LearnCisco.Ru

- Настройка и конфигурирование Cisco с нуля.
- Учебные материалы и видео курсы для чайников и новичков.
- Практические примеры и рекомендации.
- Все самое необходимое для начинающих.

«Cisco для практиков»

Подготовка маршрутизатора, коммутатора Cisco к работе

Алексей Николаев, CCIE# 27142
e-mail: anikolaev@learncisco.ru
Web: LearnCisco.Ru

LearnCisco.Ru

План Занятия:

- Уровни доступа в Cisco IOS (privilege level)
- Режим конфигурации (configure terminal)
- Рекомендуемые начальные настройки
- Простые способы аутентификации, удаленный доступ по Telnet
- Удаленный доступ по SSH, защита удаленного доступа
- Дополнительные настройки возможности
- Полезности

LearnCisco.Ru

Уровни доступа в Cisco IOS (privilege levels):

- В Cisco IOS есть 16 уровней доступа (privilege levels, с 0 по 15)
- По умолчанию существуют 3 пользовательских уровня в IOS:

  - Privilege level 0 (включает команды disable, enable, exit, help и logout)
  - Privilege level 1 (это пользовательский EXEC режим, обычный уровень на консольной и Telnet сессиях. Он включает пользовательские команды, подсказка командной строки выглядит: Router>)
  - Privilege level 15 (это привилегированный EXEC режим (режим enabled). Включает все команды (подсказка: Router#)

- Переключения между уровнями доступа – enable <0-15>
- Посмотреть текущий уровень доступа - show privilege

LearnCisco.Ru

Режим конфигурации (configure terminal):

- Режим глобальной конфигурации - configure terminal

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

- Режим конфигурирования какой либо секции, например интерфейса:

```
Router(config)#
Router(config)#interface fastEthernet 0/0
Router(config-if)#
```

- Выход из режима конфигурации:

Exit – на предыдущий уровень
Crtl-Z – выход из режима конфигурации

LearnCisco.Ru

Рекомендуемые начальные настройки:

- Задать enable пароль (на privilege level 15)
  Router(config)#enable password cisco

- Задать имя хоста hostname
  Router(config)#hostname Rack1R1
  Rack1R1(config)#

- Задать имя домена ip domain-name
  Rack1R1(config)#ip domain-name learncisco.ru

- Отключить domain lookup
  Rack1R1(config)#no ip domain lookup

LearnCisco.Ru

Рекомендуемые начальные настройки:

- Консоль

```
Rack1R1(config)#line con 0
Rack1R1(config-line)#exec-timeout 0 0
Rack1R1(config-line)#logging synchronous
```

- Терминальные линии

```
Rack1R1(config)# line vty 0 4
Rack1R1(config-line)#exec-timeout 0 0
Rack1R1(config-line)#logging synchronous
```

- Установить часовой пояс и время

```
Rack1R1(config)#clock timezone MSK +3
Rack1R1(config)#exit
Rack1R1#clock set 12:00:00 13 Sep 2011
```

LearnCisco.Ru

Простые способы аутентификации, удаленный доступ по Telnet:

- Простой пароль на Telnet сессию (line password)

```
Rack1R1(config)#line vty 0 4
Rack1R1(config-line)#password cisco
Rack1R1(config-line)#login
```

- Аутентификация через локальную базу пользователей (local authentication)

```
Rack1R1(config)#username cisco privilege 15 password cisco
Rack1R1(config)#line vty 0 4
Rack1R1(config-line)#login local
```

Или

```
Rack1R1(config)#aaa new-model
Rack1R1(config)#aaa authentication login default local
```

LearnCisco.Ru

Удаленный доступ по SSH, защита удаленного доступа:

- Задать имя хоста hostname
  Router(config)#hostname Rack1R1
  Rack1R1(config)#

- Задать имя домена ip domain-name
  Rack1R1(config)#ip domain-name learncisco.ru

- Сгенерировать RSA ключи (если длинна ключа менее 768bit, то будет включен SSH v.1.5, если 768bit и больше, то SSH v.1.99)
  Rack1R1(config)#crypto key generate rsa modulus 1024

- Посмотреть ключи
  Rack1R1#show crypto key mypubkey rsa

LearnCisco.Ru

Удаленный доступ по SSH, защита удаленного доступа:

- Разрешить только требуемые протоколы, например Telnet/SSH
  Rack1R1(config)#line vty 0 4
  Rack1R1(config-line)#transport input telnet ssh

- При необходимости, запретить Telnet/SSH и др. протоколы для выхода с нашего устройства
  Rack1R1(config)#line vty 0 4
  Rack1R1(config-line)#transport output none

- Ограничить терминальный доступ к устройству определенными сетями и конкретными хостами с помощью ACL, например:
  Rack1R1(config)#access-list 10 permit 192.168.1.0 0.0.0.255
  Rack1R1(config)#access-list 10 permit host 172.16.1.1
  Rack1R1(config)#line vty 0 4
  Rack1R1(config-if)#access-class 10 in

LearnCisco.Ru

Дополнительные настройки и возможности:

- Прописать IP адреса на интерфейсах и активировать их
  Rack1R1(config)#interface fastEthernet 0/0
  Rack1R1(config-if)#ip address 192.168.1.1 255.255.255.0
  Rack1R1(config-if)#no shutdown

- Посмотреть ip адреса на интерфейсах и их состояние
  Rack1R1#show ip interface brief

- Задать маршруты, маршрут по умолчанию (default gateway)
  Rack1R1(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.254
  Rack1R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2

- Посмотреть таблицу маршрутов (show ip route)
  Rack1R1#show ip route

- Посмотреть секцию конфигурации статических маршрутов
  Rack1R1#show run | sec ip route

LearnCisco.Ru

Дополнительные настройки и возможности:

- Скрыть пароли в тексте конфигурации
  Rack1R1(config)#service password-encryption

- Включить возможность архивации файлов конфигурации, например:
  Rack1R1(config)#archive
  Rack1R1(config-archive)#path flash:/my-configs
  Rack1R1(config-archive)#maximum 10

- Архивация текущей конфигурации (running-config)
  Rack1R1#archive config

- Замена текущей конфигурации (running-config) из архивной копии, например:
  Rack1R1#configure replace flash:/my-configs-1

Важно! Команда copy flash:/my-configs-1 running-config объединяет обе, в отличие от configure replace flash:/my-configs-1, которая заменяет

LearnCisco.Ru

Дополнительные настройки и возможности:

- Создать теневые копии образа IOS и конфигурации на случай случайного удаления

```
Rack1R1(config)#secure boot-image
Rack1R1(config)#secure boot-config
```

- Посмотреть теневые копии

```
Rack1R1#show secure bootset
```

- Восстановление из теневой копии конфигурации

```
Rack1R1(config)#secure boot-config restore
```

- Создать баннер, например:

```
Rack1R1# banner #
Enter TEXT message.  End with the character '#'.
Authorized Access Only
#
```

LearnCisco.Ru

Полезности:

- Типы паролей в IOS
  - текстовый (clear text, тип 0)
  - шифрованный алгоритмом Cisco (тип 7)
  - хэш md5 (тип 5)

- Пароли типа 7 (например, line password, user password) можно легко взломать, даже без специальных утилит, а лишь с помощью самого устройства, например:

```
Rack1R1(config)#key chain PASS
Rack1R1(config-keychain)#key 1
Rack1R1(config-keychain-key)#key-string 7 045802150C2E

Rack1R1#show key chain PASS

    Key-chain PASS:
      key 1 -- text "cisco"
```

LearnCisco.Ru

Полезности:

- Для надежной защиты паролей необходимо включить сервис шифрации паролей и использовать тип 5 (ключевое слово secret) там где это возможно, например:

```
Rack1R1(config)#service password-encryption
Rack1R1(config)#enable secret cisco
Rack1R1(config)#username cisco privilege 15 secret cisco
```

- Для отключения возможности восстановления пароля и просмотра конфигурации, имея консольный доступ, можно отключить сервис:

```
Rack1R1(config)#no service password-recovery
```

- Посмотреть другие скрытые пароли и ключи (например, ключи isakmp) в тексте конфигурации

```
Rack1R1#more system:running-config
```

Полезности:

- Для лабораторных работ и тестирования можно вообще отключить проверку пароля и сразу входить в привилегированный режим (privilege level 15) при Telnet-е на устройство:

```
Rack1R1(config)# line vty 0 4
Rack1R1(config-line)#no login
Rack1R1(config-line)#privilege level 15
```

LearnCisco.Ru

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ

Подготовка маршрутизатора, коммутатора Cisco к работе