

Элементы конфигурации Cisco

Contents

1 Введение	1
1.1 Цели	1
1.2 Замечания	1
2 Упражнения, часть I	2
2.1 Работа в группе	2
2.2 Зайдите на ваш роутер	2
2.3 Настройте роутер использовать только SSH	2
3 ЗАМЕЧАНИЯ	6

1 Введение

1.1 Цели

- Освоить базовый набор команд IOS, требующихся для настройки SSH на вашем роутере или маршрутизаторе Cisco

1.2 Замечания

- Команды, предваряемые “\$” означают, что они должны быть выполнены с правами обычного пользователя – а не администратора.
- Команды, предваряемые “#” означают, что вы должны иметь права администратора.
- Команды с более специфичными подсказками (например “rtrX>” или “mysql>”) означают что вы выполняете их либо на удаленном оборудовании, либо в какой-то другой программе.
- Если строка команды заканчивается символом “”, это означает, что команда продолжается на следующей строки и что вам следует считать это одной строкой.

2 Упражнения, часть I

2.1 Работа в группе

Во время выполнения этого упражнения работайте в группе. Выберите одного человека набирать на клавиатуре. В группе должно быть 4 человека. Например, члены группы 1 – это люди на pc1–pc4, группа 2 использует pc5–pc8, и т.д..

Если вы не уверены, в какой вы группе, обратитесь к диаграмме сети, расположенной на wiki для класса – посетите <http://noc.ws.nsrc.org/> и нажмите на ссылку Network Diagram.

2.2 Зайдите на ваш роутер

Залогиньтесь на вашу vm/pc и установите Telnet:

```
$ sudo apt-get install telnet
```

Если он уже установлен, тоже хорошо.

Теперь зайдите на роутер вашей группы:

```
$ telnet 10.10.N.254
```

```
username: cisco
```

```
password: cisco
```

Выведите информацию о вашем роутере:

```
routerN>enable
```

```
Password: (пароль по умолчанию "cisco")
```

```
RouterN#show run (пробел для пролистывания)
```

```
RouterN#show int FastEthernet0/0
```

```
RouterN#show ? (показывает все возможности)
```

```
RouterN#exit (уйти с роутера)
```

2.3 Настройте роутер использовать только SSH

Эти шаги сделают следующее:

- Создадут ssh ключ для вашего роутера
- Создадут зашифрованный пароль для пользователя cisco

- Зашифруют пароль администратора (cisco)
- Запретит telnet (нешифрованный) доступ к вашему роутеру
- Разрешит SSH (версии 2) доступ к вашему роутеру

Вы должны работать в группах по 4 человека. Соберитесь вместе с другими членами вашей группы и выберите одного человека набирать команды. Для начала, подсоединитесь к одной из PC вашей группы. Оттуда используйте telnet для подключения к роутеру:

```
$ telnet rtrN.ws.nsrc.org (or "telnet 10.10.N.254")
```

```
username: cisco
password: cisco
```

```
rtrN> enable (сокращенно en)
password: cisco
rtrN# configure terminal (сокращенно conf t)
rtrN(config)# aaa new-model
rtrN(config)# ip domain-name ws.nsrc.org
rtrN(config)# crypto key generate rsa
```

```
How many bits in the modulus [512]: 2048
```

Подождите создания ключа. Теперь вы можете указывать пароли и они будут зашифрованы. Первым делом давайте временно удалим нашего пользователя "cisco", потом мы его воссоздадим.

КРИТИЧНО ВАЖНО! КРИТИЧНО ВАЖНО!

ПОЖАЛУЙСТА, НЕ ИСПОЛЬЗУЙТЕ НИЧЕГО КРОМЕ ПАРОЛЯ ДЛЯ КЛАССА И ПОЛЬЗОВАТЕЛЯ "CISCO"

Если вы используете другие имена или пароли, вы поломаете упражнения для других участников класса в течение недели.
Спасибо!

```
rtrN(config)# no username cisco
rtrN(config)# username cisco secret 0 <CLASS PASSWORD>
```

Теперь пароль пользователя cisco () зашифрован. Следующим шагом, зашифруем и пароль администратора (enable):

```
rtrN(config)# enable secret 0 <CLASS PASSWORD>
```

Теперь скажем роутеру разрешать только SSH соединения на пяти существующих консолях (vty от 0 до 4):

```
rtrN(config)# line vty 0 4
rtrN(config-line)# transport input ssh
rtrN(config-line)# exit
```

Мы вышли из конфигурации линии и пришли назад в режим общей конфигурации. Теперь мы скажем роутеру логировать события, связанные с SSH, и только разрешать соединения по SSH версии 2:

```
rtrN(config)# ip ssh logging events
rtrN(config)# ip ssh version 2
```

Теперь выйдем из режим конфигурации:

```
rtrN(config)# exit
```

И сохраним эти изменения в постоянной памяти:

```
rtrN# write memory          (wr mem)
```

Хорошо. Теперь вы более не можете использовать telnet для осуществления соединения к вашему роутеру. Вы должны подсоединяться используя SSH, пользователя "cisco" и пароль . Пароль администратора тоже . Естественно, в реальной работе вам следует использовать гораздо более сложные пароли.

Прежде чем вы выйдете из сессии telnet, не забудьте протестировать соединение ssh с другой PC в вашей группе (или откройте другое окно терминала). Это нужно сделать потому, что если вы сделали ошибку конфигурации, и выйдете из сессии telnet, вы можете потерять все способы осуществления нового соединения.

Первым делом, попробуйте подсоединиться через telnet:

```
$ telnet rtrN.ws.nsrc.org
```

Что произойдет? Вы должны увидеть что-то вроде:

```
Trying 10.10.N.254...
telnet: Unable to connect to remote host: Connection refused
```

Теперь осуществите соединение через SSH:

```
$ ssh cisco@rtrN.ws.nsrc.org
```

Вы должны увидеть что-то вроде:

```
The authenticity of host 'rtr2.ws.nsrc.org (10.10.2.254)' can't be
established. RSA key fingerprint is 93:4c:eb:ad:5c:4a:a6:3e:8b:9e:
4f:e4:e2:eb:e4:7f. Are you sure you want to continue connecting
(yes/no)?
```

Введите “yes” и нажмите ВВОД...

Теперь вы видите:

```
Password: <CLASSS PASSWORD>
rtrN>
```

Наберите “enable”, чтобы иметь возможность выполнять привилегированные команды:

```
rtrN> enable
Password: <CLASS PASSWORD>
rtrN#
```

Теперь посмотрим текущую конфигурацию роутера:

```
rtrN# show running (sh run)
```

Нажимайте пробел для пролистывания экранов. Обратите внимание на строки типа:

```
enable secret 5 $1$p4/E$PnPk6VaF8QoZMhJx56oXs.
.
.
.
username cisco secret 5 $1$uNg1$M1yscHhYs..upaPP4p8gX1
.
.
.
line vty 0 4
exec-timeout 0 0
transport input ssh
```

Вы можете увидеть, что и пароль администратора, и пароль пользователя cisco теперь зашифрованы. Это хорошо.

Теперь выйдите с роутера для завершения этого упражнения:

```
rtrN# exit
```

И, если у вас до сих пор открыта старая сессия telnet в другом окне, не забудьте выйти и оттуда.

3 ЗАМЕЧАНИЯ

1. Если вы не можете зайти на роутер после этого упражнения, дайте знать преподавателю, и он сбросит конфигурацию роутера к исходному состоянию.
2. Сделайте это упражнение только один раз. Если несколько человек будут делать это упражнение, весьма вероятно, что доступ к роутеру будет поломан.
3. В течение этого курса вы будете настраивать на вашем роутере такие вещи, как SNMP, Netflow, и другие. С этого момента вы можете просто использовать SSH с вашего ноутбука для осуществления соединения.