ЛАБОРАТОРНА РОБОТА № 4. ВСТАНОВЛЕННЯ КОНСОЛЬНОГО З'ЄДНАННЯ З КОМУТАТОРОМ. НАЛАШТУВАННЯ БАЗОВОЇ КОНФІГУРАЦІЇ КОМУТАТОРА

Тема роботи: Встановлення консольного з'єднання з комутатором. Налаштування базової конфігурації комутатора

Мета роботи: Освоїти принципи конфігурування комутатора на прикладі комутатора Cisco 2960.

Теоретичні відомості

Комутатори Ethernet.

Комутатор – універсальний пристрій 2-го рівня, який використовується для з'єднання декількох вузлів. У більш складному варіанті комутатор підключається до одного чи декількох комутаторів для створення, контролю та обслуговування резервних каналів і з'єднань VLAN. Комутатор однаково обробляє всі типи трафіку, незалежно від їхнього призначення.

Комутатори можуть поділяти локальну мережу LAN на сегменти (segments), які складаються з кількох робочих станцій. Таким чином з одного великого сегменту створюються, вільні від колізій, домени. Комутатори рівня 2 є апаратними. Вони пересилають трафік зі швидкістю, що відповідає швидкості передачі середовища, використовуючи внутрішні схеми, що фізично з'єднують кожен порт з усіма іншими портами.

Комутатор – це пристрій, який направляє потік повідомлень від одного порту до іншого, обробляючи MAC-адресу отримувача в межах даного кадру. Комутатор не підтримує обмін трафіком між різними локальними мережами. У контексті моделі OSI комутатор працює на рівні 2. Рівень 2 - це канальний рівень.

Існує кілька моделей комутаторів Ethernet, здатних задовольнити різні потреби користувачів. Комутатор Ethernet серії Cisco Catalyst 2960 призначений для мереж компаній та філій середнього розміру. Комутатори з цієї серії представлені на рис.8.1.

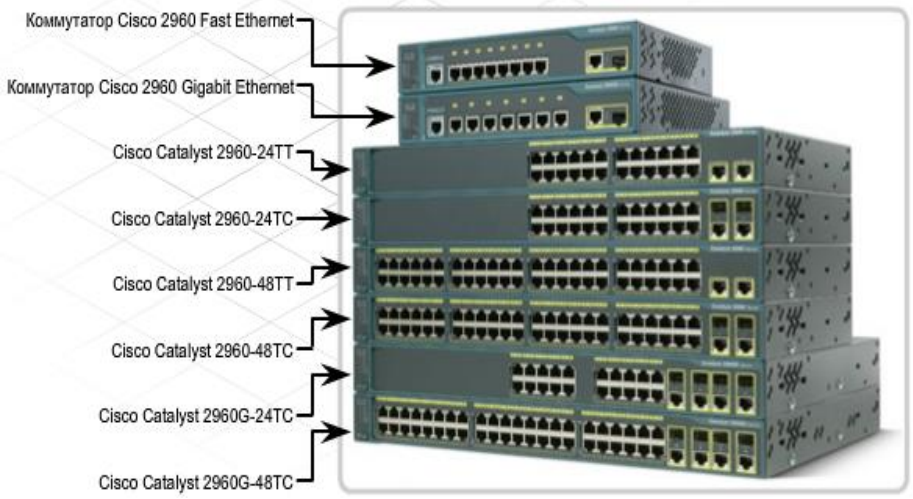

Рис.8.1. Комутатори серії Cisco 2960

Комутатори серії Catalyst 2960 являють собою автономні пристрої фіксованої конфігурації, які не підтримують модулі або слоти для флеш-карт. Оскільки фізичну конфігурацію змінити не можна, комутатори фіксованої конфігурації повинні вибиратися, виходячи з необхідної кількості та типу портів. Комутатори серії 2960 забезпечують зв'язок по протоколу 10/100 Fast Ethernet і 10/100/1000 Gigabit Ethernet. Ці комутатори використовують програмне забезпечення Cisco IOS і налаштовуються за допомогою графічного інтерфейсу користувача SDM або інтерфейсу командного рядка CLI. Передня панель комутатора Cisco 2960 представлена на рис.8.2.

Рис.8.2. Передня панель комутатора Cisco 2960

Режими роботи комутатора

Всі комутатори підтримують як в напівдуплексний, так і повнодуплексний режими роботи.

У режимі напівдуплексу він може або отримувати, або відправляти повідомлення. У режимі повного дуплексу можна і відправляти, і приймати повідомлення одночасно.

Порт і підключений пристрій повинні знаходитися в однаковому режимі. Якщо режими не співпадають, виникає невідповідність дуплексних режимів, надмірна кількість колізій і погіршення якості зв'язку.

Швидкість і режим дуплексу можна або задати вручну, або порт комутатора може виконати автоматичне узгодження. Автоматичне узгодження дозволяє комутатору автоматично визначити швидкість і режим дуплексу пристрою, підключеного до порту. У багатьох комутаторів Cisco автоматичний вибір включається за замовчуванням.

Для успішного виконання автоматичного узгодження, воно повинне підтримуватися обома пристроями. Якщо комутатор знаходиться в режимі автоматичного узгодження, а підключений пристрій не підтримує цей режим, комутатор буде використовувати швидкість цього пристрою (10, 100 або 1000) і перейде в напівдуплексний режим. Якщо по замовчуванню встановити напівдуплексний режим, то можуть виникнути проблеми в разі, коли для пристрою, що не підтримує автоматичне узгодження, заданий повнодуплексний режим.

Якщо підключений пристрій не підтримує автоматичне узгодження, налаштуйте режим дуплексу комутатора вручну, у відповідності з налаштуваннями підключеного пристрою. Параметр швидкості налаштовується сам, навіть якщо підключений порт не підтримує автоматичне узгодження.

Увімкнення комутатора

Для включення комутатора необхідно виконати три основні кроки.

Крок 1. Перевірка компонентів.

Крок 2. Підключення кабелів до комутатора.

Крок 3. Запуск комутатора.

Після запуску комутатора починається його самотестування при включенні живлення (POST). В ході POST проводиться серія перевірок функцій комутатора. Індикатори блимають.

POST закінчується, коли світлоіндикатор SYST починає швидко блимати зеленим кольором. Якщо в процесі POST відбувається збій, індикатор SYST стає жовтим. Якщо комутатор не може виконати POST, необхідно надіслати його для ремонту.

Після завершення всіх стартових процедур можна приступати до налашування комутатора Cisco 2960. Підключення до комутатора із використанням консольного кабелю, представлене на рис.8.3.

Рис.8.3. Підключення до комутатора для початкового конфігурування

Способи конфігурування комутатора

Існує кілька способів налаштування комутатора Cisco і управління ним в локальних мережах:

- Cisco Network Assistant, CNA (Мережевий помічник Cisco);
- Device Manager, SDM (Диспетчер пристроїв Cisco);
- Інтерфейс командного рядка Cisco IOS;
- Програма управління CiscoView;
- Програмні продукти управління мережею SNMP.

У деяких з цих способів для підключення до комутатора використовується IP-адресація або веб-браузер, що вимагає наявності IP-адреси. На відміну від інтерфейсів маршрутизатора, порти комутатора не отримують IP-адрес. Щоб скористатися засобом управління на базі IP або розпочати сеанс Telnet для роботи з комутатором Cisco, потрібно налаштувати для керування IP-адресу комутатора.

Якщо у комутатора немає IP-адреси, слід підключитися безпосередньо до порту консолі і використовувати для налаштування емулятор терміналу.

Налаштування комутатора Cisco Catalyst 2960 виконується на заводі-виробнику. Перед підключенням до мережі необхідно задати тільки основну інформацію про безпеку.

Команди, які потрібні для задавання на комутаторі імені вузла і паролів, є тими ж командами, які використовуються для налаштування ISR. Щоб працювати з комутатором Cisco через засоби керування на базі IP або Telnet, потрібно налаштувати IP-адресу для керування.

Для того, щоб призначити комутатору адресу, ця адреса має бути призначена інтерфейсу віртуальної локальної мережі VLAN. У мережі VLAN кілька фізичних портів можуть бути об'єднані логічно. За замовчуванням існує тільки одна мережа VLAN, яка заздалегідь налаштована в комутаторі – VLAN1, і вона забезпечує доступ до функцій управління.

Щоб створити IP-адресу інтерфейсу управління VLAN 1, потрібно перейти в режим глобальної конфігурації.

Switch> **enable**

Switch # **configure terminal**

Далі, увійдіть в режим конфігурації інтерфейсу для VLAN 1.

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

Задайте IP-адресу, маску підмережі і шлюз за замовчуванням для інтерфейсу управління. IP-адреса має знаходитися в тій же локальній мережі, що і комутатор.

Switch (config-if) # ***ip address 192.168.1.2 255.255.255.0***

Switch (config-if) # ***exit***

Switch (config) # ***ip default-gateway 192.168.1.1***

Switch (config) # ***end***

Збережіть конфігурацію за допомогою команди

Switch # ***copy running-configuration startup-configuration***

Підключення комутатора до мережі

Для підключення комутатора до маршрутизатора потрібно використовувати прямий кабель. Палаючі світлоіндикатори на комутаторі і на маршрутизаторі свідчать про успішність підключення. Схема підключення представлена на рис.8.4.

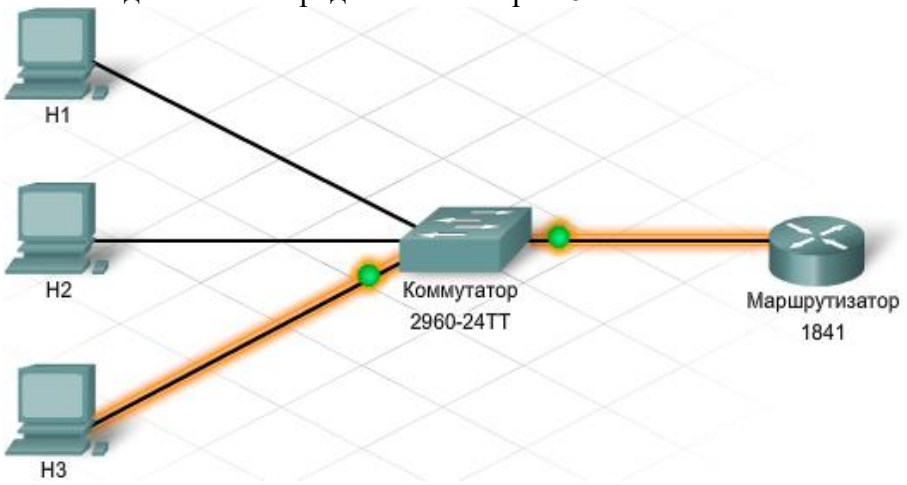

Рис.8.4. Схема підключення комутатора до мережі

Після з'єднання комутатора і маршрутизатора перевірте, чи можуть ці два пристрої обмінюватися повідомленнями.

Перш за все, перевірте налаштування IP-адреси. Використовуйте команду ***show running-configuration***, щоб переконатися в тому, що IP-адреса інтерфейсу управління

комутатора мережі VLAN 1 і IP-адреса безпосередньо підключеного інтерфейсу маршрутизатора знаходяться в одній локальній мережі.

Потім перевірте з'єднання за допомогою команди ping. Відправте з комутатора команду ping на IP-адресу безпосередньо підключеного інтерфейсу маршрутизатора. Повторіть цей процес з маршрутизатора, відправивши команду ping на IP-адресу інтерфейсу управління, призначену комутатору мережі VLAN 1.

Якщо echo-запит виконати не вдалося, перевірте під'єднання і конфігурацію ще раз. Переконайтеся в тому, що всі кабелі підключені правильно і надійно.

Коли між комутатором і маршрутизатором встановлений нормальний обмін даними, можна підключати до комутатора, за допомогою прямих кабелів, окремі ПК. Ці кабелі можуть прямо підключатися до ПК або вони можуть бути частиною структурованої кабельної системи, що йде до стінних розеток.

Безпека портів комутатора

Порти комутатора можуть служити місцями несанкціонованого входу в мережу. Для запобігання цьому, комутатори підтримують функцію, яка називається *захистом портів*. Ця функція обмежує кількість допустимих MAC-адрес на один порт. Порт не буде відправляти пакети з вихідними MAC-адресами, якщо вони не входять у групу заданих адрес.

Існує три способи налаштування безпеки порту.

Статичний

MAC-адреси призначаються вручну, використовуючи команду налаштування інтерфейсу

switchport port-security mac-address <mac-адрес>.

Статичні MAC-адреси зберігаються в таблиці адрес і додаються в поточну конфігурацію.

Динамічний

Динамічно отримані відомості про MAC-адреси зберігаються в таблиці адрес. Кількість отриманих адрес можна контролювати. За замовчуванням на один порт може бути отримано не більше однієї MAC-адреси. Отримані адреси видаляються з таблиці при вимиканні порту або при перезапуску комутатора.

Зв'язаний

Аналогічний динамічному, за винятком того, що адреси зберігаються ще й в поточну конфігурацію.

За замовчуванням безпека порту відключена. Якщо включити функцію безпеки порту, це призведе до несправності при відключенні порту. Наприклад, якщо включити функцію безпеки порту в динамічному режимі і на один порт може бути отримано не більше однієї MAC-адреси, то перша отримана адреса стає безпечною. Якщо інша робоча станція спробує отримати доступ до порту з іншою MAC-адресою, то відбудеться порушення безпеки.

Щоб можна було активувати функцію безпеки порту, необхідно перевести порт у режим доступу за допомогою команди **switchport mode access**.

Для перевірки налаштувань безпеки порту для комутатора або заданого інтерфейсу, скористайтеся командою **show port-security interface interface-id**. На екрані відображатимуться такі вихідні дані:

Максимально допустима кількість безпечних MAC-адрес для кожного інтерфейсу:

- Кількість безпечних MAC-адрес даного інтерфейсу
- Кількість порушень безпеки
- Режим порушення безпеки

Крім цього, при введенні команди **show port-security address,** відображаються безпечні MAC-адреси для всіх портів, а при введенні команди **show port-security** відображаються налаштування безпеки порту для комутатора.

Якщо включена функція безпеки порту для статичного або зв'язаного режиму, то можна використовувати команду **show running-config** для перегляду MAC-адрес, пов'язаних з конкретним портом. Існує три способи видалення отриманої MAC-адреси, яка була збережена в поточній конфігурації:

- Для видалення всіх отриманих адрес слід використовувати команду ***clear port-security sticky interface <№ порту> access***. Потім слід вимкнути порт, ввівши команду ***shutdown***. Нарешті, потрібно знову включити порт за допомогою команди ***no shutdown.***
- Для відключення режиму безпеки порту слід ввести з інтерфейсу команду ***no switchport port-security***. Після відключення знову включіть режим безпеки порту.
- Перезавантажте комутатор

Комутатор буде перезавантажуватися тільки в тому випадку, якщо поточна конфігурація не збережена у файл початкової конфігурації. Якщо ж поточна конфігурація була збережена у файл початковій конфігурації, то це виключає для комутатора можливість повторного отримання адрес при перезавантаженні системи. Однак отримані MAC-адреси будуть завжди пов'язані з конкретним портом до тих пір, поки не буде проведена очистка порту за допомогою команди ***clear port-security*** або не буде відключений режим безпеки порту. Якщо це буде зроблено, не забудьте перезберегти поточну конфігурацію в файл початкової конфігурації, щоб комутатор після перезавантаження не почав використовувати вихідні MAC-адреси.

Якщо на комутаторі є порти, що не використовуються, рекомендується відключити їх. Відключення портів на комутаторі виконується просто. Переходячи до кожного невикористовуваного порту, слід ввести команду ***shutdown***. Якщо потім треба буде активувати цей порт, введіть команду ***no shutdown*** за допомогою відповідного інтерфейсу.

Крім включення режиму безпеки порту і відключення невикористовуваних портів, існують інші налаштування безпеки комутатора, які дозволяють встановлювати паролі на порти ***vty***, застосовувати банери входу в систему і зашифровувати паролі за допомогою команди ***service password-encryption***.

Протокол знаходження пристроїв Cisco

Протокол виявлення пристроїв Cisco (CDP) – це засіб збору інформації, що використовується комутатором, ISR або маршрутизатором для обміну даними з іншими, безпосередньо підключеними, пристроями Cisco. За замовчуванням CDP починає працювати при завантаженні пристрою. Потім цей засіб періодично відправляє підключеним пристроям повідомлення, відомі як оголошення CDP.

CDP працює тільки на рівні 2. Його можна використовувати в різних типах локальних мережах, включаючи Ethernet і послідовні мережі. Протокол рівня 2 дозволяє визначити статус безпосередньо підключеного каналу за відсутності IP-адреси або при неправильному налаштуванні адреси.

Два пристрої Cisco, безпосередньо підключені до однієї і тієї ж локальної мережі, називаються сусідніми. Концепція сусідніх пристроїв важлива для розуміння вихідних даних команд CDP.

CDP збирає таку інформацію:

- Ідентифікатори пристроїв - задані імена вузлів;
- Список адрес - адреси рівня 3, якщо вони налаштовані;
- Ідентифікатор порту - безпосередньо підключений порт, наприклад, послідовний порт 0/0/0;
- Список функцій - одна або декілька функцій, які виконуються пристроєм;
- Платформа - апаратна платформа пристрою, наприклад, Cisco 1841.

Для перегляду інформації, зібраної CDP, не потрібно вхід на віддалені пристрої. Оскільки CDP збирає і відображає багато інформації про безпосередньо підключені сусідні пристрої, не заходячи на них, в мережах виробничих підприємств його, зазвичай, відключають в цілях безпеки. Крім того, CDP використовує частину смуги пропускання і може впливати на продуктивність мережі.

Порядок виконання роботи

1. Створіть конфігурацію мережі та встановіть зв’язок з комутатором через програму HyperTerminal рис.8.5, використовуючи для з'єднання консольний кабель.

Рис.8.5. Підключення до комутатора з використанням консольного кабелю

На ПК запустіть програму HyperTerminal з такими параметрами:

Bits Per Second = 9600
Data Bits = 8
Parity = None
Stop Bits = 1
Flow Control = None

2. Включення комутатора.

a) Підключіть шнур живлення до комутатора Cisco 2960 і електричної розетки, щоб включити комутатор.
b) Слідкуйте за повідомленнями, які виводяться під час запуску у вікні програми емуляції терміналу. Під час появи повідомлень не натискайте жодних клавіш на клавіатурі. Натискання клавіші перериває процес запуску комутатора. У відображуваних повідомленнях запуску вказується обсяг флеш-пам'яті на комутаторі, версія операційної системи Cisco IOS та інша інформація.

3. Видалення початкової конфігурації та перезавантаження комутатора.

a) Перейдіть в привілейований режим EXEC, ввівши команду enable. Якщо отримаєте запит на введення паролю, введіть class.
Switch> ***enable***
b) Видаліть інформаційний файл бази даних віртуальної локальної мережі.
Switch# ***delete flash: vlan.dat***
Delete filename [vlan.dat]? [Enter]
Delete flash: vlan.dat? [confirm] [Enter]
c) За відсутності файлу віртуальної локальної мережі відображається повідомлення:
% Error deleting flash: vlan. dat (No such file or directory)
d) Видаліть файл початкової конфігурації комутатора з NVRAM.
Switch# **erase startup-config**
Після цього з'явиться повідомлення:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Для підтвердження натисніть клавішу **Enter**. Послідує наступне повідомлення:
Erase of nvram: complete
e) Перезавантажте програмне забезпечення, ввівши команду reload в привілейованому режимі EXEC.
*Switch#****reload***

4. Налаштування імені вузла комутатора. Задайте ім'я вузла комутатора **CustomerSwitch**, використовуючи команди:

Switch> ***enable***
Switch# ***configure terminal***
Switch(config)# ***hostname CustomerSwitch***

5. Налаштування паролю і секретного паролю в привілейованому режимі:

a) в режимі глобальної конфігурації задайте в якості значення паролю **cisco**:
CustomerSwitch(config)# ***enable password cisco***
b) в режимі глобальної конфігурації задайте в якості значення таємного паролю **cisco123**:

CustomerSwitch(config)# ***enable secret cisco123***

6. Налаштування паролю консолі.

a) в режимі глобальної конфігурації переключіться в режим налаштування лінії консолі:

CustomerSwitch (config)# ***line console 0***
CustomerSwitch (config-line)#

b) в режимі налаштування лінії задайте пароль cisco і вкажіть умову вводу паролю при кожному вході в систему:

CustomerSwitch (config-line)# ***password cisco***
CustomerSwitch (config-line)# ***login***
CustomerSwitch (config-line)# ***exit***

7. Налаштування паролю vty.

a) в режимі глобальної конфігурації переключіться в режим налаштування для ліній vty з 0 до 15:

CustomerSwitch (config)# ***line vty 0 15***
CustomerSwitch (config-line)#

b) в режимі налаштування лінії задайте пароль **cisco** і вкажіть умову вводу паролю при кожному вході в систему:

CustomerSwitch (config-line)# ***password cisco***
CustomerSwitch (config-line)# ***login***
CustomerSwitch (config-line)# ***exit***

8. Налаштування IP-адреси для інтерфейсу VLAN1.

a) в режимі глобальної конфігурації переключіться в режим налаштування інтерфейсу для VLAN1 і призначте IP-адресу 192.168.1.5 з маскою підмережі 255.255.255.0:

CustomerSwitch (config)# ***interface VLAN1***
CustomerSwitch (config-if)# ***ip address 192.168.1.5 255.255.255.0***
CustomerSwitch (config-if)# ***no shutdown***
CustomerSwitch (config-if)# ***exit***

9. Налаштування шлюзу по замовчуванню.

a) в режимі глобальної конфігурації призначте шлюзу по замовчуванню адресу 192.168.1.1:

CustomerSwitch (config)# ***ip default-gateway 192.168.1.1***

10. Налаштування параметрів порту комутатора:

CustomerSwitch (config)# ***interface fastEthernet 0/1***
CustomerSwitch (config-if)# ***duplex full***
CustomerSwitch (config-if)# ***speed 100***
CustomerSwitch (config-if)#

11. Перевірка конфігурації комутатора.

Введіть команду ***show running-config***, щоб перевірити налаштування IP-адреси комутатора.

CustomerSwitch# ***show running-config***
Building configuration...
Current configuration : 1283 bytes
!
version 12,2
no service pad
hostname CustomerSwitch
!
enable secret 5 1XUe/$ch4WQ/SpcFCDd2iqd9bda/
enable password cisco
!
interface FastEthernet0/1
!
interface FastEthernet0/24
!
interface Vlan1

ip address 192.168.1.5 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
line con 0
password cisco123
login
line vty 0 4
password cisco123
login
line vty 5 15
password cisco123
login
! end

12. Збереження текучої конфігурації.

CustomerSwitch# ***copy running-config startup-config***

13. Оформіть звіт про виконання даної роботи.

Контрольні питання

1) На якому рівні працює комутатор та які основні функції він виконує?
2) Які базові налаштування задаються при конфігуруванні комутатора?
3) Про що інформують LED на передній панелі комутатора?
4) Які відмінності між командами enable secret class та enable password class?
5) Яка команда відображає в консолі конфігурацію комутатора?

Чим відрізняються комутатори другого та третього рівнів?