Доступ к устройству по telnet, ssh

1.Установка пароля на доступ к привилегированному режиму.
Для установки пароля на доступ к привилегированному режиму перейдем в режим глобальной конфигурации и установим пароль.

```
router#config terminal
router(config)#enable secret cisco
router(config)#enable password ciscocisco
```

Команда enable secret создает зашифрованный пароль
Команда enable password хранит пароль в открытом виде

При использовании одновременно двух команд приоритет отдается enable secret, а пароль в enable password не используется, так же не рекомендуется использовать одинаковый пароль в этих командах.

2.Установка пароля на доступ устройству через консольный порт.

```
router#configure terminal
router(config)#line console 0
router(config-line)#password cisco
router(config-line)#login
router(config-line)#end
```

3.Установка пароля на доступ устройству через telnet.

```
router#configure terminal
router(config)#line vty 0 15
router(config-line)#password cisco
router(config-line)#login
```

В данном случае пароль установлен на все 16 линий, если нужно то можно менять диапазон, например line vty 0 4.

Смотрим что у нас получилось. Ниже приведены интересующие нас строчки из running-config

```
router#show running-config
!
enable secret 5 $1$tasv$QdGGQJIj.PEPk3sz66NMe/
enable password ciscocisco
!
!
line con 0
exec-timeout 0 0
privilege level 15
password cisco
logging synchronous
login line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
 password cisco
login line vty 5 15
 password cisco
 login
!
```

Проверяем подключение

4. Включаем шифрование паролей.

Как мы видим пароли в конфигурации лежат в открытом виде, зашифруем их для этого используем команду **service password-encryption** в режиме глобальной конфигурации.

```
router#configure terminal
router(config)#service password-encryption
```

Смотрим что получилось

```
router#show running-config
!
enable secret 5 $1$tasv$QdGGQJIj.PEPk3sz66NMe/
enable password 7 00071A150754080F1C2243
!
line con 0
exec-timeout 0 0
privilege level 15
```

```
password 7 1511021F0725
logging synchronous
login
line vty 0 4
password 7 110A1016141D
login line vty 5 15
password 7 110A1016141D
login
!
```

Пароли зашифрованы, если перед хешем пароля стоит цифра 5 то пароль зашифрован алгоритмом MD5 и плохо поддается дешифровке, а цифра 7 обозначает слабый алгоритм шифрования, который легко подвержен дешифровке.

5. Настройка доступа по ssh

Пароли передаваемые протоколом telnet никак не шифруются, и могут быть перехвачены, для того чтоб этого не случилось настроим доступ к устройству через протокол ssh.

Для генерации ключа ssh необходимо задать ip domain-name.

```
router(config)#ip domain-name test.dom
```

Генерируем ключ ssh, размер ключа указываем максимально возможный 2048

```
router(config)#crypto key generate rsa general-keys modulus 2048
```

Создаем пару логин пароль

```
router(config)#username admin secret cisco
```

В конфигурации линий vty 0-15 покажем что логин берется из локальной базы и входящий протокол будет ssh

```
router(config)#line vty 0-15
router(config-line)#login local
router(config-line)#transport input ssh
```

По умолчанию CISCO включает версию ssh 1.99

```
router#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

изменим её на ssh 2 командой

```
router#config t
router(config)#ip ssh version 2
```

проверяем

```
router#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

Пробуем подключится

Для большей безопасности на вход line vty можно повесить стандартный access-list со списком разрешенных хостов.

Создаем стандартный access-list 2 разрешающий хост 10.1.2.3, остальные он запрещает по умолчанию.

```
router#configure terminal
router(config)#access-list 2 permit 10.1.2.3
```

Весим его на вход line vty 0 15

```
router#configure terminal
router(config)#line vty 0 15
router(config-line)#access-class 2 in
```

Проверяем