**Практична робота № 10**

**ЗАХИСТ КОМУТАТОРІВ І МАРШРУТИЗАТОРІВ**

**Мета роботи**: Навчитися ставити парольний захист на комутатор і маршрутизатор на різні режими роботи.

Робота з програмним забезпеченням: CPT.

**1. Теоретичні відомості**

Мережеві пристрої можуть працювати в режимах, які поділяються на три великі категорії.

**Перша і основна категорія**-це передача даних (площину даних, data plane). Це режим роботи комутатора з передачі кадрів, що генеруються пристроями, підключеними до комутатора. Іншими словами, передача даних є основним режимом роботи комутатора.

**По-друге**, управління передачею даних відноситься до налаштувань і процесам, які керують і змінюють вибір, зроблений передає рівнем комутатора. Системний адміністратор може контролювати, які інтерфейси включені і відключені, які порти працюють з якою швидкістю, як сполучна дерево блокує деякі порти, щоб запобігти цикли, і так далі. Так само важливою частиною є управління пристроєм, здійснюване через площину спостереження (management plane). Площина спостереження - це управління самим пристроєм, а не управління тим, що робить пристрій.

**Захист комутатора через CLI**

За замовчуванням комутатор Cisco Catalyst дозволяє будь-якому користувачеві підключитися до консольного порту, отримати доступ до призначеного для користувача режиму, а потім перейти в привілейований режим без будь-якого захисту. Ці настройки задані в мережевих пристроях Cisco за замовчуванням і, якщо у вас є фізичний доступ до пристрою, то ви спокійно можете підключитися до пристрою через консольний порт або USB, використовуючи відповідний кабель і відповідно виробляти різні настройки.

Однак не завжди є фізичний доступ до комутатора і тоді необхідно мати доступ до пристроїв для віддаленого управління, і першим кроком в цьому процесі є забезпечення безпеки комутатора так, щоб тільки відповідні користувачі могли отримати доступ до інтерфейсу командного рядка комутатора (CLI).

**Налаштування парольного доступу до комутатора Cisco**

Захист CLI включає захист доступу в привілейований режим, оскільки з цього режиму зловмисник може перезавантажити комутатор або змінити конфігурацію.

Захист призначеного для користувача режиму також важлива, оскільки зловмисники можуть бачити настройки комутатора, отримати настройки мережі і знаходити нові способи атаки на мережу.

Особливо важливо, щоб всі протоколи віддаленого доступу і управління, щоб IP-налаштування комутатора були налаштовані і працювали.

Для того, щоб отримати віддалений доступ по протоколах Telnet і Secure Shell (SSH) до комутатора, необхідно на комутаторі налаштувати IP-адресацію.

**Захист призначеного для користувача і привілейованого режиму за допомогою простих паролів.**

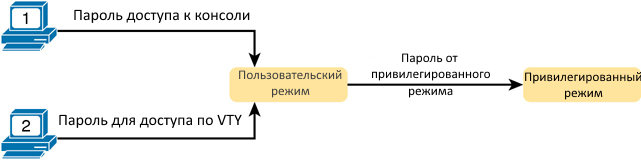
Отримати повний доступ до комутатора Cisco можна тільки через консольний порт.

В цьому випадку, налаштування за замовчуванням, дозволяють отримати доступ спочатку до режиму користувача, а потім можна перейти в привілейований режим без використання паролів.

А ось по протоколам віддаленого доступу Telnet або SSH отримати доступ навіть до режиму користувача неможливо.

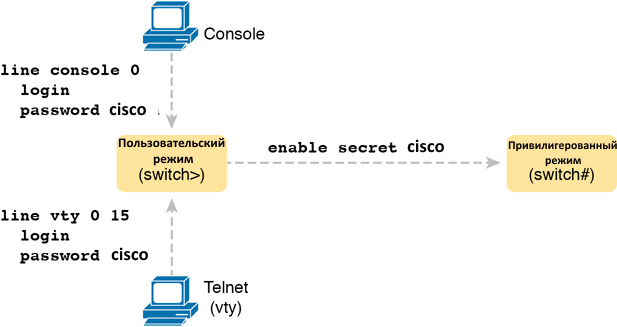
Налаштування за замовчуванням йдуть у зовсім нового комутатора, але у виробничому середовищі необхідно забезпечити безпечний доступ через консоль, а також включити віддалений вхід через Telnet і / або SSH, щоб була можливість підключатися до всіх комутаторів в локальній мережі.

Можна організувати доступ до мережного обладнання з використанням одного загального пароля.

Цей метод дозволяє підключитися до обладнання, використовуючи тільки пароль - без введення імені користувача - з одним паролем для входу через консольний порт і іншим паролем для входу по протоколу Telnet. Користувачі, які підключаються через консольний порт, повинні ввести пароль консолі, який був попередньо налаштований в режимі конфігурації. Користувачі, які підключаються через протокол Telnet, повинні ввести пароль від Telnet, також званий паролем vty, так званий, тому що це режим конфігурації термінальних ліній (vty). На малюнку 1 представлені варіанти використання паролів з точки зору користувача, що підключається до комутатора.

Як видно з малюнка 1, на комутаторах Cisco стоїть захист привілейованого режиму (enable) за допомогою ще одного загального пароля, що задається командою enable password. Системний адміністратор, який підключається до CLI комутатора потрапляє в режим користувача і далі, вводить команду enable.

Ця команда запитує у користувача пароль входу в привілейований режим; якщо користувач вводить правильний пароль, IOS переміщує користувача в привілейований режим.

Щоб налаштувати загальні паролі для консолі, Telnet і привілейованого режиму (enable), необхідно ввести кілька команд. На рис. 2 показаний порядок завдання всіх трьох паролів.

На рисунку показані два ПК, які намагаються отримати доступ до режиму управління пристроєм. Один з ПК підключений за допомогою консольного кабелю, що з'єднується через лінію console 0, а інший за допомогою Telnet, що з'єднується через термінальну лінію vty 0 15. Обидва комп'ютери не мають Логінов, пароль для консолі і Telnet -cisco. Призначений для користувача режим отримує доступ до привілейованого режиму (enable) за допомогою введення команди "enable secret cisco". Для настройки цих паролів не треба докладати багато зусиль. Все робиться легко. По-перше, конфігурація консолі і пароля vty встановлює пароль на основі контексту: для консолі (рядок con 0) і для ліній vty для пароля Telnet (рядок vty 0 15). Потім в режимі консолі і режимі vty, відповідно вводимо команди:

login

password <пароль задається користувачем>

Налаштований пароль привілейованого режиму, показаний в правій частині малюнка, застосовується до всіх користувачів, незалежно від того, підключаються вони до призначеного для користувача режиму через консоль, Telnet або іншим чином. Команда для настройки enable password є командою глобальної конфігурації: enable secret <пароль користувача>.

У старих версіях, для завдання пароля на привілейований режим, використовувалася команда password. В сучасних IOS застосовується два режими завдання пароля: password і secret.

Рекомендується використовувати команду secret, так як вона найбільш безпечна в порівнянні з password.

Для правильного налаштування захисту комутатора Cisco паролями необхідно слідувати по кроках, зазначеним нижче:

**Крок 1.** Задайте пароль на привілейований режим командою enable secret password-value

**Крок 2.** Задайте пароль на доступ по консолі

1. Використовуйте команду line con 0 для входу режим конфігурації консолі;

2. Використовуйте команду password password-value для завдання пароля на консольний режим;

3. Використовуйте команду login для запиту пароля при вході по консолі;

**Крок 3.** Задайте пароль на термінальні підключення vty (Telnet)

1. Використовуйте команду line vty 0 15 для входу режим конфігурації термінальних ліній. В даному прикладі налаштування будуть застосовані до всіх 16 термінальним лініях;

2. Використовуйте команду password password -value для завдання пароля на режим vty;

3. Використовуйте команду login для запиту пароля при вході по Telnet

У прикладі 2 показаний процес налаштування, відповідно до описаних вище кроків, а також установка пароля enable secret. Рядки, які починаються з! - це рядки коментарів. Вони призначені для коментування призначення команд.

! Enter global configuration mode, set the enable password, and also set the hostname (just because it makes sense to do so)

Switch # configure terminal

Switch (config) # enable secret cisco

Switch # (config) # line console 0

Switch # (config-line) # password cisco

Switch # (config-line) # login

Switch # (config-line) # exit

Switch # (config) # line vty 0 15

Switch # (config-line) # password cisco

Switch # (config-line) # login

Switch # (config-line) # end

Switch #

**2. Завдання на практичну роботу.**

1. Створити в CPT локальну мережу, що складається з 1 комутатора, 1 маршрутизатора і 4 комп'ютерів.

2. Створити таблицю IP адрес.

3. Налаштувати IP адресацію пристроїв мережі.

4. Встановити паролі на призначений для користувача і привілейований режим комутатора, використовуючи консольний з'єднання.

5. Установити паролі на призначений для користувача і привілейований режим комутатора, використовуючи консольний з'єднання.

6. В якості пароля користувача режиму використовувати власне ім'я.

7. В якості пароля привілейованого режиму використовувати власне прізвище.

8. Провести перевірку отриманих налаштувань.

9. Зберегти файл.