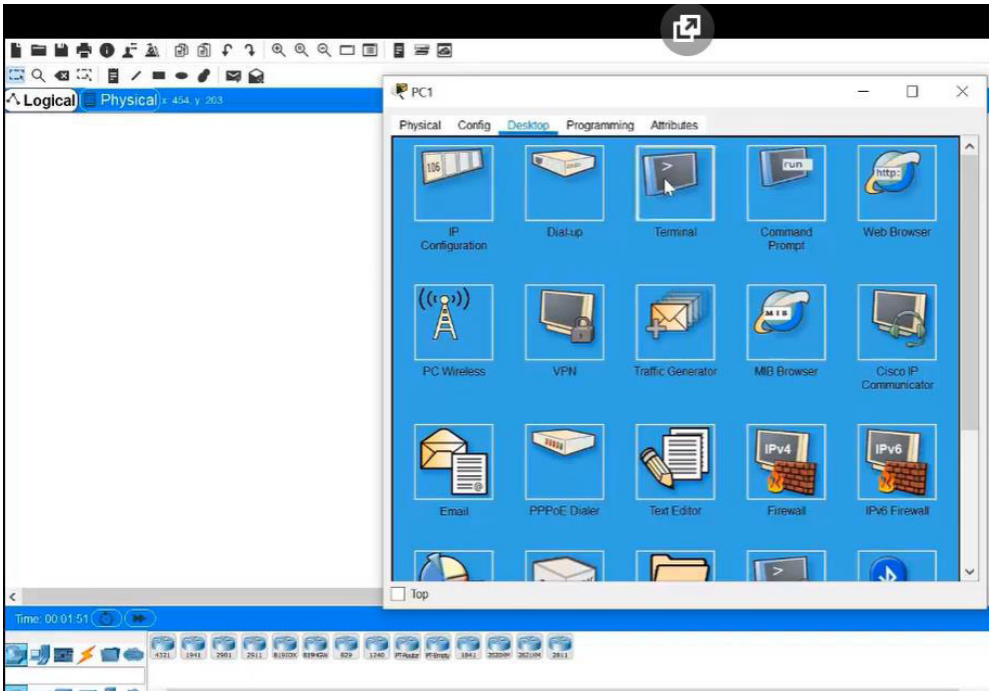
- **Режим конфігурації лінії -** Використовується для налаштування доступу до консолі, SSH, Telnet або AUX.
- **Режим конфігурації інтерфейсу -** Використовується для налаштування порту комутатора або мережного інтерфейсу маршрутизатора.

При використанні CLI режим ідентифікується за допомогою командного рядка, який є унікальним для цього режиму. За замовчуванням кожен запит починається з імені пристрою. Після імені, решта підказки вказує режим. Наприклад, запрошення за замовчуванням для режиму конфігурації лінії **Switch(config-line)#** та запрошення за замовчуванням для режиму конфігурації інтерфейсу **Switch(config-if)#**.

2.2.3. *Відео – Основні режими команд CLI IOS*



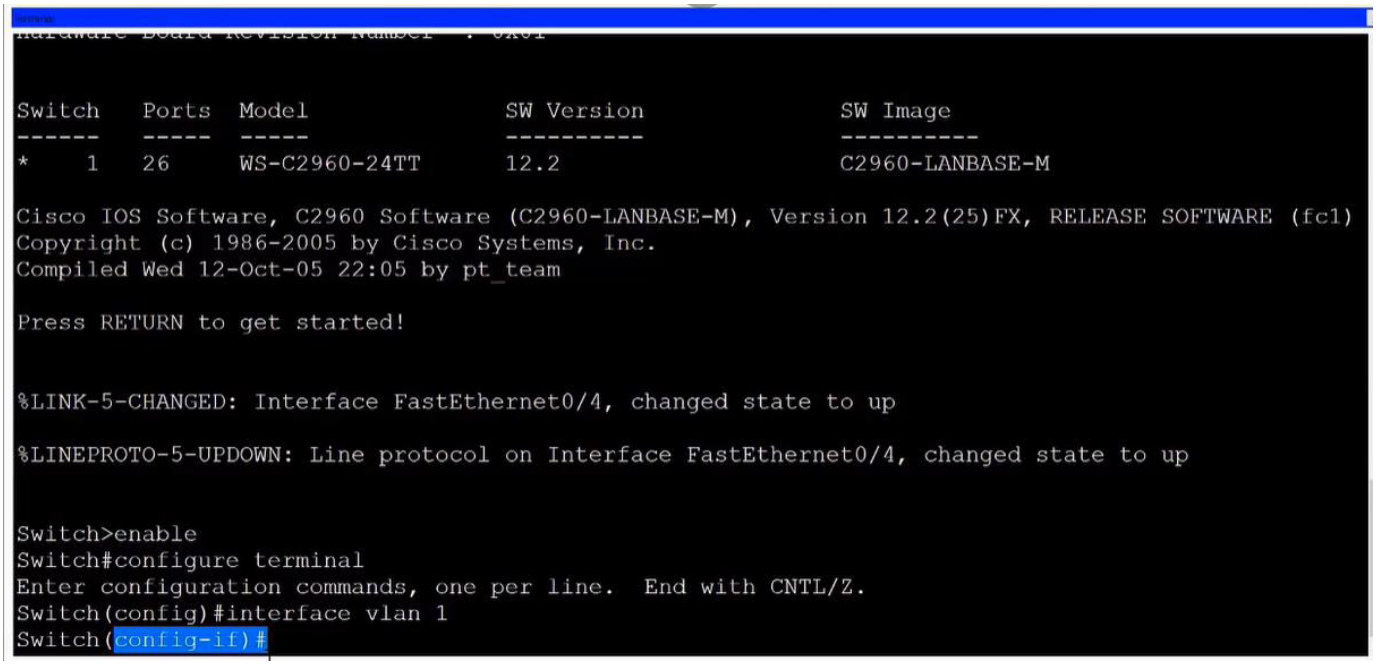
Натискаємо на **PC1 – terminal + Ok:**



+Enter – буде командний режим (command mode)

Switch> enable + Enter (User exact mode)

Switch# (privilege EXEC mode)



(на рис. ми в **interface configuration mode)**

2.2.4. Навігація між режимами IOS

Для переходу між режимами командного рядку використовуються різні команди. Щоб перейти з користувацького режиму EXEC в привілейований, використовуйте команду **enable**. Для повернення в користувацький режим EXEC використовуйте команду привілейованого режиму **disable**.

Примітка: Привілейований режим EXEC іноді називається режимом *enable*.

Щоб перейти в режим глобальної конфігурації і вийти з нього, використовуйте команду **configure terminal** привілейованого режиму EXEC. Щоб повернутися до привілейованого режиму EXEC, введіть команду **exit** режиму глобальної конфігурації.

Існує багато різних підрежимів конфігурації. Наприклад, для входу в підрежим конфігурації лінії ви використовуєте команду **line**, за якою слідує тип і номер лінії керування, до якої ви хочете отримати доступ. Для виходу з підрежиму конфігурації та повернення в режим глобальної конфігурації використовуйте команду **exit**.

```
Switch(config)# line console 0
```

```
Switch(config-line)# exit
```

```
Switch(config)#
```

Щоб перейти з будь-якого підрежиму конфігурації в рамках режиму глобальної конфігурації на один рівень вище в ієрархії режимів, введіть команду **exit**.

Щоб перейти з будь-якого підрежиму конфігурації в привілейований режим EXEC, введіть команду **end** або введіть комбінацію клавіш **Ctrl+Z**.

```
Switch(config-line)# end
```

```
Switch#
```

Також можна переходити безпосередньо з одного підрежиму конфігурації в інший. Зверніть увагу, що після вибору інтерфейсу командний рядок змінюється з **(config-line)#** на **(config-if)#**.

```
Switch(config-line)# interface FastEthernet 0/1
```

```
Switch(config-if)#
```

2.2.5 Відео - Навігація між режимами IOS

Рисунок демонструє перехід між різними режимами CLI в IOS

Video – Navigate between IOS Modes

This video will cover the following:

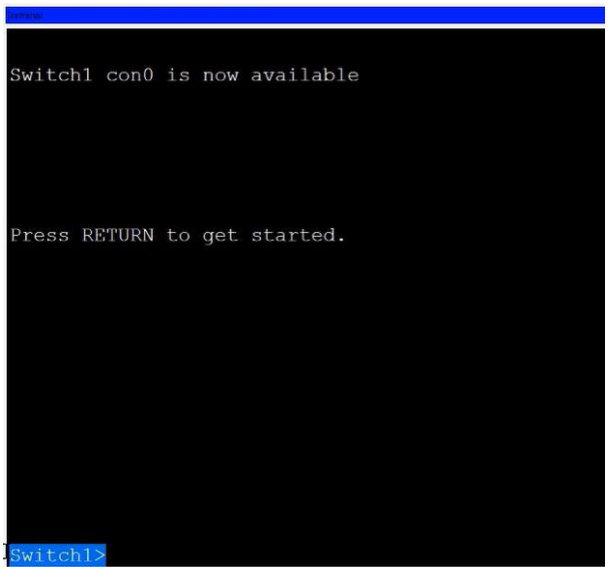
- enable
- disable
- configure terminal
- exit
- end
- Control + Z on keyboard
- Other commands to enter sub configuration modes

PC is connected with consol cable to switch1

Navigate Between IOS Modes

enable
disable
configure terminal
exit
end
Ctrl+Z
line console 0
line vty 0 15
interface vlan 1

Click on PC1 + press Enter (входимо в USER EXEC mode)




```
Switch1>enable
Switch1#disable
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#exit
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#exit
```

Switch1#exit - Live consol connection.

Enter – знову підключаємось до консолі:

```
Switch1>enable
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#
```

Ми в global config mode.

Sub config mode : **line console 0**

```
Switch1>enable
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line console 0
Switch1(config-line)#
```

#End or ctrl+z (+Enter) – вийти з під режиму вище в привілейований **privileged (enable) EXEC mode**

Так пробуємо різними варіантами по колу декілька разів:

```
Switch1(config-if)#line console 0
Switch1(config-line)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line console 0
Switch1(config-line)#^Z
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#
```

2.2.6. Примітка про інструмент перевірки синтаксису Syntax Checker

Коли ви вивчаєте, як змінювати конфігурації пристрою, ви можете почати роботу в безпечному невиробничому середовищі, перш ніж робити це на реальному обладнанні. NetAcad надає вам різні інструменти моделювання, які допоможуть вам отримати навички налаштування і усунення несправностей. Оскільки це інструменти для моделювання, вони, як правило, не мають усієї функціональності реального обладнання. Одним із таких інструментів є перевірка синтаксису (Syntax Checker). У кожному завданні перевірки синтаксису вам надається набір інструкцій для введення певного набору команд. Ви не можете просуватись у програмі перевірки синтаксису, якщо не буде введено точну та повну команду, як зазначено. Більш досконалі інструменти моделювання, такі як **Packet Tracer, дозволяють вводити скорочені команди, як і на реальному обладнанні.**

2.2.7. *Перевірка синтаксису – Навігація між режимами IOS*

Використовуйте Syntax Checker для переміщення між командними рядками IOS на комутаторі.

```
Switch> enable
```

Увійдіть у режим глобальної конфігурації, використовуючи команду **configure terminal**.

```
Switch# configure t
Команди потрібно вводити повністю і точно.
Switch# configure terminal
```

Вийдіть із режиму глобальної конфігурації та поверніться до привілейованого режиму EXEC за допомогою команди **exit**.

```
Switch(config)#
```

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

З режиму конфігурації інтерфейсу перейдіть до режиму підконфігурації лінії консолі за допомогою команди глобальної конфігурації **line console 0**.

```
Switch(config-if)# line console 0
```

Поверніться в привілейований режим EXEC за допомогою команди **end**.

```
Switch(config-line)# end

Ви успішно переключалися між різними режимами командного рядка IOS.
```

2.2.8. *Питання для самоперевірки - Навігація в IOS*

1. Який режим IOS дозволяє отримати доступ до всіх команд та функцій?

- ◯ Режим глобальної конфігурації
- ◯ Підрежим конфігурації інтерфейсу
- ◯ Підрежим конфігурації лінії консолі
- ◯ Привілейований режим EXEC
- ◯ Користувацький режим EXEC

2. У якому режимі IOS ви перебуваєте, якщо відображається підказка Switch(config)#?

- ◯ Режим глобальної конфігурації
- ◯ Режим підконфігурації інтерфейсу
- ◯ Режим підконфігурації консольної лінії
- ◯ Привілейований режим EXEC
- ◯ Користувацький режим EXEC

3. У якому режимі IOS ви перебуваєте, якщо відображається підказка Switch>?

- ◯ Режим глобальної конфігурації
- ◯ Підрежим конфігурації інтерфейсу
- ◯ Підрежим конфігурації консольної лінії
- ◯ Привілейований режим EXEC
- ◯ Користувацький режим EXEC

4. Які дві команди повернуть вас до запиту привілейованого режиму EXEC незалежно від режиму конфігурації, в якому ви перебуваєте? (Оберіть два варіанти.)

- ☐ **CTRL+Z**
- ☐ **disable**
- ☐ **enable**
- ☐ **end**
- ☐ **exit**

1. Який режим IOS дозволяє отримати доступ до всіх команд та функцій?

Правильно!

- ○ Режим глобальної конфігурації
- ○ Підрежим конфігурації інтерфейсу
- ○ Підрежим конфігурації лінії консолі
- ◉ Привілейований режим EXEC
- ○ Користувацький режим EXEC

2. У якому режимі IOS ви перебуваєте, якщо відображається підказка Switch(config)#?

Правильно!

- ◉ Режим глобальної конфігурації
- ○ Режим підконфігурації інтерфейсу
- ○ Режим підконфігурації консольної лінії
- ○ Привілейований режим EXEC
- ○ Користувацький режим EXEC

3. У якому режимі IOS ви перебуваєте, якщо відображається підказка Switch>?

Правильно!

- ○ Режим глобальної конфігурації
- ○ Підрежим конфігурації інтерфейсу
- ○ Підрежим конфігурації консольної лінії
- ○ Привілейований режим EXEC
- ◉ Користувацький режим EXEC

4. Які дві команди повернуть вас до запиту привілейованого режиму EXEC незалежно від режиму конфігурації, в якому ви перебуваєте? (Оберіть два варіанти.)

Правильно!

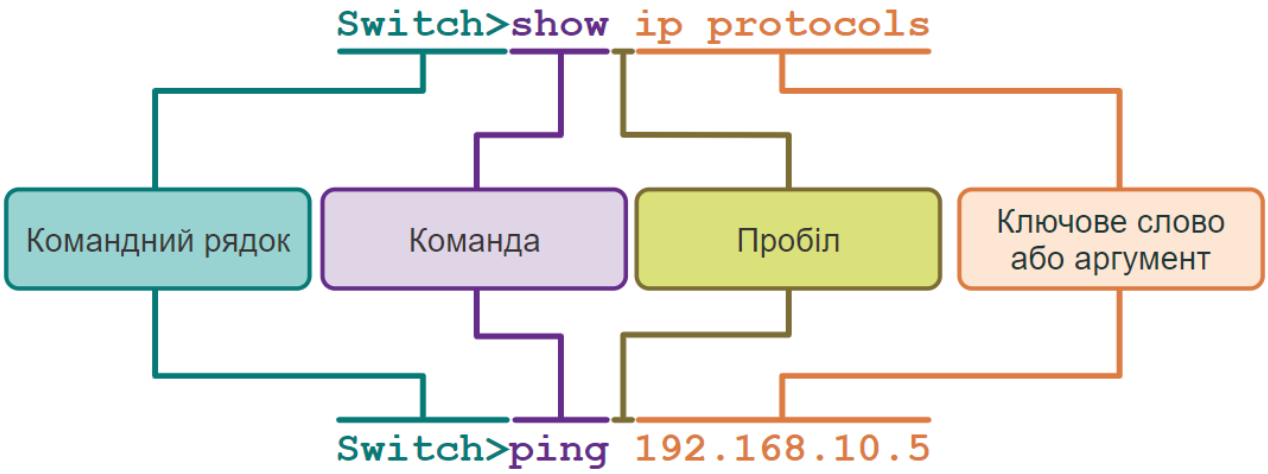
- ☑ **CTRL+Z**
- ☐ **disable**
- ☐ **enable**
- ☑ **end**
- ☐ **exit**

2.3. Структура команд

2.3.1. Базова структура команд IOS

Ця тема охоплює основну структуру команд для IOS Cisco. Адміністратор мережі повинен знати основну структуру команд IOS, щоб мати можливість використовувати інтерфейс командного рядка (CLI) для конфігурації пристрою.

Пристрій Cisco IOS підтримує безліч команд. Кожна команда IOS має певний формат або синтаксис і може виконуватися лише у відповідному режимі. Загальний синтаксис команди, показаний на рисунку, - це команда, за якою слідують всі відповідні ключові слова і аргументи.



- **Ключове слово** – це специфічний параметр, визначений в операційній системі (на рисунку, **ip protocols**).
- **Аргумент** – це значення або змінна, визначена користувачем (на рисунку, **192.168.10.5**).

Після введення кожної повної команди, включаючи будь-які ключові слова та аргументи, натисніть клавішу **Enter**, щоб подати команду інтерпретатору команд.

2.3.2. Перевірка синтаксису команд IOS

Команда може вимагати одного або декількох аргументів. Щоб визначити ключові слова та аргументи, необхідні для команди, зверніться до синтаксису команд. Синтаксис надає шаблон або формат, який необхідно використовувати при введенні команди.

Як визначено в таблиці, текст жирним шрифтом позначає команди та ключові слова, які вводяться як показано. Курсивом виділено аргумент, значення якого надає користувач.

Заголовок таблиці	
Умовне позначення	**Опис**
напівжирний	Напівжирним шрифтом виділені команди і ключові слова, які ви вводите буквально як показано.
курсив	Курсивом відображаються аргументи, для яких потрібно вказати значення.

Заголовок таблиці	
Умовне позначення	**Опис**
[x**]**	В квадратних дужках відображаються додаткові елементи (ключове слово або аргумент).
{x}	У фігурних дужках вказується необхідний елемент, такий як ключове слово або аргумент.
[x {y | z **}]**	Фігурні дужки і вертикальні лінії у квадратних дужках вказують на те, що необхідно обрати додатковий елемент. Пробіли використовуються для чіткого розмежування частин команди.

Наприклад, синтаксис використання **description** команди **description** *string*. Аргумент - значення *string*, надане користувачем. Команда **description** зазвичай використовується для опису призначення інтерфейсу. Наприклад, команда **description Connects to the main headquarter office switch** (Під'єднання до комутатора головного офісу) визначає, де знаходиться інший пристрій на кінці з'єднання.

Нижче представлені приклади умовних позначень для документування та використання команд IOS:

- **ping** *ip-address* - команда **ping**, а визначений користувачем аргумент - це ip-адреса пристрою призначення. Наприклад, **ping 10.10.10.5**.
- **traceroute** *ip-address* - команда **traceroute**, а визначений користувачем аргумент - це ip-адреса пристрою. Наприклад, **traceroute 192.168.254.254**.

Якщо команда складна, з декількома аргументами, її можна представити таким чином:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Команда зазвичай супроводжується докладним описом команди і кожного аргументу.

Довідник по командам Cisco IOS є основним джерелом інформації для конкретної команди IOS.

2.3.3 Функції довідки IOS

У IOS доступні дві форми надання довідкової інформації: контекстна допомога та перевірка синтаксису команд.

Контекстна допомога дозволяє швидко знайти відповіді на такі запитання:

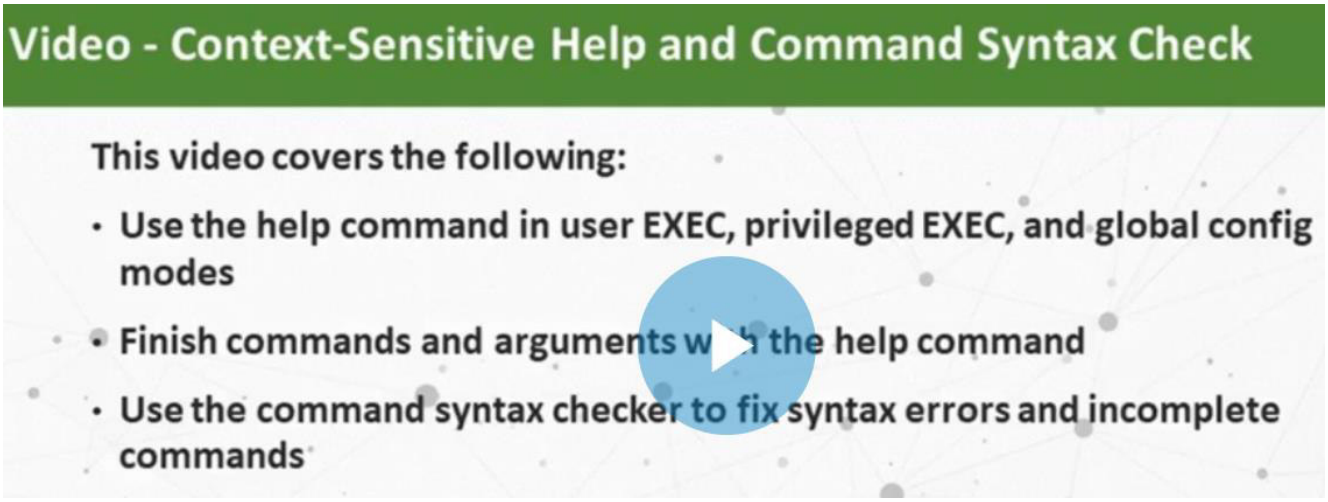
- Які команди доступні в кожному режимі команд?
- Які команди починаються з конкретних символів або групи символів?
- Які аргументи та ключові слова доступні для певних команд?

Для доступу до контекстної допомоги просто введіть знак питання, **?**, у командному рядку CLI.

Перевірка синтаксису команд підтверджує, що користувачем було введено дійсну команду. Коли команда введена, інтерпретатор командного рядка оцінює команду зліва направо. Якщо інтерпретатор розуміє команду, запитувана дія виконується, і інтерфейс CLI повертається у відповідний запит. Однак якщо інтерпретатор не може зрозуміти введену команду, він надасть зворотній зв'язок із описом помилок.

2.3.4. Відео - Контекстна довідка та перевірка синтаксису команд

Демонструє контекстно-залежну довідку та перевірку синтаксису команд.



2.3.5. Гарячі клавіші та ярлики

Інтерфейс командного рядка (CLI) в IOS підтримує використання гарячих клавіш та ярликів, які спрощують налаштування, моніторинг та усунення несправностей.

Команди та ключові слова можна скоротити до мінімальної кількості символів, які однозначно ідентифікують обрану команду чи слово. Наприклад, команду **configure** можна скоротити до **conf** оскільки **configure** є єдиною командою, яка починається з **conf**. Скорочення **con** використовувати не можна, так як з символів **con** починається кілька команд. Ключові слова також можна скоротити.

У таблиці перелічені комбінації клавіш для вдосконалення редагування командного рядка.

Заголовок таблиці	
Комбінація клавіш	**Опис**
Tab	Завершує частковий запис команди.
Backspace	Стирає символ зліва від курсору.
Ctrl+D	Стирає символ за курсором.
Ctrl+K	Стирає всі символи від курсору до кінця командного рядка.
Esc D	Стирає всі символи від курсору до кінця слова.
Ctrl+U або **Ctrl+X**	Стирає всі символи перед курсором до початку командного рядка.
Ctrl+W	Стирає слово зліва від курсору.
Ctrl+A	Переміщує курсор на початок рядка.
Стрілка ліворуч або **Ctrl+B**	Переміщує курсор на один символ ліворуч.
Esc B	Переміщує курсор на одне слово ліворуч.

Заголовок таблиці	
Комбінація клавіш	**Опис**
Esc F	Переміщує курсор на одне слово праворуч.
Стрілка праворуч або **Ctrl+F**	Переміщує курсор на один символ праворуч.
Ctrl+E	Переміщує курсор до кінця командного рядка.
Стрілка вгору або **Ctrl+P**	Повторює команду в буфері історії, починаючи з останніх команд.
Ctrl+R або **Ctrl+I** або **Ctrl+L**	Повторно відкриває командний рядок системи після того, як консольне повідомлення отримано.

Примітка: Хоча клавіша **Delete** зазвичай видаляє символ праворуч від підказки, командна структура IOS не розпізнає клавішу Delete.

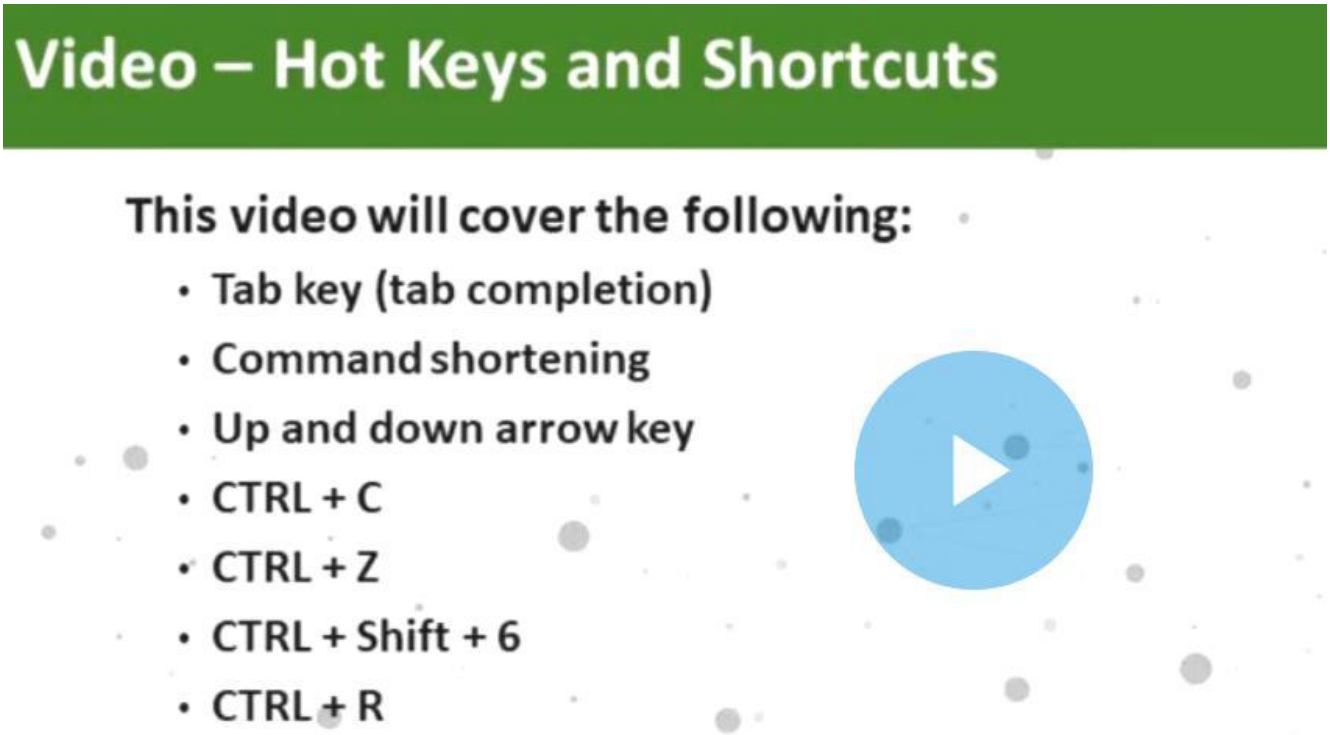
Коли результат виконання команди повертає більше тексту, ніж можна відобразити у вікні терміналу, IOS відобразить запрошення **"--More--"**. У таблиці нижче описано комбінації клавіш, які можна використовувати в такому випадку.

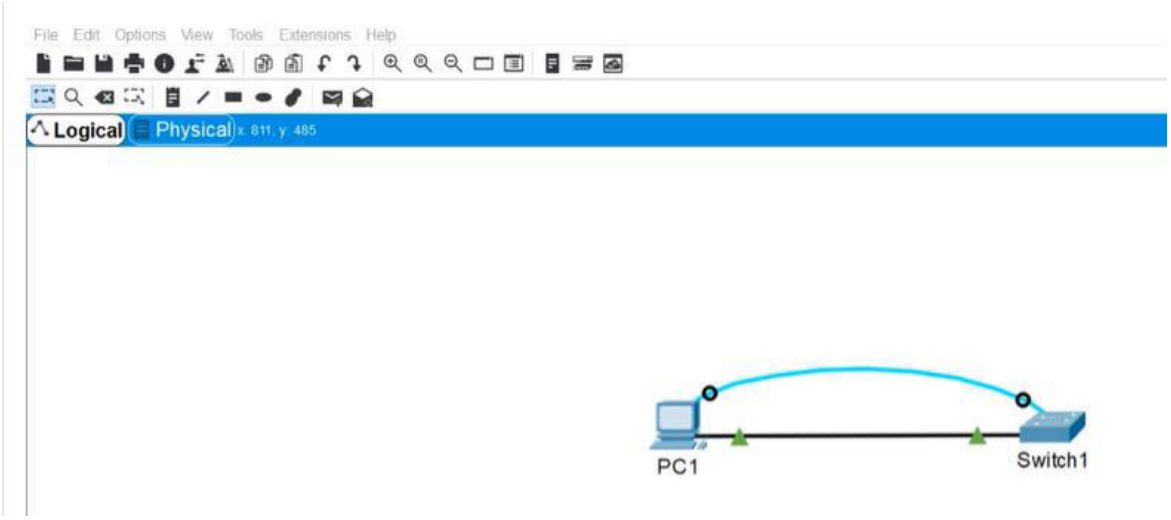
Заголовок таблиці	
Комбінація клавіш	**Опис**
Клавіша **Enter**	Відображає наступний рядок.
Клавіша **Пробіл**	Відображає наступний екран.
Будь-яка інша клавіша	Закінчує рядок, повертаючись у привілейований режим EXEC.

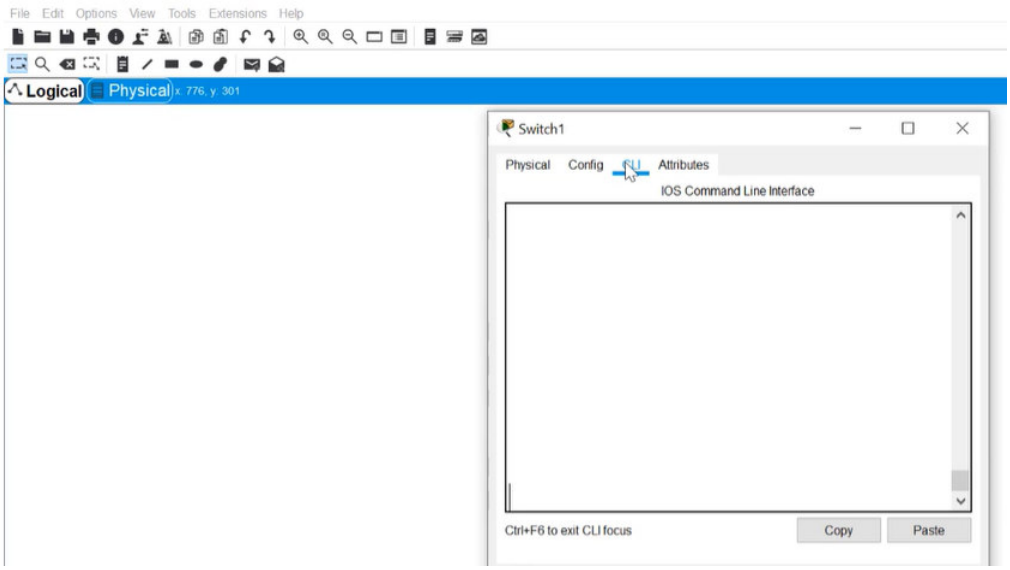
У таблиці нижче наведені команди, які можна використовувати для виходу з режиму.

Заголовок таблиці	
Комбінація клавіш	**Опис**
Ctrl+C	У будь-якому режимі конфігурації завершує цей режим та повертається у привілейований режим EXEC. Перебуваючи в режимі налаштування, повертається до командного рядка.
Ctrl+Z	У будь-якому режимі конфігурації завершує цей режим та повертається у привілейований режим EXEC.
Ctrl+Shift+6	Універсальна послідовність для переривань, яка використовується для припинення пошуку DNS-каналів, трасування, пінгування, тощо.

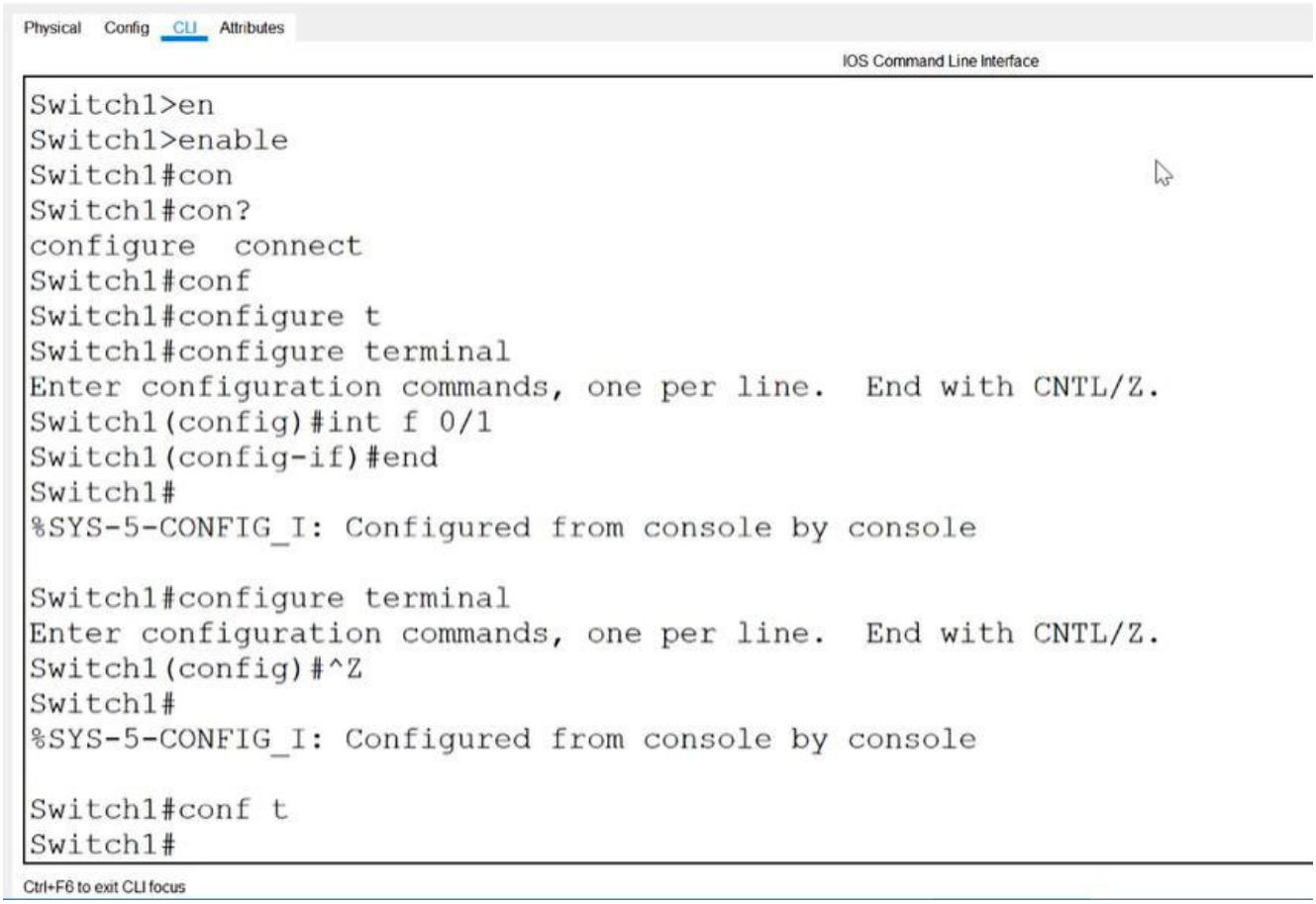
2.3.6. *Гарячі клавіші та ярлики*





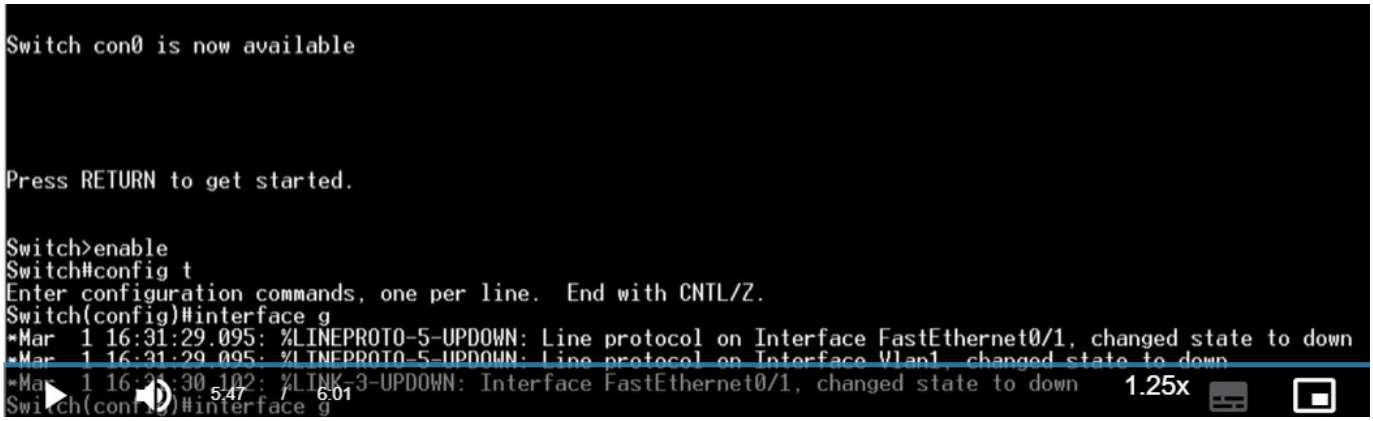


Cli + Enter (емуляція командного рядка для комутатора)



Щоб відмінити неправильну команду: ctrl+shift+6 (commant aboarded)

Ctrl+R (повернутися на 1 дію назад)



З передостаннього рядка повернулися до 5-го знизу.

2.3.7. *Packet Tracer - Навігація в IOS (практична робота)*

У цьому завданні ви отримаєте практичні 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 контекстно-залежною довідки, налаштувавши команду clock.

Networking Academy

Packet Tracer - 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.

8) IOS надає різні вихідні дані для неправильних або неповних команд. Продовжуйте використовувати команду **clock**, щоб вивчити інші повідомлення, які можуть зустрітися при використанні IOS.

9) 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?

2.3.8. *Лабораторна робота - Навігація в IOS з використанням Tera Term для консольного під'єднання*

В цій лабораторній роботі ви виконаєте наступні завдання:

- Частина1: Доступ до комутатора Cisco через консольний порт
- Частина2: Відображення та налаштування основних параметрів пристрою
- Частина3: (Додатково) Отримання доступу до маршрутизатора Cisco за допомогою консольного кабелю Mini-USB

Networking Academy

Лабораторна робота - Навігація в IOS з використанням Tera Term для консольного під'єднання

Топологія

Цілі та задачі

Частина 1: Доступ до комутатора Cisco через консольний порт

Частина 2: Відображення та налаштування основних параметрів пристрою

Частина 3: (Додатково) Отримання доступу до маршрутизатора Cisco за допомогою консольного кабелю Mini-USB

Примітка: Користувачі NetLab або інші, що використовують обладнання віддаленого доступу, повинні заповнити лише частину 2.

Довідкова інформація / Сценарій

У мережах усіх типів застосовуються різні моделі маршрутизаторів і комутаторів Cisco. Цими пристроями керують за допомогою під'єднання до локального консольного порту або віддаленого з'єднання. Майже на всіх пристроях Cisco є послідовний консольний порт, до якого можна під'єднатися. Новіші моделі, що використовуються в цій лабораторній роботі, наприклад Cisco 4221, також мають USB-консольний порт.

У цій лабораторній роботі ви дізнаєтесь, як отримати доступ до пристрою Cisco через пряме локальне під'єднання до консольного порту, використовуючи програму емуляції терміналів Tera Term. Ви також дізнаєтесь, як налаштувати параметри послідовного порту для під'єднання консолі через Tera Term. Після встановлення консольного з'єднання з пристроєм Cisco, ви можете відобразити або налаштувати параметри пристрою. В цій лабораторній роботі Ви будете тільки відображати параметри і налаштовувати годинник.

Примітка: Маршрутизатори, що використовуються в практичних лабораторних роботах CCNA, - це Cisco 4221 під керуванням Cisco IOS XE Release 16.9.3 (образ universalk9). Комутатори, які використовуються в лабораторних роботах - це Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Також можна використовувати інші маршрутизатори, комутатори та версії Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що показані в лабораторних роботах. Правильні ідентифікатори інтерфейсу див. у кінці лабораторної роботи в підсумковій таблиці інтерфейсів маршрутизатора.

Примітка: Переконайтесь, що налаштування на маршрутизаторах та комутаторах були видалені та пристрої не мають початкових конфігурацій. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 1 Маршрутизатор (Cisco 4221 з Cisco IOS XE версія 16.9.3 образ universal або аналогічний)

Лабораторна робота - Навігація в IOS з використанням Tera Term для консольного під'єднання

- 1 Комутатор (Cisco 2960 з Cisco IOS версія 15.0(2) образ lanbasek9 або аналогічний)
- 1 ПК (Windows 10 з програмою емуляції терміналу, наприклад, Tera Term)
- Консольний кабель (DB-9 до RJ-45) для налаштування комутатора або маршрутизатора через консольний порт RJ-45
- Міні-USB-кабель для налаштування маршрутизатора через USB-порт консолі

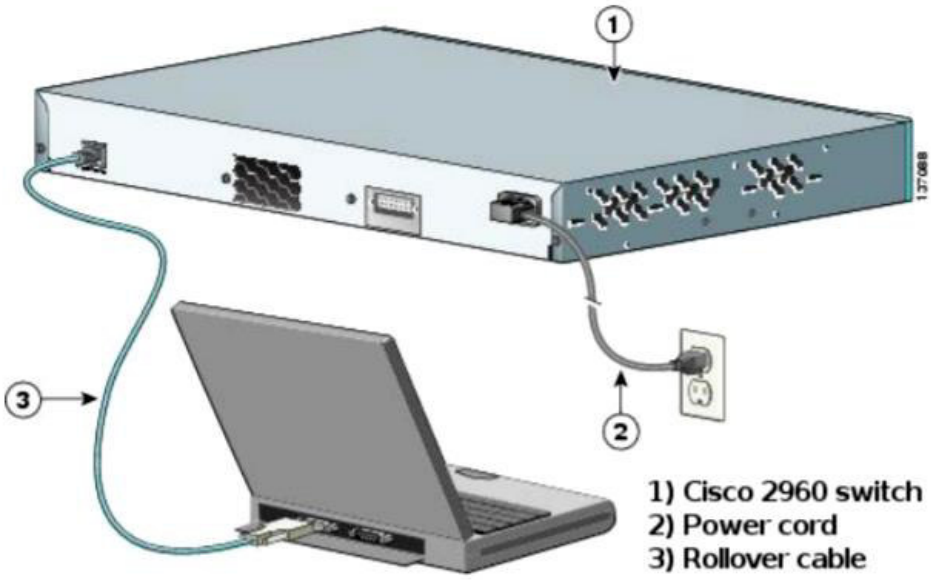
Інструкції

Частина 1: Доступ до комутатора Cisco через консольний порт

Ви під'єднаєте ПК до комутатора Cisco за допомогою консольного кабелю. Це з'єднання дозволить отримати доступ до інтерфейсу командного рядка (CLI) та відобразити параметри або налаштувати комутатор.

Крок 1: З'єднайте комутатор Cisco та комп'ютер за допомогою консольного кабелю.

a. Під'єднайте консольний кабель до консольного входу RJ-45 комутатора. Під'єднайте інший кінець кабелю до послідовного COM-порту на комп'ютері.



Примітка: На більшості комп'ютерів послідовні COM-порти наразі відсутні. Для консольного з'єднання між комп'ютером та пристроєм Cisco можна використовувати адаптер USB-DB9 разом з консольним кабелем. Такі адаптери можна придбати в будь-якому роздрібному магазині електроніки.

Примітка: Якщо для під'єднання до порту COM використовується адаптер USB-DB9, можливо, вам потрібно буде встановити драйвер для адаптера, наданий виробником вашого комп'ютера. Щоб визначити COM-порт, який використовується адаптером, див. Частину 3 Крок 3. Правильний номер COM-порту потрібен для під'єднання до пристрою Cisco IOS за допомогою емулятора терміналу на кроці 2.

2.4. Базові налаштування пристрою

2.4.1. Імена пристроїв

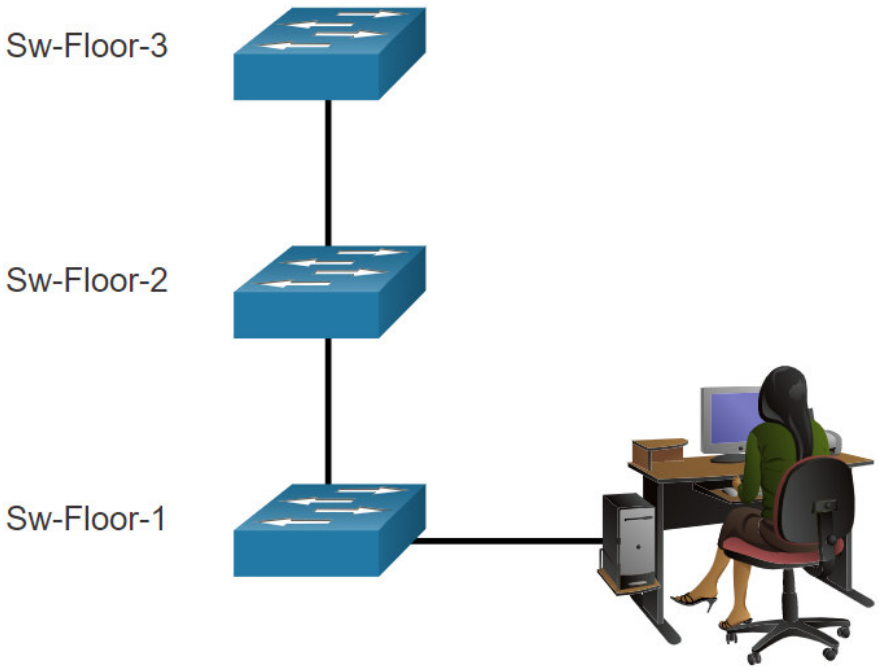
Ви багато дізналися про IOS Cisco, навігацію по IOS та структуру команд. Тепер ви готові налаштовувати пристрої! Першою командою налаштування на будь-якому пристрої має бути присвоєння йому унікального імені пристрою або імені вузла. За замовчуванням, всім пристроям присвоєне заводське ім'я за замовчуванням. Наприклад, у комутатора Cisco IOS ім'я "Switch”

Проблема полягає в тому, що якщо всі комутатори в мережі залишилися зі своїми іменами за замовчуванням, було б важко визначити конкретний пристрій. Наприклад, як ви дізнаєтеся, що ви під'єднані до потрібного пристрою при віддаленому доступі до нього по SSH? Ім'я вузла підтверджує, що ви під'єднані до правильного пристрою.

Ім'я за замовчуванням слід змінити на щось більш описове. Розумний вибір імен полегшує запам'ятовування, документування та ідентифікацію мережних пристроїв. Ось кілька важливих рекомендацій щодо іменування для вузлів:

- Починати імена з літери
- Не використовувати пробіли
- Закінчувати літерою або цифрою
- Використовувати лише літери, цифри і тире
- Мати довжину не більше 64 символів

Організація повинна вибрати конвенцію про іменування, яка дозволяє легко та інтуїтивно визначити конкретний пристрій. Імена вузлів, які використовуються в пристроях IOS, зберігають великі та малі літери. Наприклад, на рисунку видно, що три комутатори, що охоплюють три різні поверхи, з'єднані між собою в мережу. Конвенція про іменування, яка використовувалась, містила місце розташування та призначення кожного пристрою. Мережна документація повинна пояснювати, як були обрані ці імена, щоб додаткові пристрої могли бути названі відповідно.



Коли мережні пристрої мають імена, їх легко ідентифікувати для цілей конфігурації.

Коли угоду про імена визначено, наступним кроком є використання інтерфейсу командного рядка для застосування імен до пристроїв. Як показано в прикладі, у привілейованому режимі EXEC перейдіть до режиму глобальної конфігурації, ввівши команду **configure terminal**. Зверніть увагу на командний рядок.

```
Switch# configure terminal
```

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

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

У режимі глобальної конфігурації введіть команду **hostname** , а потім ім'я комутатора та натисніть **Enter**. Зверніть увагу на зміну імені у командному рядку.

Примітка: Щоб повернути комутатор до запрошення за замовчуванням, використовуйте команду глобальної конфігурації **no hostname**.

Завжди перевіряйте, чи оновлюється документація при кожному додаванні або зміні пристрою. У цій документації пристроям повинно бути присвоєно розташування, призначення та адреса.

2.4.2. Правила вибору паролів

Використання слабких або легко вгадуваних паролів продовжує залишатися найбільшою проблемою безпеки організацій. Мережні пристрої, включаючи домашні бездротові маршрутизатори, завжди повинні налаштовуватися з паролем для обмеження адміністративного доступу.

В Cisco IOS можна налаштувати паролі ієрархічних режимів, щоб дозволити різні права доступу до мережного пристрою.

Усі мережні пристрої повинні обмежувати адміністративний доступ, встановлюючи захищений паролями доступ до привілейованого та користувацького EXEC режимів, віддаленого доступу до Telnet. Крім того, всі паролі повинні бути зашифровані, та встановлене сповіщення про обмеження доступу.

При виборі паролів використовуйте надійні паролі, які важко вгадати. Враховуйте наступні ключові моменти при виборі паролів:

- Використовуйте паролі довжиною більше восьми символів.
- Використовуйте комбінацію великих і малих літер, цифр, спеціальних символів та/або числових послідовностей.
- Уникайте використання однакового пароля для всіх пристроїв.
- Не вживайте загальних слів, тому що їх легко вгадати.

Використовуйте пошук в Інтернеті, щоб знайти генератор паролів. Багато з них дозволять вам встановити довжину, набір символів і інші параметри.

Примітка: В більшості лабораторних робіт цього курсу використовуються прості паролі, такі як **cisco** або **class**. Ці паролі вважаються слабкими і легко вгадуваними, тому їх слід уникати у виробничих умовах. Ми використовуємо ці паролі лише для зручності в класі або для ілюстрації прикладів конфігурації.

2.4.3. Налаштування паролів

Коли ви спочатку під'єднуєтесь до пристрою, ви перебуваєте в користувацькому режимі EXEC. Цей режим захищається за допомогою консолі.

Для безпечного доступу в користувацькому режимі EXEC, увійдіть в режимі конфігурації консольної лінії за допомогою команди глобальної конфігурації **line console 0**, як показано в прикладі. Нуль використовується для представлення першого (і в більшості випадків єдиного) консольного інтерфейсу. Далі встановіть пароль користувацького режиму EXEC, використовуючи команду **password** *password*. Нарешті, активуйте доступ до користувацького режиму EXEC, використовуючи команду **login**.

```
Sw-Floor-1# configure terminal
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)# end
Sw-Floor-1#
```

Тепер для доступу до користувацького режиму EXEC з консолі необхідно ввести пароль.

Щоб мати доступ адміністратора до всіх команд IOS, включаючи налаштування пристрою, ви повинні отримати доступ в привілейований режим EXEC. Це найважливіший метод доступу, оскільки він забезпечує повний доступ до пристрою.

Щоб забезпечити захист доступу до привілейованого режиму EXEC, використовуйте команду глобальної конфігурації **enable secret** *password*, як показано в прикладі.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Лінії віртуального терміналу (VTY) забезпечують віддалений доступ до пристрою за допомогою Telnet або SSH. Багато комутаторів Cisco підтримують до 16 ліній VTY, які пронумеровані від 0 до 15.

Щоб захистити лінії VTY, увійдіть у режим лінії VTY за допомогою команди глобальної конфігурації **line vty 0 15**. Далі вкажіть пароль VTY за допомогою команди **password** *password* . Нарешті, активуйте доступ до VTY, використовуючи команду **login**.

Нижче наведено приклад захисту ліній VTY на комутаторі.

```
Sw-Floor-1# configure terminal
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)# end
Sw-Floor-1#
```

2.4.4. Шифрування паролів

Файли startup-config та running-config відображають більшість паролів у форматі відкритого тексту. Це загроза безпеці, оскільки будь-хто може побачити паролі, якщо має доступ до цих файлів.

Для шифрування всіх паролів у вигляді відкритого тексту використовуйте команду глобальної конфігурації **service password-encryption**, як показано в прикладі.

```
Sw-Floor-1# configure terminal

Sw-Floor-1(config)# service password-encryption

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

Команда застосовує слабкий алгоритм шифрування до всіх незашифрованих паролів. Це шифрування стосується лише паролів у файлі конфігурації, а не паролів, коли вони надсилаються по мережі. Мета цієї команди - запобігти сторонній особі переглянути паролі у файлі конфігурації.

Використовуйте команду **show running-config**, щоб перевірити, що паролі тепер зашифровані.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
login
!
!
end
```

2.4.5. Банерне повідомлення

Хоча вимога паролів є одним із способів захистити від несанкціонованого доступу в мережу, вкрай важливо забезпечити спосіб оголошення того, що тільки авторизований персонал може

отримати доступ до пристрою. Для цього додайте банер до вихідних даних пристрою. Банери можуть бути важливою складовою юридичного процесу в тому випадку, якщо когось притягують до кримінальної відповідальності за несанкціонований доступ. Окремі законодавства не дозволяють порушувати судові справи проти користувачів або навіть просто стежити за їхніми діями без попередження.

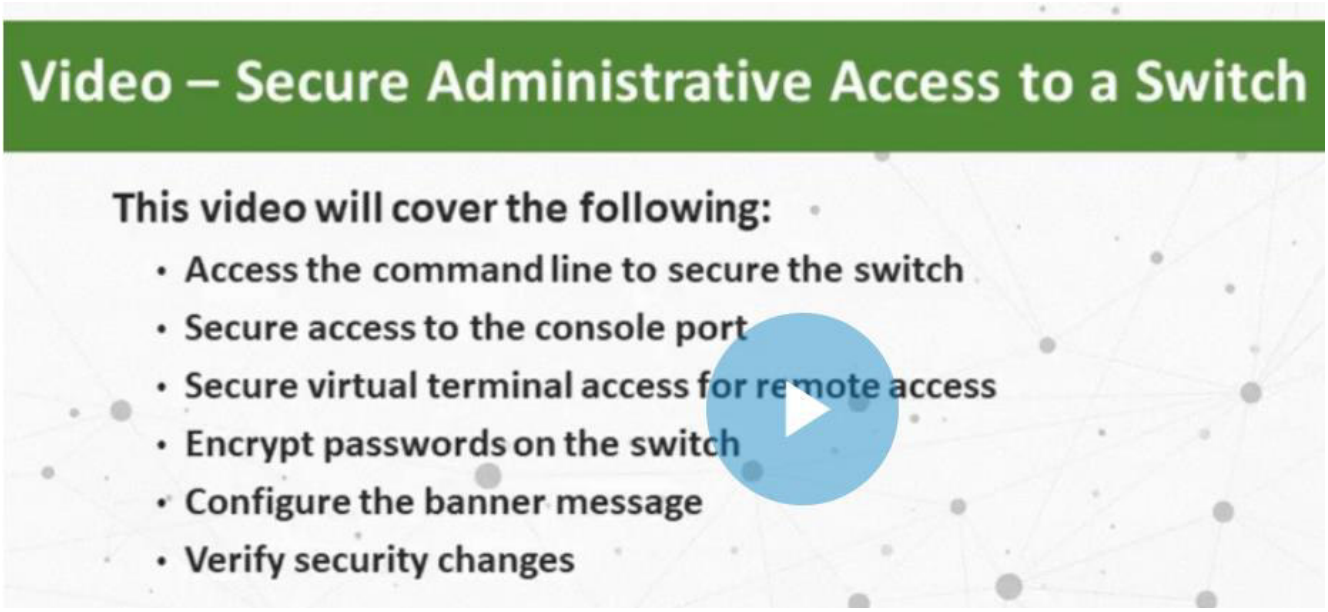
Щоб створити банерне повідомлення дня на мережному пристрої, використовуйте команду глобальної конфігурації **banner motd #** *the message of the day* **#**. Символ "#" у синтаксисі команд називається символом розмежування. Він вводиться до і після повідомлення. Символом-роздільником може бути будь-який символ, якщо він не присутній в повідомленні. З цієї причини часто використовуються такі символи, як #. Після виконання команди банер буде відображатися при всіх наступних спробах доступу до пристрою, поки не буде видалений.

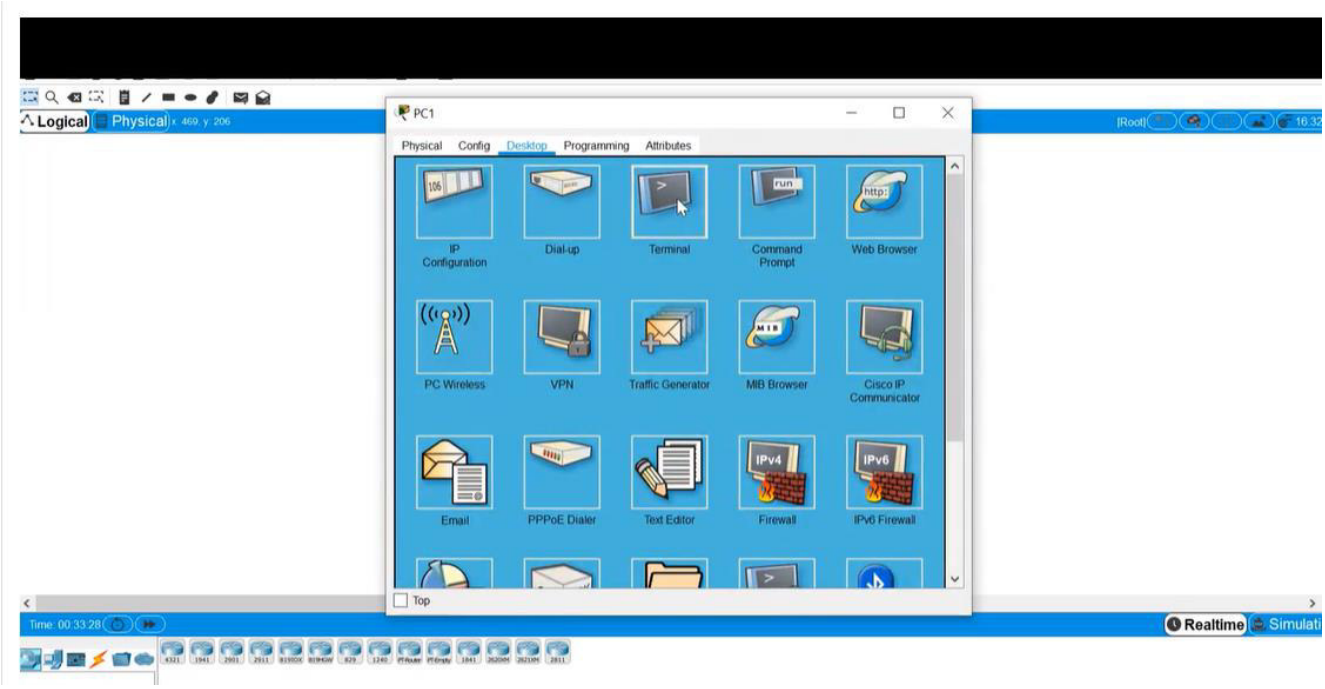
Наступний приклад показує кроки налаштування банера на Sw-Floor-1.

```
Sw-Floor-1# configure terminal
```

```
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6. *Захист адміністративного доступу до комутатора*





+Enter (без пароля доступ до командного рядку, в тому числі до привіледж мод):

```
Switch1 con0 is now available



Press RETURN to get started.









Switch1>enable
Switch1#
```

```
Switch1>enable
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config)#enable secret class
Switch1(config)#
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#exit
```

+Enter (Exit the switch)

```
Switch1 con0 is now available



Press RETURN to get started.
```

+Enter

```
User Access Verification

Password:
```

Вже просить пароль. Перевіримо

```
User Access Verification

Password:

Switch1>enable
Password:
Switch1#show running-config
```

```
Switch1#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
 --More--
```

Якщо натиснути пробіл на клавіатурі:

```
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


Switch1#
```

Покаже пароль без шифру. Це теж можна виправити.

```
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#
```

Ctrl+c (to get the privilege mode)

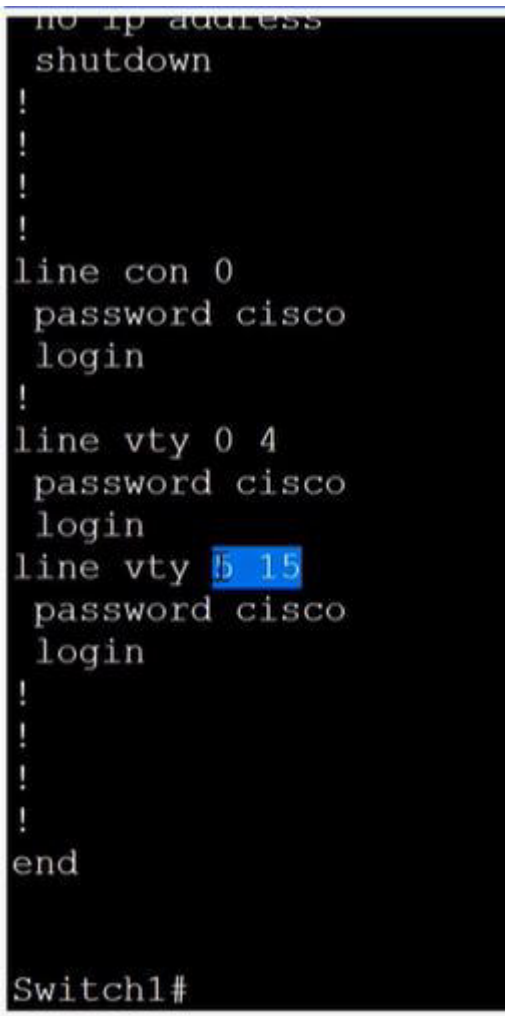
Show run (побачити запущену конфігурацію)

```
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#show run
```

Буде:

```
Building configuration...

Current configuration : 1183 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
 --More--
```

Space bar (пробіл тиснемо пару разів поки не спустимося вниз до кінця) all to the end



Система поділила лінії на 2 групи. Зашифруємо пароі Cisco/

Лінії 0 15 – всього 16 портів для підключення до switch.

```
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#service password-encryption
Switch1(config)#
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#show ru
```

Space …

Вже зашифровані паролі:

```
 shutdown
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
!
!
!
end


Switch1#
```

Sending Banner messege to users:

```
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#banner motd # Authorized access only!  Violators will be prosecuted to the full
extent of the law! #
Switch1(config)#
```

```
Switch1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#banner motd # Authorized access only!  Violators will be prosecuted to the full
extent of the law! #
Switch1(config)#
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#exit
```

Виходимо з свіча (exit)

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

User Access Verification

Password:
```

Password1: Cisco, password2: class (їх не видно при вводі)

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

User Access Verification

Password:

Switch1>enable
Password:
Switch1#
```

Тоді має адмін. Повний доступ до конфігурації свіча.

2.4.7. *Перевірка синтаксису - Базові налаштування пристрою*

Безпечний доступ для керування комутатором.

- Призначте ім’я пристрою.
- Захистіть доступ до користувацького режиму EXEC.
- Забезпечте безпечний доступ до привілейованого режиму EXEC.
- Захистіть доступ до VTY.
- Зашифруйте всі відкриті паролі.
- Покажіть банер при вході в систему.

Увійдіть до режиму глобальної конфігурації

```
Switch# config t
Команди потрібно вводити повністю і точно.
Switch# config terminal
Команди потрібно вводити повністю і точно.
Switch# configure terminal
```

Назвіть комутатор «Sw-Floor-1».

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

Захистіть доступ до користувацького режиму EXEC, ввівши **line console 0**, призначте пароль **cisco**, активуйте його та поверніться до режиму глобальної конфігурації за допомогою **exit.**

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

Захистіть доступ до користувацького режиму EXEC, ввівши **line console 0**, призначте пароль **cisco**, активуйте його та поверніться до режиму глобальної конфігурації за допомогою **exit.**

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# exit
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config-line)# exit
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
```

Забезпечте безпечний доступ до привілейованого режиму EXEC за допомогою пароля **class.**

```
Sw-Floor-1(config)# enable secret class
```

Захистіть лінії VTY від 0 до 15, призначте пароль **cisco**, активуйте його і поверніться в режим глобальної конфігурації, використовуючи **exit.**

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
```

Зашифруйте всі відкриті паролі.

```
Sw-Floor-1(config)# service password-encryption
```

Створіть банерне повідомлення, використовуючи символ **“#”** як роздільник. Банер повинен відображатись саме: **Warning! Authorized access only!**

```
Sw-Floor-1(config)# banner motd #Authorized Access Only#
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config)# banner motd #Authorized Access Only#
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config)# end
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config)# show running-config
Команди потрібно вводити повністю і точно.
Sw-Floor-1(config)# banner motd #Warning! Authorized access only!#

Ви успішно виконали основні вимоги щодо доступу та захисту пристрою.
```

2.4.8. *Питання для самоперевірки - Базові налаштування пристрою*

1. Яка команда використовується для призначення імені «Sw-Floor-2» комутатору?

- ◯ **hostname** Sw-Floor-2
- ◯ **host name** Sw-Floor-2
- ◯ **name** Sw-Floor-2

2. Як забезпечується захист доступу до привілейованого режиму EXEC на комутаторі?

- ◯ **enable class**
- ◯ **secret class**
- ◯ **enable secret class**
- ◯ **service password-encryption**

3. Яка команда дозволяє встановити автентифікацію по паролю для доступу до користувацького режиму EXEC на комутаторі?

- ◯ **enable secret**
- ◯ **login**
- ◯ **secret**
- ◯ **service password-encryption**

4. Яка команда шифрує всі незашифровані паролі доступу до комутатора?

- ◯ **enable secret**
- ◯ **login**
- ◯ **secret**
- ◯ **service password-encryption**

5. Яка команда використовується для налаштування банера, який відображатиметься під час під'єднання до комутатора?

- ◯ **banner $ Keep out $**
- ◯ **banner motd $ Keep out $**
- ◯ **display $ Keep out $**
- ◯ **login banner $ Keep out $**

1. Яка команда використовується для призначення імені «Sw-Floor-2» комутатору?

✓ Правильно!

- ◉ **hostname** Sw-Floor-2
- ◯ **host name** Sw-Floor-2
- ◯ **name** Sw-Floor-2

2. Як забезпечується захист доступу до привілейованого режиму EXEC на комутаторі?

✓ Правильно!

- ◯ **enable class**
- ◯ **secret class**
- ◉ **enable secret class**
- ◯ **service password-encryption**

3. Яка команда дозволяє встановити автентифікацію по паролю для доступу до користувацького режиму EXEC на комутаторі?

Правильно!

- ○ **enable secret**
- ◉ **login**
- ○ **secret**
- ○ **service password-encryption**

4. Яка команда шифрує всі незашифровані паролі доступу до комутатора?

Правильно!

- ○ **enable secret**
- ○ **login**
- ○ **secret**
- ◉ **service password-encryption**

5. Яка команда використовується для налаштування банера, який відображатиметься під час під'єднання до комутатора?

Правильно!

- ○ **banner $ Keep out $**
- ◉ **banner motd $ Keep out $**
- ○ **display $ Keep out $**
- ○ **login banner $ Keep out $**

2.5. Зберігання налаштувань

2.5.1. Файли конфігурації

Тепер ви знаєте, як виконати базову конфігурацію на комутаторі, включаючи паролі та банерні повідомлення. Ця тема покаже вам, як зберегти конфігурації.

Є два системні файли, які зберігають конфігурацію пристрою:

- **startup-config** - Це збережений файл конфігурації, який зберігається в NVRAM. Він містить усі команди, які будуть використовуватися пристроєм під час запуску або перезавантаження. Флеш-накопичувач не втрачає свого вмісту, коли пристрій вимкнено.
- **running-config** - Це файл поточної конфігурації, який зберігається в оперативній пам'яті (RAM). В ньому відображена поточна конфігурація. Зміна поточної конфігурації негайно впливає на роботу пристрою Cisco. Оперативна пам'ять (RAM) - енергозалежна пам'ять. Вона втрачає весь свій вміст при вимкненні або перезавантаженні пристрою.

Команда привілейованого режиму EXEC **show running-config** використовується для перегляду поточної конфігурації. Як показано в прикладі, команда відобразить повну конфігурацію, яка в даний момент зберігається в оперативній пам'яті.

```
Sw-Floor-1# show running-config
Building configuration...
Current configuration : 1351 bytes
!
! Last configuration change at 00:01:20 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Sw-Floor-1
!
(output omitted)
```

Щоб переглянути файл стартової конфігурації, використовуйте команду привілейованого режиму EXEC **show startup-config**.

Якщо втрачено живлення на пристрої або перезавантажено пристрій, всі зміни конфігурації будуть втрачені, якщо вони не були збережені. Для збереження змін, внесених до поточної конфігурації, у файл стартової конфігурації використовуйте команду привілейованого режиму EXEC **copy running-config startup-config**.

2.5.2. Зміна поточної конфігурації

Якщо зміни, внесені до поточної конфігурації, не мають потрібного ефекту, а running-config ще не збережений, ви можете відновити налаштування пристрою до його попередньої конфігурації. Видаліть змінені команди окремо або перезавантажте пристрій, використовуючи команду привілейованого режиму EXEC **reload** для відновлення конфігурації запуску.

Недоліком використання команди **reload** для видалення незбереженої робочої конфігурації є короткий час, протягом якого пристрій знаходиться в автономному режимі, що призводить до простою мережі.

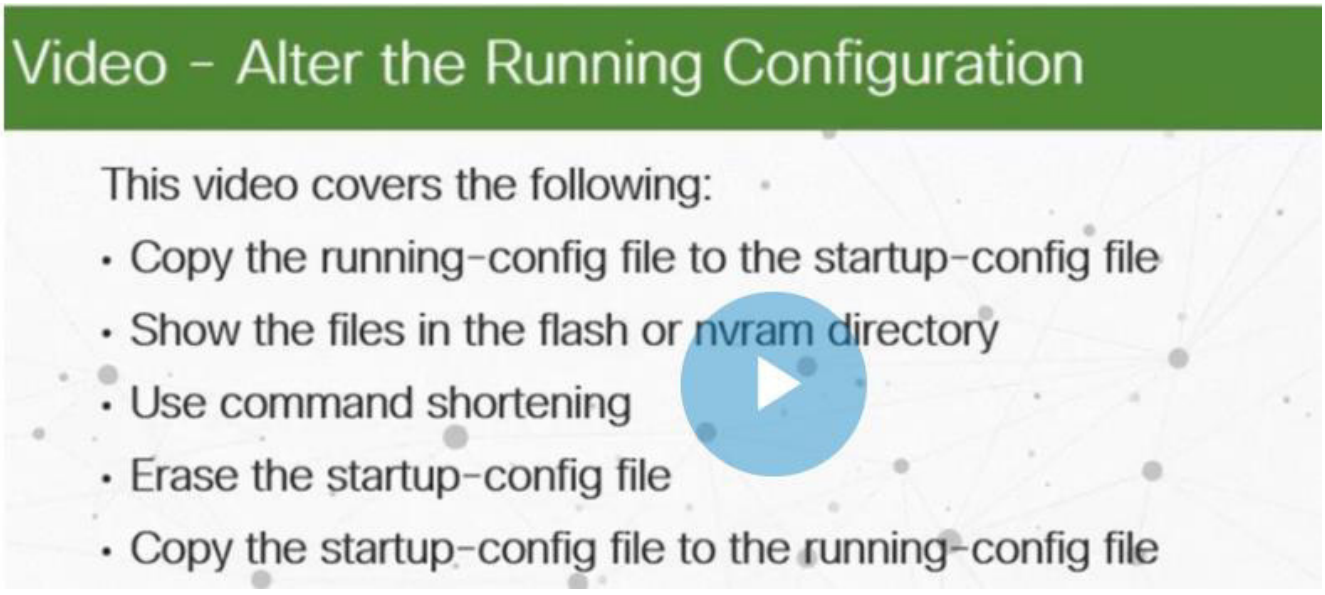
Коли ініціюється перезавантаження, IOS виявить, що у поточному файлі конфігурації є зміни, які не були збережені у файл стартової конфігурації. З'явиться запит на збереження змін. Щоб відмовитись від змін, введіть **n** або **no**.

Крім того, якщо в конфігурацію запуску були збережені небажані зміни, можливо, доведеться очистити всі конфігурації. Для цього потрібно видалити стартову конфігурацію та перезапустити пристрій. Стартова конфігурація видаляється за допомогою команди привілейованого режиму EXEC **erase startup-config**. Після виконання команди комутатор запросить підтвердження. Натисніть **Enter** для підтвердження.

Після видалення стартової конфігурації з NVRAM перезавантажте пристрій, щоб видалити файл поточної конфігурації з оперативної пам'яті. При перезавантаженні комутатор завантажить стартову конфігурацію за замовчуванням, яка постачалася з пристроєм.

2.5.3. Відео – Зміна поточної конфігурації

демонструє, як зберегти файли конфігурації коммутатора



IOS Command Line Interface

```
No unauthorized access allowed violators will be prosecuted to the
extent of the law!

User Access Verification

Password:

Switch>enable
Password:
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
```

+Enter

```
S1#copy running-config startup-config
Destination filename [startup-config]?
```

+Enter

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

Saved

```
S1#dir ?
  flash:  Directory or file name
  nvram:  Directory or file name
  <cr>
S1#dir nvram:
Directory of nvram:/

  238  -rw-        1205          <no date>  startup-config

1205 bytes total (237588 bytes free)

S1#
```

```
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#reload
Proceed with reload? [confirm]
```

+Enter

```
2960-24TT starting...
Base ethernet MAC Address: 0000.0CE9.C632
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4416217
flashfs[0]: Bytes available: 59600167
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
#########################################
```

IOS Command Line Interface

```
*    1   26     WS-C2960-24TT      12.2                        C2960-
LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

No unauthorized access allowed violators will be prosecuted to the
extent of the law!

User Access Verification

Password:

S1>
```

Configuration is saved (checked)

Якщо хочу стерти конфігурацію (erase configuration):

```
Password:

S1>enable
Password:
S1#erase sta
S1#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1#
```

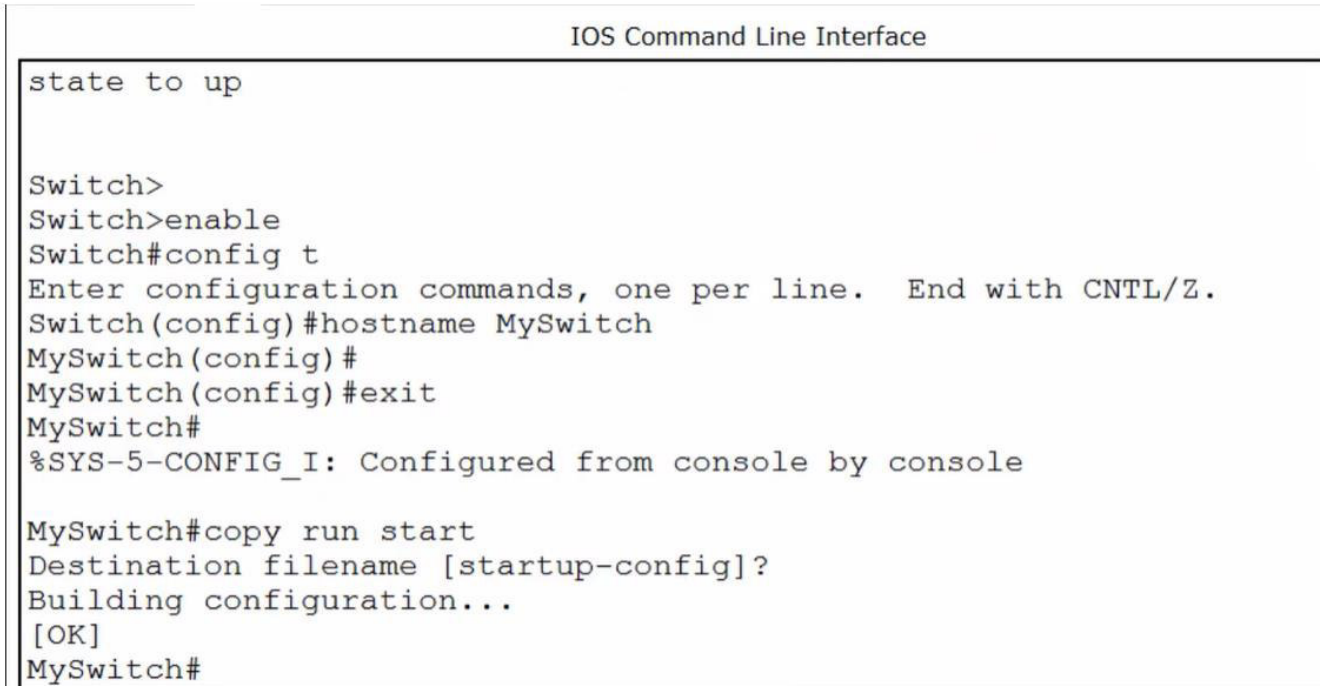
```
S1#reload
```
switch

```
2960-24TT starting...
Base ethernet MAC Address: 0000.0CE9.C632
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
###################################
```

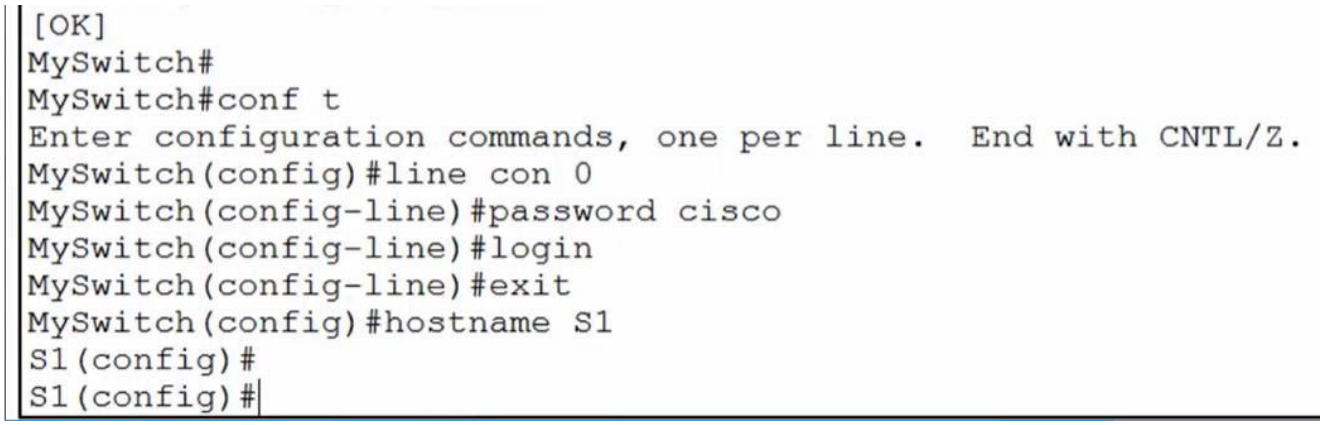
IOS Command Line Interface

```
LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, ch
state to up


Switch>
Switch>
```

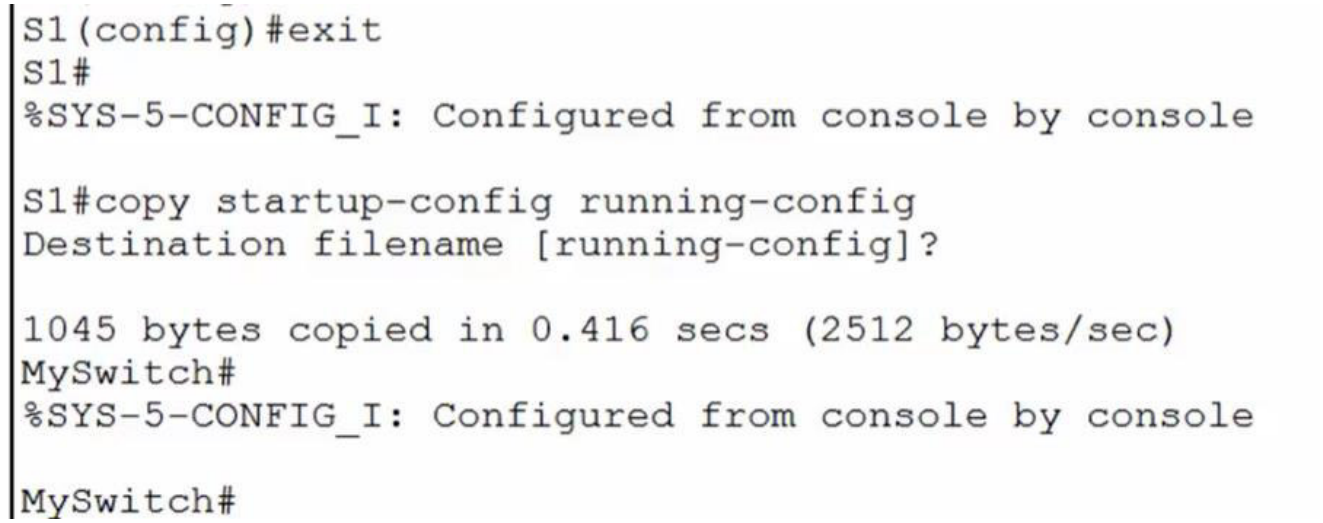
Замість стертого збережемо інший варіант конфігурації налаштувань свіча (комутатора):



Ще раз:



Якщо на цей раз не зберігати то можна загрузити іншу останню збережену конфігурацію:

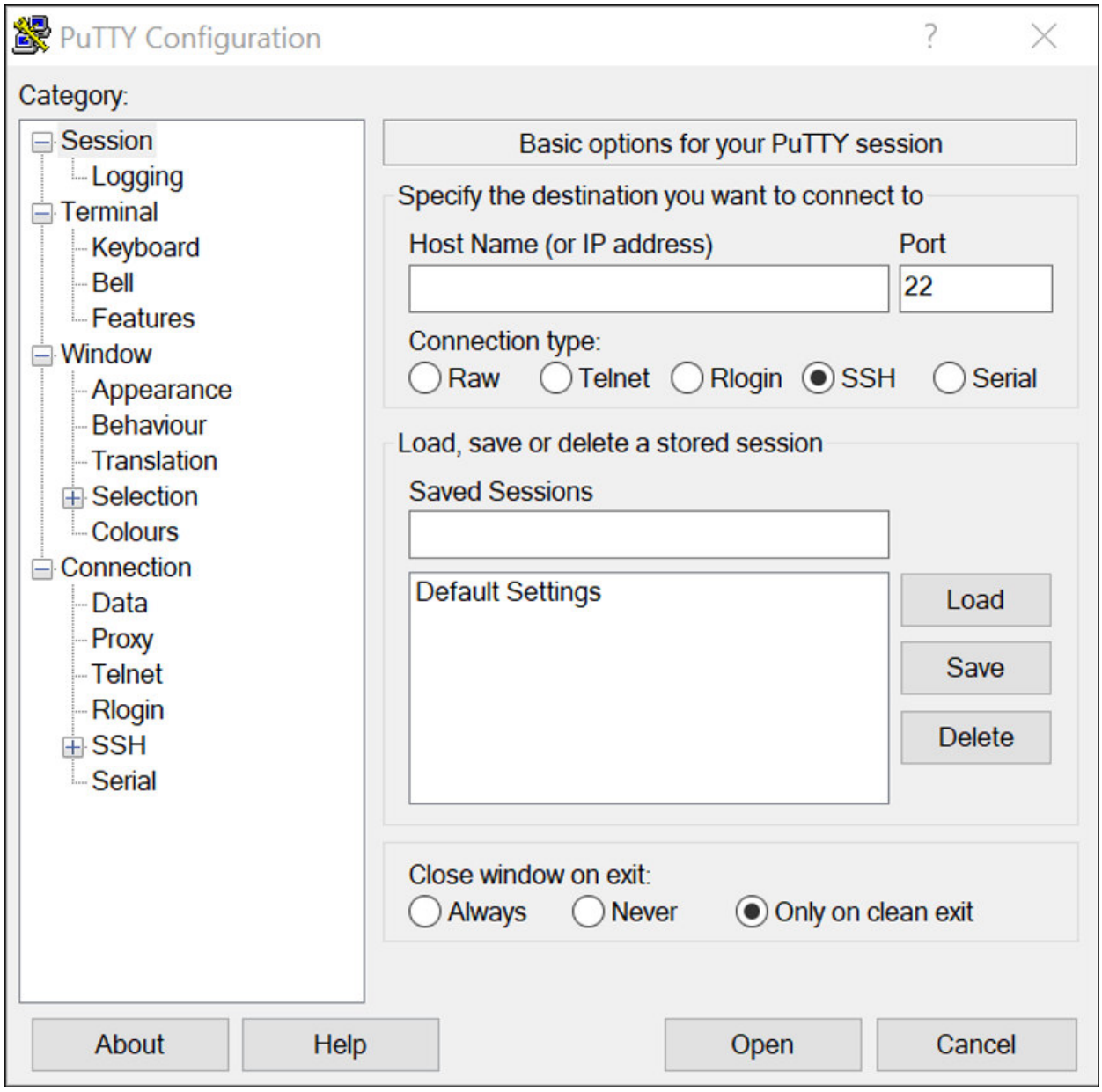


2.5.4. Запис конфігурації у текстовий файл

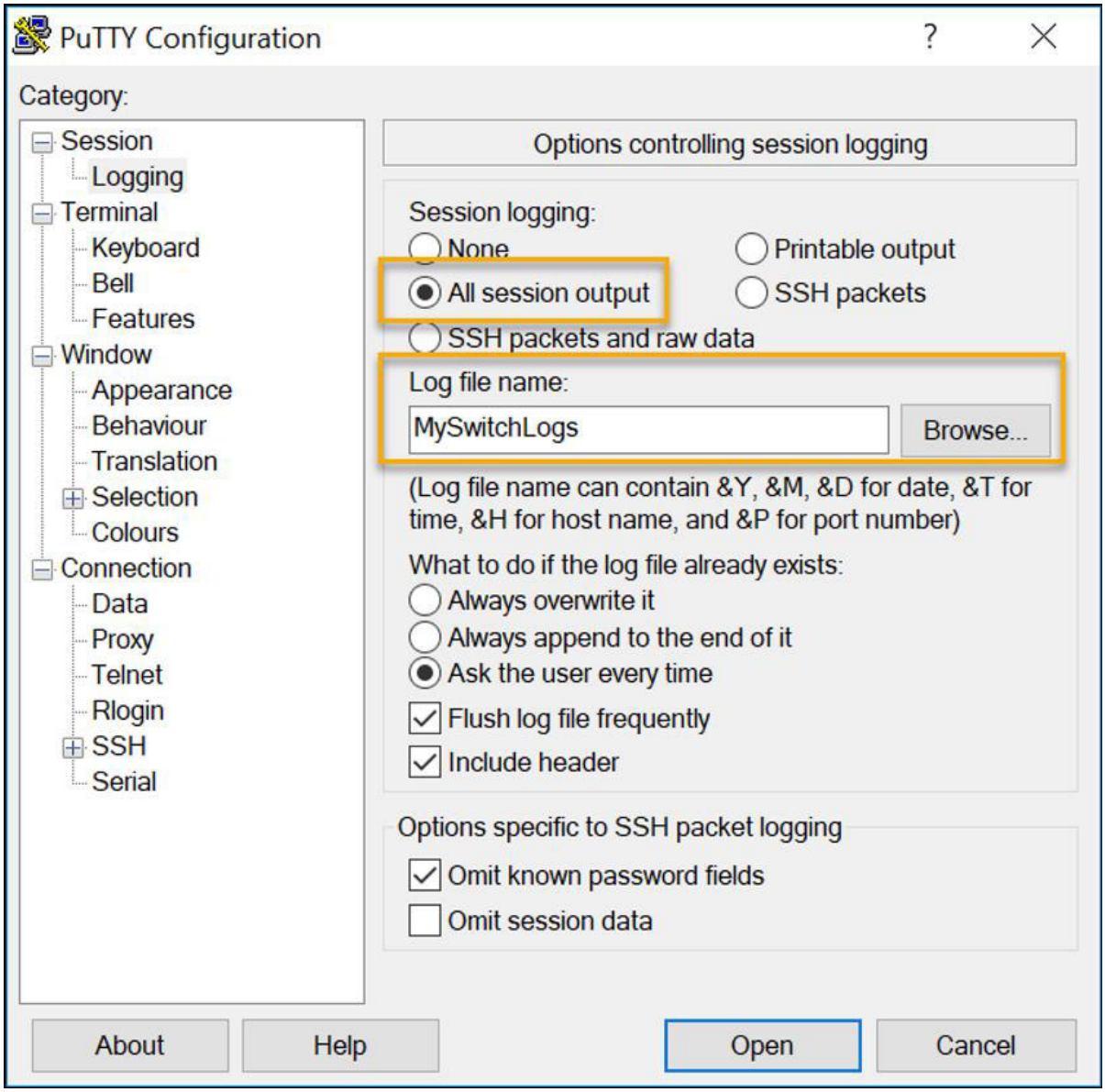
Файли конфігурації також можна зберігати та архівувати у текстовий документ. Ця послідовність кроків забезпечує доступність робочої копії файлу конфігурації для редагування або повторного використання пізніше.

Наприклад, припустимо, що комутатор налаштовано, а поточна конфігурація збережена на пристрої.

Крок 1. Відкрийте програмне забезпечення для емуляції терміналу, наприклад PuTTY або Tera Term, яке вже підключено до комутатора.



Крок 2. Активуйте ведення журналу в програмі терміналу і призначте файлу журналу ім'я і місце збереження. На рисунку показано, що **All session output** буде зберігатися у визначений файл (наприклад, MySwitchLogs).

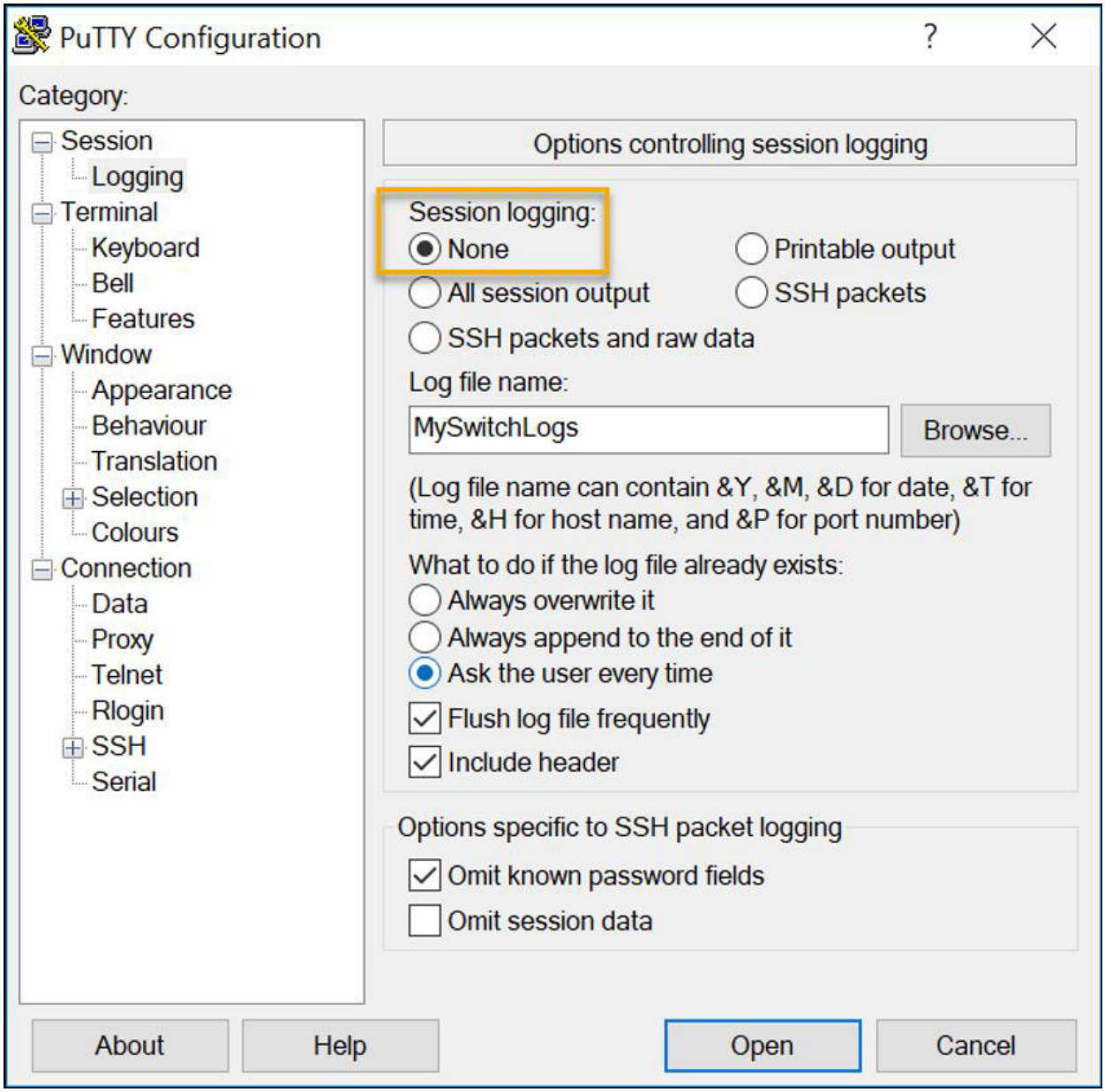


Крок 3. Виконайте команду **show running-config** або **show startup-config** у привілейованому режимі EXEC. Текст, що відображається у вікні терміналу, буде розміщено у вибраному файлі.

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

```
Building configuration...
```

Крок 4. Вимкніть ведення журналу в програмі терміналу. На рисунку показано, як відключити ведення журналу сеансу, вибравши параметр **None**.



Створений текстовий файл може використовуватися як запис поточної конфігурації пристрою. Можливо, файл потрібно буде редагувати, перш ніж використовувати для відновлення збереженої конфігурації на пристрої.

Щоб відновити файл конфігурації на пристрої:

Крок 1. Увійдіть до режиму глобальної конфігурації на пристрої.

Крок 2. Скопіюйте та вставте текстовий файл у вікно терміналу, підключеного до комутатора.

Текст у файлі буде застосовано як команди в CLI та стане поточною конфігурацією на пристрої. Це зручний спосіб налаштувати пристрій вручну.

2.5.5. *Packet Tracer - Налаштування початкових параметрів комутатора*

У цьому завданні ви налаштуєте базові параметри комутатора. Ви забезпечите доступ до інтерфейсу командного рядку CLI і 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.

Networking Academy

Packet Tracer - 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

Packet Tracer - Налаштування початкових параметрів комутатора

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**.

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
```

Packet Tracer - Налаштування початкових параметрів комутатора

```
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

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**?

Packet Tracer - Налаштування початкових параметрів комутатора

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 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.

2.6. Порти і адреси

2.6.1. IP-адреси

Вітаємо, ви виконали базову конфігурацію пристрою! Звичайно, веселощі ще не закінчилися. Якщо ви хочете, щоб ваші кінцеві пристрої спілкувалися один з одним, ви повинні переконатися, що кожен з них має відповідну IP-адресу та правильно під'єднаний. У цьому розділі ви дізнаєтесь про IP-адреси, порти пристроїв та носії, які використовуються для під'єднання пристроїв.

Використання IP-адрес є основним засобом, що дозволяє пристроям знаходити один одного та встановлювати наскрізне з'єднання в Інтернеті. Кожен кінцевий пристрій в мережі повинен бути налаштований з IP-адресою. Приклади кінцевих пристроїв:

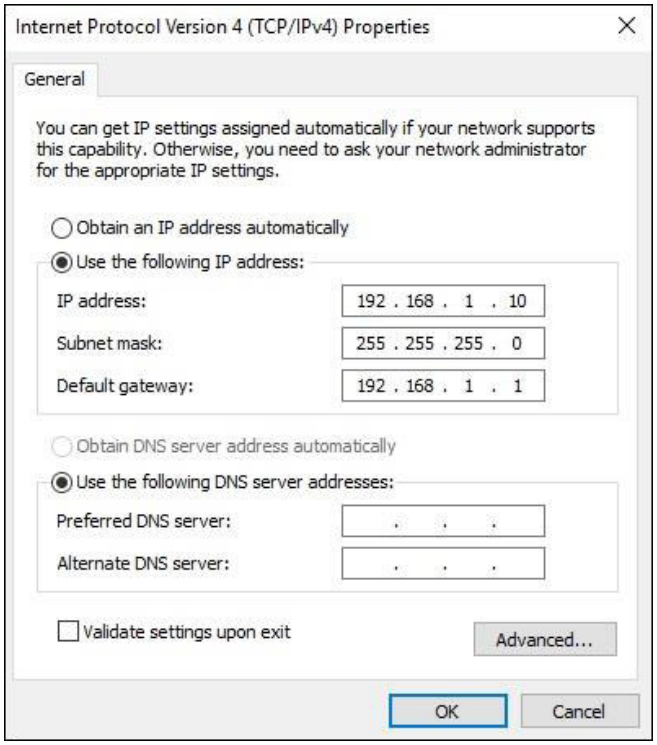
- Комп'ютери (робочі станції, ноутбуки, файлові сервери, веб-сервери)
- Мережні принтери
- VoIP-телефони
- Камери охоронного відеоспостереження
- Смартфони
- Мобільні кишенькові пристрої (наприклад, бездротові сканери штрих-коду)

Структура адреси IPv4 - це крапково-десяткове представлення у вигляді чотирьох десяткових чисел в діапазоні від 0 до 255. Адреси IPv4 призначаються окремим пристроям, під'єднаним до мережі.

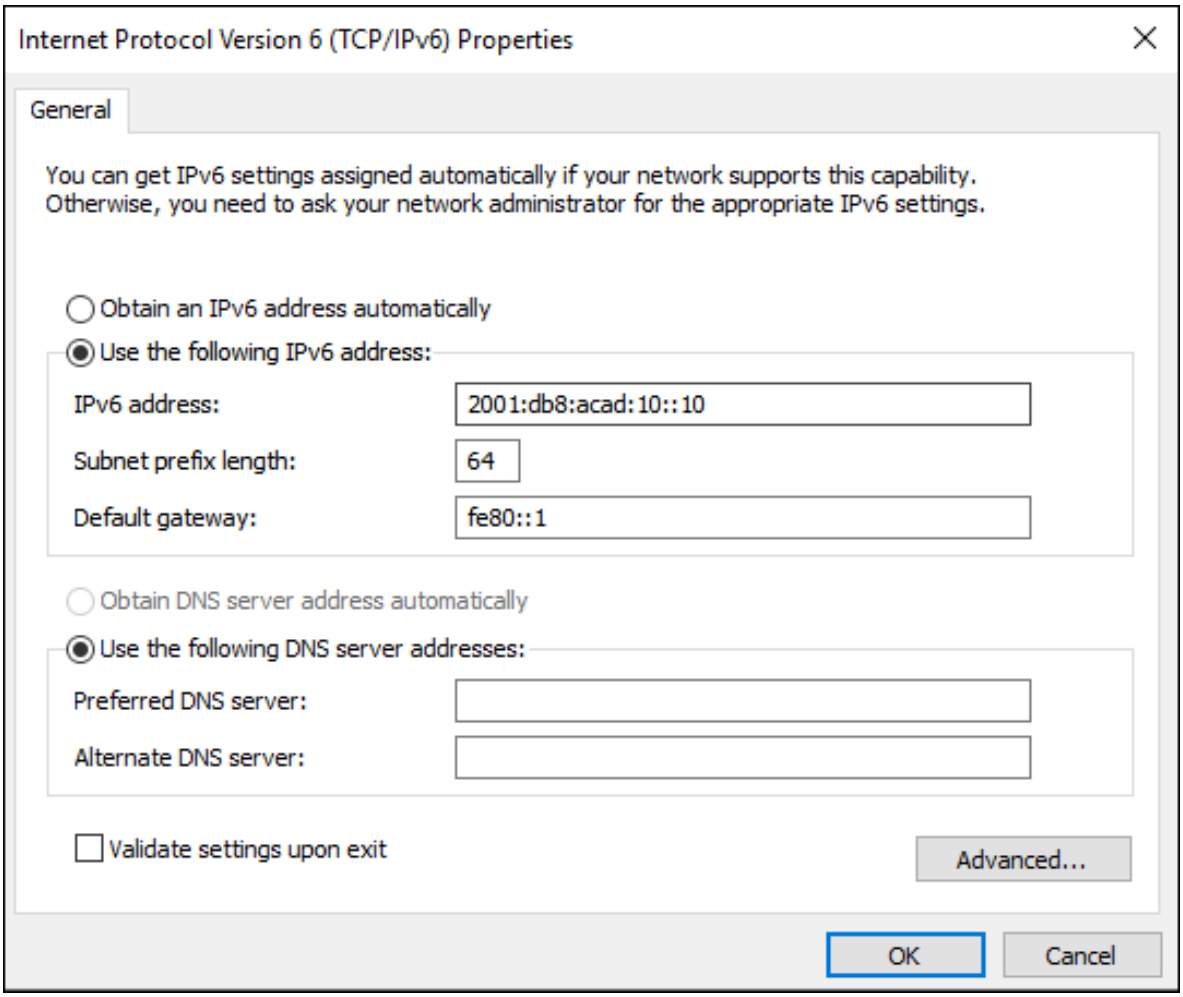
Примітка: Термін IP в цьому курсі використовується, коли мова йде про обидва протоколи: IPv4 та IPv6. IPv6 - це найновіша версія IP, яка замінює поширений зараз IPv4.

З IPv4-адресою необхідно використовувати маску підмережі. Маска підмережі IPv4 - це 32-бітове значення, яке відокремлює мережну частину адреси від вузлової частини. У поєднанні з IPv4-адресою маска підмережі визначає, до якої підмережі належить пристрій.

У прикладі на рисунку показані адреса IPv4 (192.168.1.10), маска підмережі (255.255.255.0) і шлюз за замовчуванням (192.168.1.1), які призначені хосту. Адреса шлюзу за замовчуванням - це IP-адреса маршрутизатора, яку вузол використовуватиме для доступу до віддалених мереж, включаючи Інтернет.

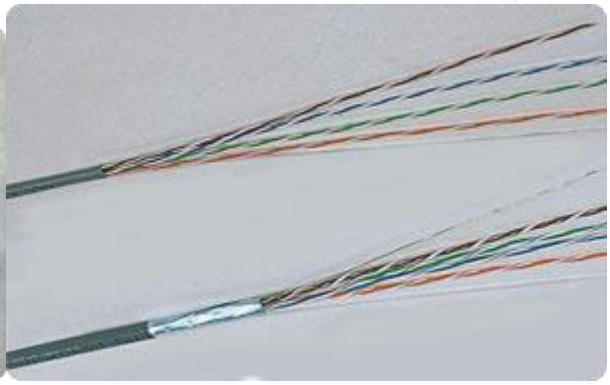


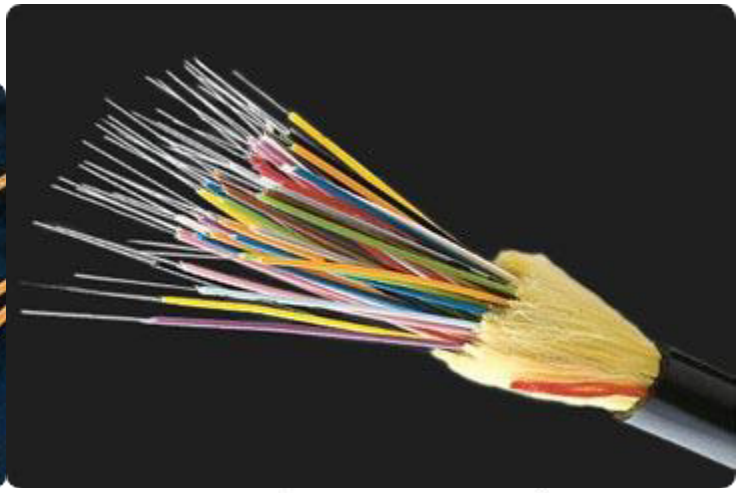
Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень. Кожні чотири біти представлені однією шістнадцятковою цифрою; загалом 32 шістнадцяткові цифри. Групи з чотирьох шістнадцяткових цифр розділені двокрапкою “:”. IPv6-адреси не чутливі до регістру і можуть бути записані як в нижньому регістрі, так і у верхньому.



2.6.2. Інтерфейси і порти

Мережний зв'язок залежить від інтерфейсу пристрою кінцевого користувача, інтерфейсів мережних пристроїв та кабелів, що їх з'єднують. Кожен фізичний інтерфейс має технічні характеристики або стандарти, які його визначають. Кабель, що підключається до інтерфейсу, повинен відповідати фізичним стандартам інтерфейсу. Типи мережних носіїв включають мідні кабелі з витою парою, волоконно-оптичні кабелі, коаксіальні кабелі або бездротові, як показано на рисунку.




Мідний кабель. Бездротове середовище. Волоконно-оптичний кабель

Різні типи мережних носіїв мають різні особливості та переваги. Не всі мережні середовища мають однакові характеристики. Не всі середовища підходять для однієї і тієї ж мети. Ось деякі відмінності між різними видами середовища:

- Відстань, на яку носій може успішно передавати сигнал
- Середовище, у якому потрібно прокласти носій
- Кількість даних і швидкість, з якою їх потрібно передати
- Вартість носія та його прокладання

Не тільки кожне посилання в Інтернеті вимагає певного типу мережних носіїв, але і кожне посилання вимагає певної мережної технології. Наприклад, Ethernet - це найпоширеніша технологія локальних мереж (LAN), яка використовується сьогодні. Порти Ethernet знаходяться на пристроях кінцевих користувачів, комутаційних пристроях та інших мережних пристроях, які можуть фізично під'єднуватися до мережі за допомогою кабелю.

Комутатори Cisco IOS рівня 2 мають фізичні порти для під'єднання пристроїв. Ці порти не підтримують IP-адреси 3 рівня. Тому комутатори мають один або більше віртуальних інтерфейсів комутаторів (switch virtual interface, SVI). Такі інтерфейси називаються віртуальними, тому що на пристрої, пов'язаному з ними, немає фізичного обладнання. SVI створюється в програмному забезпеченні.

Віртуальний інтерфейс дозволяє віддалено керувати комутатором через мережу за допомогою IPv4 та IPv6. Кожен комутатор постачається з одним SVI у конфігурації за замовчуванням. Віртуальним інтерфейсом за замовчуванням є VLAN 1.

Примітка: Комутатору рівня 2 не потрібна IP-адреса. IP-адреса, призначена SVI, використовується для віддаленого доступу до комутатора. Для роботи комутатора IP-адреса не потрібна.

2.6.3. *Питання для самоперевірки - Порти і адреси*

Перевірте своє розуміння портів та адрес, обравши правильну відповідь на такі запитання.

1. Як називається структура адреси IPv4?

- двійковий формат з крапками
- крапково-десятковий формат
- крапково-шістнадцятковий формат

2. Як представлена адреса IPv4?

- чотири двійкових числа від 0 до 1, які розділені двокрапкою.
- чотири десяткових числа від 0 до 255, які розділені крапками.
- тридцять два шістнадцяткових числа, які розділені двокрапками.
- тридцять два шістнадцяткових числа, які розділені крапками.

3. Який тип інтерфейсу не має пов'язаного з ним фізичного порту?

- консольний
- Ethernet
- послідовний порт
- віртуальний інтерфейс комутатора (SVI)

Перевірити

Показати

Скинути

1. Як називається структура адреси IPv4?

Правильно!

- ○ двійковий формат з крапками
- ◉ крапково-десятковий формат
- ○ крапково-шістнадцятковий формат

2. Як представлена адреса IPv4?

Правильно!

- ○ чотири двійкових числа від 0 до 1, які розділені двокрапкою.
- ◉ чотири десяткових числа від 0 до 255, які розділені крапками.
- ○ тридцять два шістнадцяткових числа, які розділені двокрапками.
- ○ тридцять два шістнадцяткових числа, які розділені крапками.

3. Який тип інтерфейсу не має пов'язаного з ним фізичного порту?

Правильно!

- ○ консольний
- ○ Ethernet
- ○ послідовний порт
- ◉ віртуальний інтерфейс комутатора (SVI)

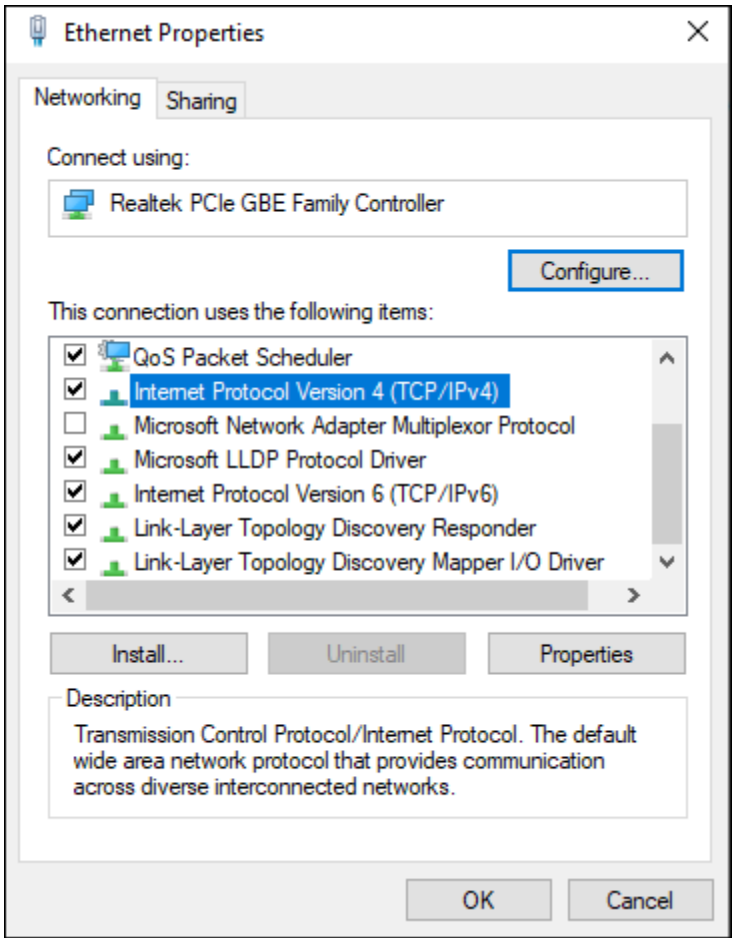
2.7. Налаштування IP-адресації

2.7.1. Ручне налаштування IP-адресації на кінцевому пристрої

Настільки ж, як вам потрібні номери телефонів ваших друзів, щоб надіслати їм текстові повідомлення або зателефонувати, кінцеві пристрої у вашій мережі потребують IP-адреси, щоб вони могли спілкуватися з іншими пристроями у вашій мережі. У цьому розділі ви будете створювати основні під'єднання, налаштовуючи IP-адреси на комутаторах та ПК.

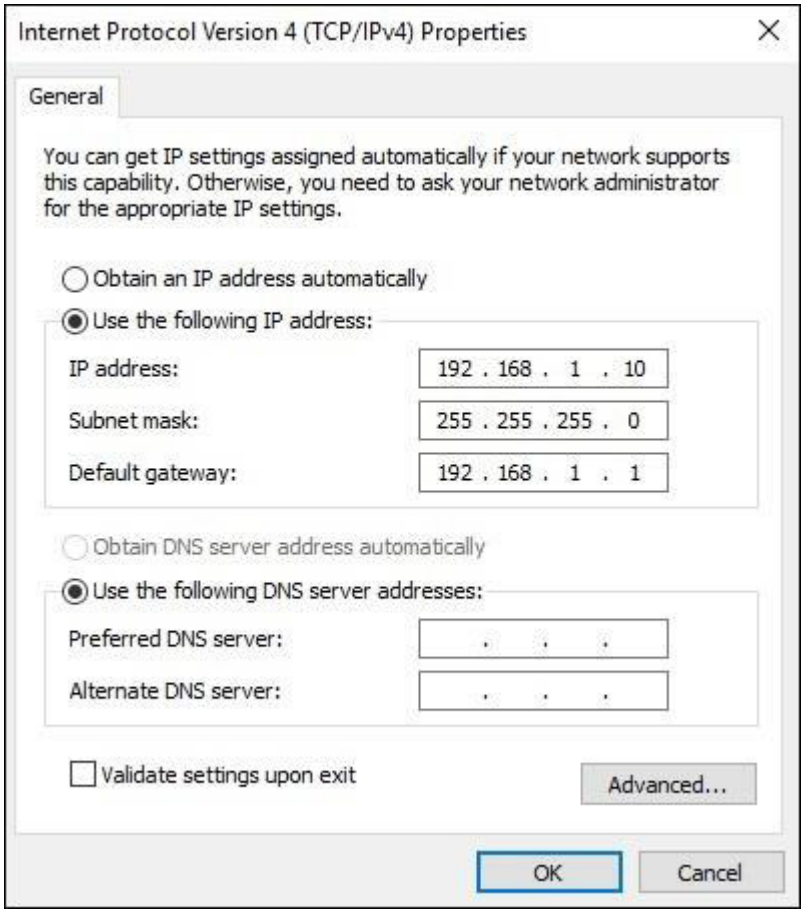
IP-адресу можна налаштувати на кінцевому пристрої вручну або отримати автоматично за допомогою протоколу DHCP.

Щоб вручну налаштувати IPv4-адресу на вузлі з ОС Windows, відкрийте **Control Panel > Network Sharing Center > Change adapter settings** і виберіть потрібний адаптер. Клацніть правою кнопкою миші та оберіть **Properties** для відображення **Local Area Connection Properties**, як показано на рисунку.



Виділіть Internet Protocol Version 4 (TCP/IPv4) та натисніть **Properties**, щоб відкрити **Internet Protocol Version 4 (TCP/IPv4) Properties** вікно, яке відображено на рисунку. Налаштуйте адресу IPv4, маску підмережі та параметри шлюзу за замовчуванням на PC-A.

Примітка: Для IPv6 параметри адресації та налаштування схожі на IPv4.



Примітка: Адреси DNS-серверів - це адреси IPv4 та IPv6 серверів системи доменних імен (DNS), які використовуються для перекладу IP-адрес на доменні імена, наприклад www.cisco.com.

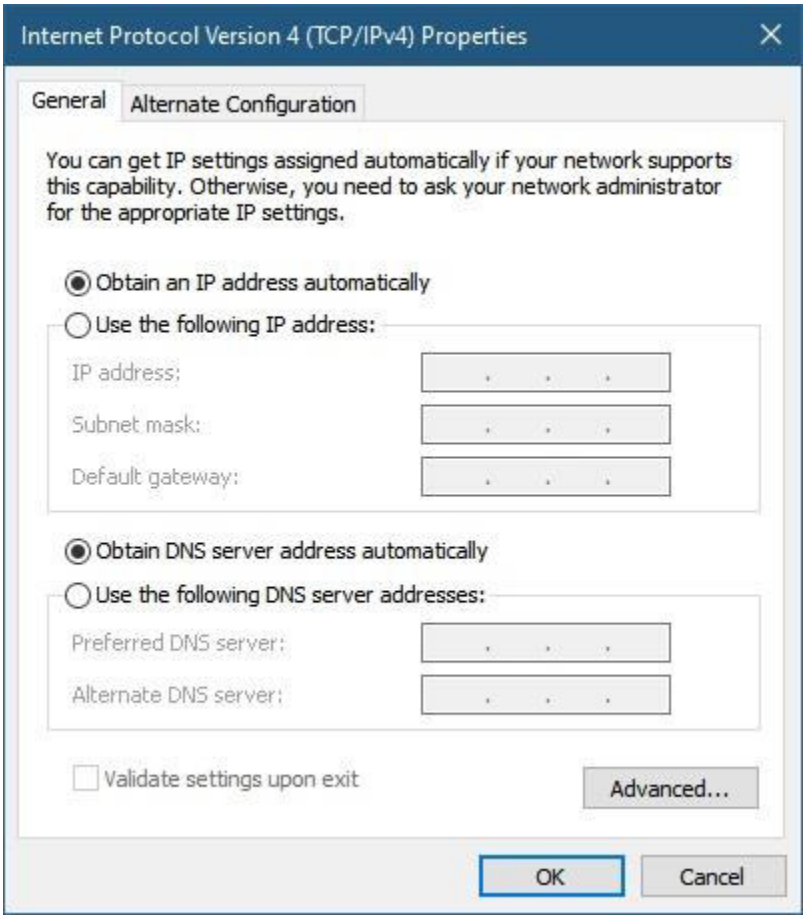
2.7.2. *Автоматичне налаштування IP-адресації на кінцевому пристрої*

Для автоматичного налаштування адреси IPv4 кінцеві пристрої зазвичай використовують за замовчуванням DHCP. DHCP - це технологія, яка використовується майже в кожній мережі. Найкращий спосіб зрозуміти, чому DHCP настільки популярний, - розглянути всю додаткову роботу, яка мала б пройти без нього.

Протокол DHCP робить можливою автоматичну конфігурацію адреси IPv4 для кожного кінцевого пристрою, що підтримує DHCP. Уявіть, скільки часу знадобиться, якби кожен раз, коли ви підключалися до мережі, вам довелося вручну вводити адресу IPv4, маску підмережі, шлюз за замовчуванням та сервер DNS. Помножте це на кожного користувача та кожний пристрій в організації, і ви побачите проблему. Ручна конфігурація також збільшує ймовірність неправильної конфігурації шляхом дублювання IPv4-адреси іншого пристрою.

Як показано на рисунку, щоб налаштувати DHCP на ПК з Windows, потрібно лише вибрати **Obtain an IP address automatically** та **Obtain DNS server address automatically**. Ваш комп'ютер виконає пошук DHCP-сервера і отримає налаштування адреси, необхідні для зв'язку в мережі.

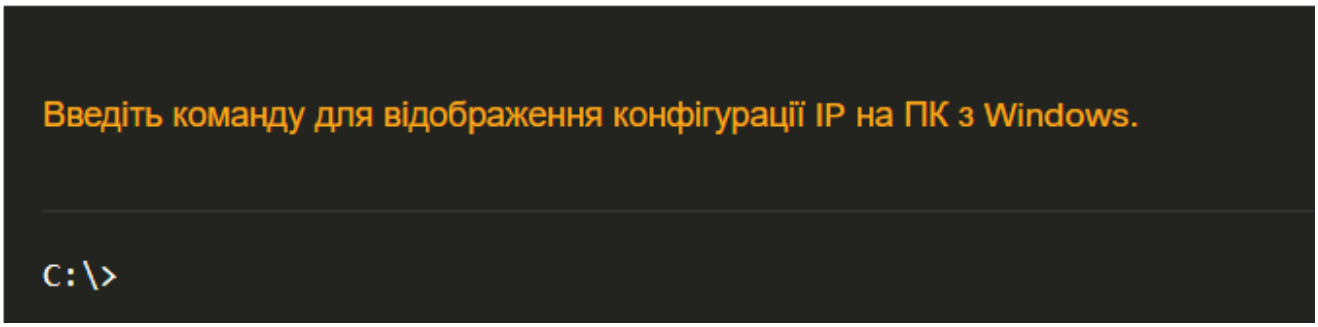
Примітка: IPv6 для динамічного розподілу адрес використовує DHCPv6 та SLAAC (Stateless Address Autoconfiguration).



2.7.3. Перевірка синтаксису – Перевірка налаштування протоколу IP на ПК з Windows

Можна відобразити параметри конфігурації IP на ПК з Windows за допомогою команди **ipconfig** в командному рядку. Вихідні дані команди будуть показувати адресу IPv4, маску підмережі та інформацію про шлюз, отримані від сервера DHCP.

Введіть команду для відображення конфігурації IP на ПК з Windows.



2.7.4. *Налаштування віртуального інтерфейсу комутатора*

Щоб отримати віддалений доступ до комутатора, на віртуальному інтерфейсі комутатора (SVI) повинні бути налаштовані IP-адреса та маска підмережі. Щоб налаштувати SVI на комутаторі, використовуйте команду глобальної конфігурації **interface vlan 1**. Vlan 1 - це не фізичний, а віртуальний інтерфейс. Далі призначте адресу IPv4 за допомогою команди конфігурації інтерфейсу **ip address** *ip-address subnet-mask*. Нарешті, увімкніть віртуальний інтерфейс за допомогою команди конфігурації інтерфейсу **no shutdown**.

Після налаштування цих команд комутатор має всі елементи IPv4, готові до спілкування по мережі.

```
Sw-Floor-1# configure terminal
```

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

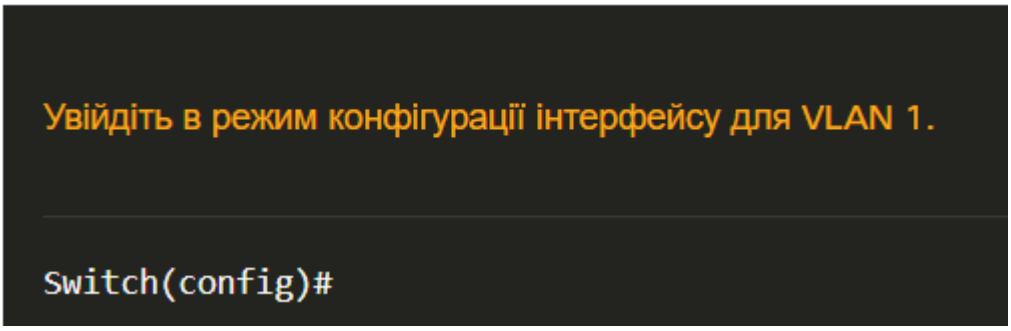
```
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
```

```
Sw-Floor-1(config-if)# no shutdown
```

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

```
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

2.7.5. *Перевірка синтаксису – Налаштування віртуального інтерфейсу комутатора*



2.7.6. *Packet Tracer - Реалізація базового з'єднання*

У цьому завданні ви спочатку налаштуєте основні параметри комутатора. Потім ви створите основні під'єднання, налаштувавши IP адреси на комутаторах і ПК. Після завершення налаштування IP-адресації ви будете використовувати різні команди **show** для перевірки конфігурацій та використовувати команду **ping** для перевірки базового з'єднання між пристроями.

Networking Academy

Packet Tracer - Реалізація базового з'єднання

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?

Packet Tracer - Реалізація базового з'єднання

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.

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

```
Packet Tracer PC Command Line 1.0
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.

2.8. Перевірка з'єднання

2.8.1. Відео завдання - Тестування призначень інтерфейсу

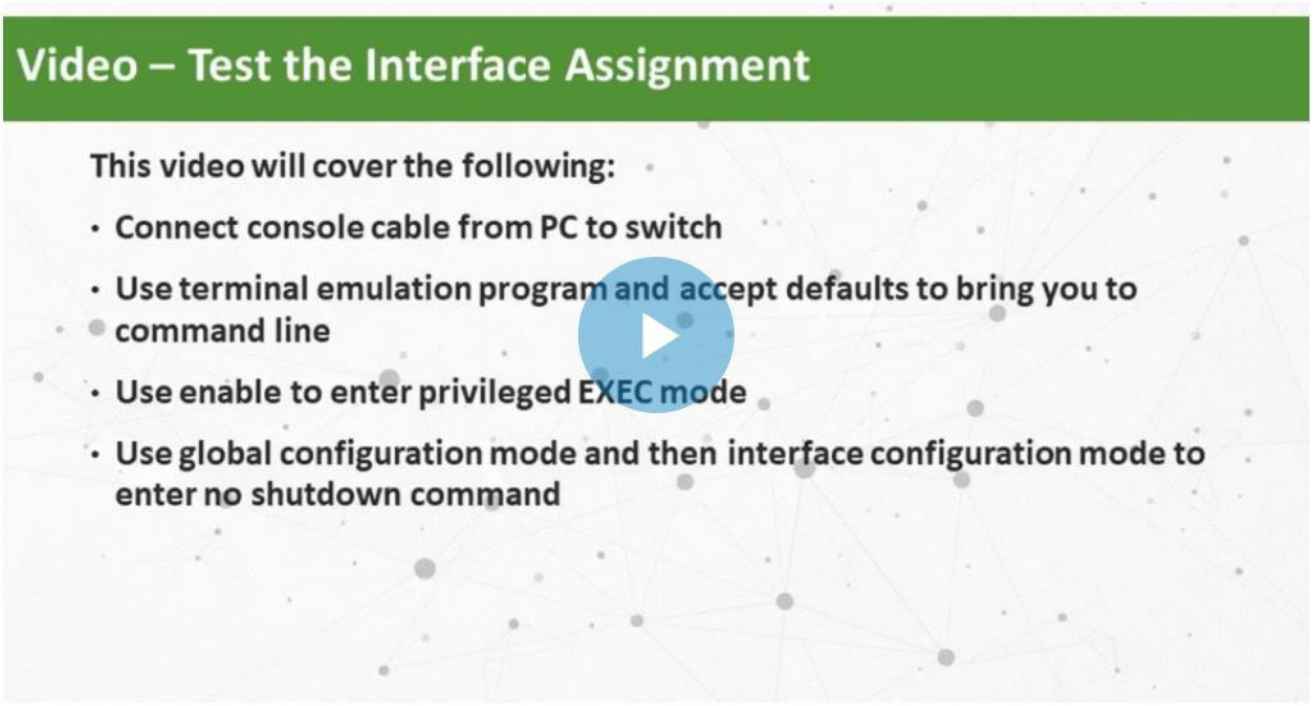
У попередній темі ви реалізували базове під'єднання, налаштувавши IP-адресацію на комутаторах та ПК. Потім ви перевірили свої конфігурації та під'єднання, адже, який сенс налаштовувати пристрій, якщо ви не переконалися, що конфігурація працює? Ви продовжите цей процес у цьому розділі. Використовуючи інтерфейс командного рядка (CLI), ви перевірите інтерфейси та адреси комутаторів та маршрутизаторів у вашій мережі.

Таким же чином, як ви використовуєте команди і утиліти, наприклад **ipconfig**, для перевірки мережної конфігурації вузла, ви також використовуєте команди для перевірки інтерфейсів і налаштувань адрес проміжних пристроїв, таких як комутатори і маршрутизатори.

Натисніть кнопку Відтворити на рисунку, щоб переглянути відеодемонстрацію команди **show ip interface brief**. Ця команда корисна для перевірки стану інтерфейсів комутатора.

Тестування призначень інтерфейсу

Завантажте той самий файл PKT, який використовується у відео. Практикуйтеся у використанні команд **ipconfig** і **show ip interface brief** , як показано на відео.



Тестування призначень інтерфейсу

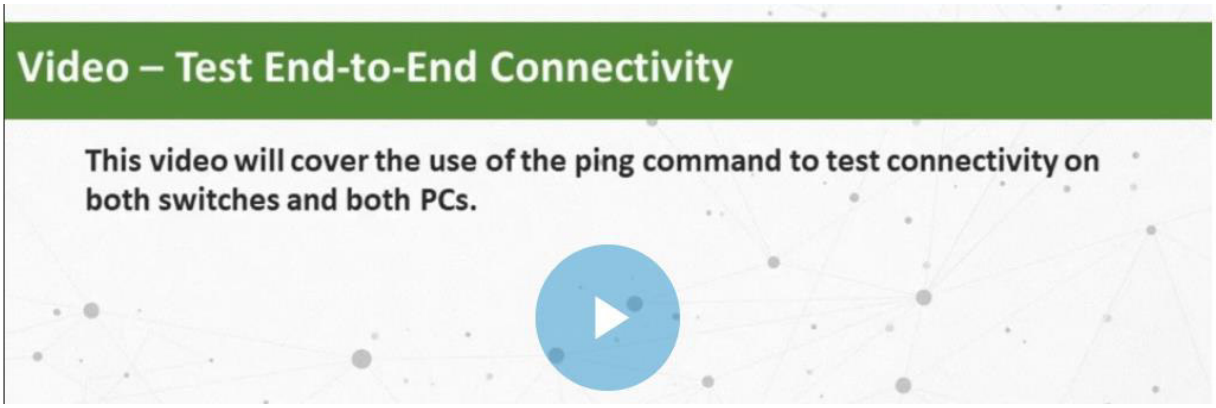
2.8.2. *Відео - Тестування наскрізного з'єднання*

Команда **ping** може використовуватися для перевірки з'єднання з іншим пристроєм в мережі або веб-сайту в Інтернеті.

Натисніть кнопку Відтворити на рисунку, щоб переглянути відео, яке демонструє використання команди **ping** для перевірки з'єднання з комутатором і іншим ПК.

Тестування призначень інтерфейсу

Завантажте той самий файл PKT, який використовується у відео. Тренуйтеся, використовуючи команду **ping**, як показано на відео.



Практичне завдання та контрольна робота

2.9.1. *Packet Tracer - Базові налаштування комутатора та кінцевого пристрою*

Менеджер попросив вас, нового фахівця з обслуговування локальних мереж, продемонструвати навички налаштування невеликої локальної мережі. Вам потрібно налаштувати базові параметри на двох комутаторах під керуванням Cisco IOS, а також налаштувати параметри IP-адресації на вузлах для створення наскрізного з'єднання. У схемі під'єднання ви повинні використовувати два комутатора і два ПК.

Networking Academy

Packet Tracer - Базові налаштування комутатора та кінцевого пристрою

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Цілі та задачі

- Налаштування імен та IP-адрес на двох комутаторах під керуванням Cisco IOS (Internetwork Operating System) за допомогою інтерфейсу командного рядка (CLI).
- Використання команд Cisco IOS для надання або обмеження доступу до конфігурацій пристроїв.
- Використання команд IOS для зберігання поточних налаштувань.
- Налаштування IP-адрес на двох кінцевих пристроях.
- Перевірка зв'язку між двома кінцевими пристроями.

Сценарій

....

2.9.2. *Лабораторна робота – Базові налаштування комутатора та кінцевого пристрою*

В цій лабораторній роботі ви виконаєте наступні завдання:

- Частина1: Налаштування мережної топології
- Частина2: Налаштування ПК-вузлів
- Частина3: Налаштування та перевірка основних параметрів комутатора

Networking Academy

Лабораторна робота – Базові налаштування комутатора та кінцевих пристроїв

Топологія

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Цілі та задачі

- Налаштування мережної топології
- Налаштування ПК-вузлів
- Налаштування та перевірка основних параметрів комутатора

Довідкова інформація / Сценарій

2.9.3. *Що ми вивчили у цьому розділі?*

Усі кінцеві пристрої та мережні пристрої потребують операційної системи (ОС). Користувач може взаємодіяти з оболонкою за допомогою інтерфейсу командного рядка (CLI), щоб використовувати клавіатуру для запуску мережних програм на основі CLI, використовувати клавіатуру для введення тексту та текстових команд та переглядати вихідні дані на моніторі.

В якості функції захисту програмне забезпечення Cisco IOS розподіляє доступ до керування на наступні два режими команд: користувацький режим EXEC та привілейований режим EXEC.

Перед тим, як перейти в інші спеціалізовані режими конфігурації, потрібно увійти в режим глобальної конфігурації. З режиму глобальної конфігурації користувач може перейти в різні підрежими конфігурації. Кожен з цих режимів дозволяє сконфігурувати певну частину або функцію пристрою IOS. Два поширених підрежими конфігурації включають: режим

конфігурації ліній та режим конфігурації інтерфейсу. Щоб перейти в режим глобальної конфігурації і вийти з нього, використовуйте команду **configure terminal** привілейованого режиму EXEC. Щоб повернутися до привілейованого режиму EXEC, введіть команду **exit** режиму глобальної конфігурації.

Кожна команда IOS має певний формат або синтаксис і може виконуватися лише у відповідному режимі. Загальним синтаксисом для команди є команда, за якою слідують будь-які відповідні ключові слова та аргументи. У IOS доступні дві форми допомоги: контекстна довідка та перевірка синтаксису команд.

Першою командою налаштування на будь-якому пристрої має бути присвоєння йому унікального імені вузла. Мережні пристрої завжди повинні мати паролі, налаштовані для обмеження адміністративного доступу. Cisco IOS можна налаштувати на використання паролів ієрархічних режимів, щоб дозволити різні права доступу до мережного пристрою. Налаштування та шифрування всіх паролів. Вкажіть спосіб оголошення, що тільки авторизований персонал повинен намагатися отримати доступ до пристрою, додавши банер до вихідних даних пристрою.

Є два системні файли, в яких зберігаються конфігурації пристрою: startup-config та running-config. Файли поточної конфігурації можуть бути змінені, якщо вони не були збережені. Файли конфігурації також можна зберігати та архівувати у текстовий документ.

IP-адреси дозволяють пристроям знаходити один одного та встановлювати наскрізне з'єднання в Інтернеті. Кожен кінцевий пристрій в мережі повинен бути налаштований з IP-адресою. Структура адреси IPv4 називається крапково-десятковим позначенням і представлена чотирма десятковими числами від 0 до 255.

Адресу IPv4 можна вводити на кінцевих пристроях вручну або автоматично, використовуючи протокол динамічної конфігурації хоста (DHCP - Dynamic Host Configuration Protocol). Протокол DHCP робить можливою автоматичну конфігурацію адреси IPv4 для кожного кінцевого пристрою, що підтримує DHCP. Щоб отримати віддалений доступ до комутатора, на віртуальному інтерфейсі комутатора (SVI) повинні бути налаштовані IP-адреса та маска підмережі. Щоб налаштувати SVI на комутаторі, використовуйте команду глобальної конфігурації **interface vlan 1**. Vlan 1 - це не фізичний, а віртуальний інтерфейс.

Таким же чином, як ви використовуєте команди і утиліти, такі як перевірка мережної конфігурації вузла, ви також використовуєте команди для перевірки інтерфейсів і налаштувань адрес проміжних пристроїв, таких як комутатори і маршрутизатори. Команда **show ip interface brief** перевіряє стан інтерфейсів комутатора. Команда **ping** може використовуватися для перевірки під'єднання до іншого пристрою в мережі або веб-сайту в Інтернеті.

2.9.4. *Контрольна робота з розділу - Базові налаштування комутатора і кінцевого пристрою*

1. Яке твердження вірне відносно файлу поточної конфігурації на пристрої Cisco IOS?

- ◯ Він зберігається в NVRAM.
- ◯ Його слід видалити за допомогою команди **erase running-config**.
- ◯ Він автоматично зберігається при перезавантаженні маршрутизатора.
- ◯ Він впливає на роботу пристрою відразу після його модифікації.

2. Які два твердження вірні щодо користувацького режиму EXEC? (Оберіть два варіанти.)

- ☐ Можуть бути налаштовані інтерфейси і протоколи маршрутизації.
- ☐ Доступ до режиму глобальної конфігурації можна отримати за допомогою введення команди **enable**.
- ☐ Можна подивитися тільки деякі аспекти налаштування маршрутизатора.
- ☐ Всі команди маршрутизатора доступні.
- ☐ Запит пристрою для цього режиму закінчується символом «>».

3. Який тип доступу захищено на маршрутизаторі Cisco або комутаторі за допомогою команди **enable secret**?

- ◯ Порт AUX
- ◯ Консольна лінія
- ◯ Віртуальні термінали
- ◯ Привілейований режим EXEC

4. Який інтерфейс є інтерфейсом SVI за замовчуванням на комутаторі Cisco?

- ◯ VLAN99
- ◯ VLAN100
- ◯ VLAN999
- ◯ VLAN1

5. Які три угоди про іменування є частиною рекомендацій при налаштуванні імені вузла через командний рядок на пристроях Cisco? (Оберіть три варіанти.)

- ☐ назва вузла має закінчуватися спеціальним символом
- ☐ назва вузла має бути менше 64 символів у довжину
- ☐ назва вузла не повинна містити пробілів
- ☐ назва вузла має починатися з літери
- ☐ назва вузла повинна бути записана літерами нижнього регістру

6. Яка функція оболонки операційної системи?

- ◯ Вона надає послуги захисту від вторгнення для пристрою.
- ◯ Вона взаємодіє з апаратним забезпеченням пристрою.
- ◯ Вона взаємодіє між користувачами та ядром.
- ◯ Вона надає спеціалізовані служби брандмауера.

7. Маршрутизатор з діючою операційною системою містить файл конфігурації, що зберігається в NVRAM. У файлі конфігурації є пароль на привілейований режим, але немає пароля консолі. Коли маршрутизатор завантажиться, який режим буде відображатися?

- ◯ Привілейований режим EXEC
- ◯ Режим налаштування
- ◯ Режим глобальної конфігурації
- ◯ Користувацький режим EXEC

8. Адміністратор щойно змінив IP-адресу інтерфейсу на пристрої IOS. Що ще необхідно зробити для того, щоб застосувати ці зміни до пристрою?

- ◯ Зберегти стартову конфігурацію у файл поточної конфігурації.
- ◯ Нічого не треба робити. Зміни конфігурації на пристрої IOS вступають в силу, як тільки команда набрана правильно і натиснута клавіша Enter.
- ◯ Перезавантажити пристрій і ввести **yes**, коли з'явиться запит на збереження конфігурації.
- ◯ Зберегти поточну конфігурацію у файл стартової конфігурації.

9. Який вид пам'яті на маршрутизаторі або комутаторі Cisco втратить весь контент під час перезавантаження пристрою?

- ◯ NVRAM
- ◯ флеш-пам'ять (flash)
- ◯ оперативна пам'ять (RAM)
- ◯ постійний запам'ятовувальний пристрій (ROM)

10. Чому технік вводить команду **copy startup-config running-config**?

- ◯ для копіювання існуючої конфігурації в оперативну пам'ять
- ◯ щоб видалити всі конфігурації з комутатора
- ◯ щоб змінити налаштування нової стартової конфігурації
- ◯ для збереження поточної конфігурації в NVRAM

11. Які функції надає DHCP?

- ◯ автоматичне присвоєння IP-адреси кожному вузлу
- ◯ тест наскрізного з'єднання
- ◯ дистанційне керування комутатором
- ◯ переклад IP-адрес на доменні імена

12. Які дві функції надає користувачам контекстно-залежна довідка CLI Cisco IOS? (Оберіть два варіанти.)

- ☐ надання повідомлення про помилку під час надсилання неправильної команди
- ☐ вибір найкращої команди для виконання завдання
- ☐ дозволяє користувачеві завершити залишок скороченої команди клавішею TAB
- ☐ визначення того, який параметр, ключове слово або аргумент доступний для введеної команди
- ☐ показ списку всіх доступних команд у поточному режимі

13. У якому місці пам'яті маршрутизатора або комутатора Cisco зберігається файл стартової конфігурації?

- ◯ флеш-пам'ять (flash)
- ◯ NVRAM
- ◯ оперативна пам'ять (RAM)
- ◯ постійний запам'ятовувальний пристрій (ROM)

14. До якої підмережі відноситься IP-адреса 10.1.100.50, якщо використовується маска підмережі 255.255.0.0?

- ◯ 10.1.100.0
- ◯ 10.0.0.0
- ◯ 10.1.0.0
- ◯ 10.1.100.32