# КОНФИГУРИРОВАНИЕ СЕТЕВЫХ УСТРОЙСТВ ФИРМЫ CISCO

# Конфигурирование коммутаторов

### Конфигурирование паролей на подключение к устройству

Пароли обеспечивают некоторый уровень защиты коммутатора, предотвращающий неавторизованное подключение к нему. Комму- таторы Catalyst стандартно имеют два уровня парольной защиты: пользовательский и привилегированный. Для обеспечения защиты устройства следует применять аутентификацию пользователя с ис- пользованием локальной базы коммутатора и шифрование паролей. Пароль уровня пользователя предотвращает доступ неавтори- зованных лиц к интерфейсу командной строки (CLI) из Telnet- или консольного сеанса. Он настраивается для каждой линии подклю- чения отдельно с помощью команд **password**, параметром кото- рой является устанавливаемый пароль, и **login** без параметров. Команда **login** обеспечивает процесс аутентификации пользова- теля и является обязательной для линий подключения IOS-коммутаторов. До тех пор, пока пароль не будет установлен или в конфигурации линии будет отсутствовать команда **login**, подключение по Telnet невозможно. Выбор той или иной линии для ее конфигурирования осуществляется с помощью команды режима

глобального конфигурирования:

**Switch(config)#line con 0** – для консольной линии,

**Switch(config)#line vty 0 4** – для линий виртуального

терминала в диапазоне номеров с 0 по 4.

## ВЫПОЛНИТЬ!

1. В текущей конфигурации найти команды, устанавливающие пароли на линии **con** и **vty**.
2. Установить пароль **console** для линии **con0**.
3. Выйти из сеанса консоли с помощью команды **logout** и войти в новый сеанс, используя введенные данные аутентификации.

Пароль привилегированного режима предотвращает доступ неавторизованных лиц к соответствующему режиму, в котором мо- гут вноситься изменения в конфигурацию коммутатора и осу- ществляться другие функции администрирования. Он задается с помощью команды **enable secret**, обеспечивающей его шиф- рование, устаревшая команда **enable password** не шифрует па- роль и оставлена для совместимости с программным обеспечением ранних версий, причем во второй команде пароль должен отличать- ся от устанавливаемого в первой.

## ВЫПОЛНИТЬ!

1. В текущей конфигурации найти команды, устанавливающие пароль для входа в привилегированный режим.

Для того чтобы пароли не хранились в файле конфигурации в открытом виде, можно использовать встроенную службу шифро- вания, но учтите, что она не обеспечивает их шифрование, а при- звана лишь усложнить чтение паролей с экрана. Указанная служба запускается командой:

# service password-encryption.

## ВЫПОЛНИТЬ!

1. Запустить службу шифрования паролей и в текущей конфигурации найти команды, устанавливающие пароли.

Как упоминалось ранее, предпочтительнее применять аутен- тификацию пользователя с использованием локальной базы данных коммутатора, для чего сначала создаются записи локальной базы пользователей с помощью команды:

# Switch(config)#username <имя> privilege

**<уровень> secret <пароль>.**

Затем для каждой линии подключения к коммутатору указы- вается команда **login** с параметром локальной аутентификации: **Switch(config-line)#login local.**

## ВЫПОЛНИТЬ!

1. Создать запись в локальной базе данных аутентификации о пользователе **admin** c уровнем привилегий **0** и секретным паролем **cisco**.
2. Настроить линии **con0** и **vty0** – **vty4** на использование локальной аутентификации. Для отмены старых паролей можно использовать команду:

# Switch(config-line)#no password.

1. Выйти из сеанса консоли и войти в новый сеанс, используя введенные данные аутентификации.
2. В текущей конфигурации найти команды, устанавливающие действующие на коммутаторе пароли.
3. Сохранить текущую конфигурацию.