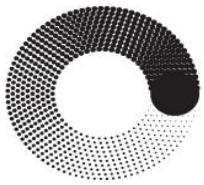
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



МОСКОВСКИЙ
ПОЛИТЕХ

Лабораторная работа №3

по дисциплине

«Основы сетевых технологий»

Группа 231-351

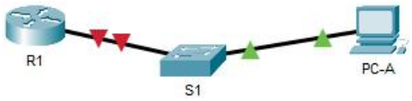
Студент Павлюченко М.С

Москва – 2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1011, y: 423 [Root] 01:59:30



Time: 00:03:54 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Copper Straight-Through

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

1 / 7

Cisco Networking Academy® Mind Wide Open™

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH

Часть 3. Настройка коммутатора для доступа по протоколу SSH

Часть 4. SSH через интерфейс командной строки (CLI) коммутатора

Общие сведения/сценарий

Раньше для удаленной настройки сетевых устройств в основном применялся протокол Telnet. Однако он не обеспечивает шифрование информации, передаваемой между клиентом и сервером, что позволяет анализаторам сетевых пакетов перехватывать пароли и данные конфигурации.

Secure Shell (SSH) — это сетевой протокол, устанавливающий безопасное подключение с эмуляцией терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удаленного компьютера. Протокол SSH все больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удаленного входа в систему. Чаще всего протокол SSH применяется для входа в удаленное устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH мог работать, на сетевых устройствах, взаимодействующих между собой, должна быть настроена поддержка SSH. В этой лабораторной работе необходимо включить SSH-сервер на маршрутизаторе, после чего подключиться к этому маршрутизатору, используя ПК с установленным клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP.

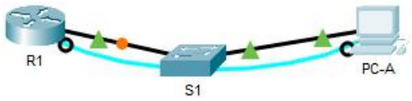
Поиск

15:52
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1180, y: 581 [Root] 03:07:00



PC-A

Physical Config Desktop Programming Attributes

Terminal

```
Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#serv
Router(config)#service pas
Router(config)#service password-encryption
Router(config)#banner motd "This is a secure system. Authorized Acccess Only!"
Router(config)#int g0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ex
Router(config)#hostname R1
R1(config)#do w
Building configuration...
[OK]
R1(config)#
```

Top

Time: 00:06:07 Realtime Simulation

Console

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

2 / 7

их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (Windows 7 или 8 с программой эмуляции терминала, например, Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
g. Зашифруйте открытые пароли.
h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Шаг 4: Настройте компьютер PC-A.

a. Настройте для PC-A IP-адрес и маску подсети.

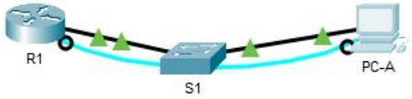
Поиск

15:54
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical | Physical x: 1221, y: 349 [Root] 03:34:30



PC-A

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

DHCP Static

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

Automatic Static

IPv6 Address /

Link Local Address FE80::20C:85FF:FE9A:C485

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication MD5

Username

Password

Top

Time: 00:07:01 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

3 / 7

b. Войдите в режим конфигурации.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
g. Зашифруйте открытые пароли.
h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Шаг 4: Настройте компьютер PC-A.

a. Настройте для PC-A IP-адрес и маску подсети.
b. Настройте для PC-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шифрует данные сеанса и обеспечивает аутентификацию устройств, поэтому для удаленных подключений рекомендуется использовать именно этот протокол. В части 2 вам нужно настроить маршрутизатор для приема соединений SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имя устройства.

```
Router(config)# hostname R1
```

b. Задайте домен для устройства.

```
R1(config)# ip domain-name ccna-lab.com
```

Шаг 2: Создайте ключ шифрования с указанием его длины.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
```

Поиск

15:55
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1234, y: 493 [Root] 03:46:00

R1 S1 PC-A

PC-A

Physical Config Desktop Programming Attributes

Command Prompt X

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Top

Time: 00:07:24 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

3 / 7

b. Войдите в режим конфигурации.
c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
g. Зашифруйте открытые пароли.
h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Шаг 4: Настройте компьютер PC-A.

a. Настройте для PC-A IP-адрес и маску подсети.
b. Настройте для PC-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Пошлите с PC-A команду Ping на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шифрует данные сеанса и обеспечивает аутентификацию устройств, поэтому для удаленных подключений рекомендуется использовать именно этот протокол. В части 2 вам нужно настроить маршрутизатор для приема соединений SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имя устройства.

```
Router(config)# hostname R1
```

b. Задайте домен для устройства.

```
R1(config)# ip domain-name ccna-lab.com
```

Шаг 2: Создайте ключ шифрования с указанием его длины.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
```

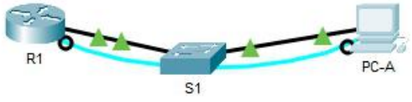
Поиск

15:55
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1181, y: 441 [Root] 04:42:00



PC-A

Physical Config Desktop Programming Attributes

Terminal

```
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ex
Router(config)#hostname R1
R1(config)#do w
Building configuration...
[OK]
R1(config)#
R1(config)#ip doma
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto key gene
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#username admin privilege 15 secret adminpass
*Mar 1 0:8:12.859: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#transport input all
R1(config-line)#login local
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line.  End with CNTL/2.
R1(config)#ip ssh ver 2
R1(config)#
```

Top

Time: 00:09:13 Realtime Simulation

Console

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

3 / 7

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передается в виде открытого текста. Протокол SSH шифрует данные сеанса и обеспечивает аутентификацию устройств, поэтому для удаленных подключений рекомендуется использовать именно этот протокол. В части 2 вам нужно настроить маршрутизатор для приема соединений SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

a. Задайте имя устройства.

```
Router(config)# hostname R1
```

b. Задайте домен для устройства.

```
R1(config)# ip domain-name ccna-lab.com
```

Шаг 2: Создайте ключ шифрования с указанием его длины.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Шаг 3: Создайте имя пользователя в локальной базе учетных записей.

```
R1(config)# username admin privilege 15 secret adminpass
```

Примечание. Уровень привилегий 15 дает пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```


b. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

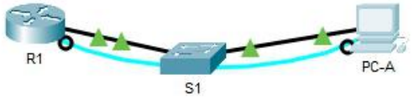
Поиск

15:57
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1167, y: 118 [Root] 05:21:00



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#
```

Top

Time: 00:10:29 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

4 / 7

```
R1#
```

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Шаг 6: Установите соединение с маршрутизатором по протоколу SSH.

a. Запустите Tera Term с PC-A.

b. Установите SSH-подключение к R1. Используйте имя пользователя **admin** и пароль **adminpass**. У вас должно получиться установить SSH-подключение к R1.

Часть 3: Настройка коммутатора для доступа по протоколу SSH

В части 3 вам предстоит настроить коммутатор в топологии для приема подключений по протоколу SSH, а затем установить SSH-подключение с помощью программы Tera Term.

Шаг 1: Настройте основные параметры коммутатора.

a. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.

g. Зашифруйте открытые пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблице адресации.

b. Задайте домен для устройства.

```
S1(config)# ip domain-name ccna-lab.com
```


c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

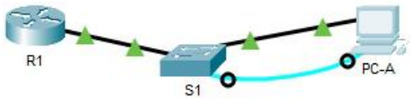
Поиск

15:58
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1145, y: 498 [Root] 06:57:00



PC-A

Physical Config Desktop Programming Attributes

Terminal X

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#enable secret class
Switch(config)#line con 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)#exit
Switch(config)#serv
Switch(config)#service pas
Switch(config)#service password-encryption
Switch(config)#banner motd "This is a secure system. Authorized Access Only!"
Switch(config)#int vlan1
Switch(config-if)#192.168.1.11 255.255.255.0
                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip add 192.168.1.11 255.255.255.0
Switch(config-if)#no shut

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#ip defa
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#do w
Building configuration...
[OK]
Switch(config)#
```

Top

Time: 00:13:38 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

4 / 7

```
[OK]
R1#
```

Шаг 6: Установите соединение с маршрутизатором по протоколу SSH.

a. Запустите Tera Term с PC-A.

b. Установите SSH-подключение к R1. Используйте имя пользователя **admin** и пароль **adminpass**. У вас должно получиться установить SSH-подключение к R1.

Часть 3: Настройка коммутатора для доступа по протоколу SSH

В части 3 вам предстоит настроить коммутатор в топологии для приема подключений по протоколу SSH, а затем установить SSH-подключение с помощью программы Tera Term.

Шаг 1: Настройте основные параметры коммутатора.

a. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.

f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.

g. Зашифруйте открытые пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблице адресации.

b. Задайте домен для устройства.

```
S1(config)# ip domain-name ccna-lab.com
```


c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Создайте имя пользователя в локальной базе учетных записей.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Активируйте протоколы Telnet и SSH на линиях VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

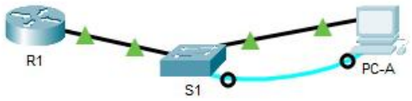
Поиск

16:01
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1002, y: 685 [Root] 07:42:00



PC-A

Physical Config Desktop Programming Attributes

Terminal

```
Switch(config-if)#ip add 192.168.1.11 255.255.255.0
Switch(config-if)#no shut

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#ip defa
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#do w
Building configuration...
[OK]
Switch(config)#
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#username admin privilege 15 secret adminpass
*Mar 1 0:14:1.166: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 15
S1(config-line)#transport input all
S1(config-line)#login local
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Top

Time: 00:15:05 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

5 / 7

e. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю.
f. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю.
g. Зашифруйте открытые пароли.
h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
i. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблице адресации.
b. Задайте домен для устройства.

```
S1(config)# ip domain-name ccna-lab.com
```


c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Создайте имя пользователя в локальной базе учетных записей.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Активируйте протоколы Telnet и SSH на линиях VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
S1(config-line)# login local
S1(config-line)# end
```

Шаг 3: Установите соединение с коммутатором по протоколу SSH.

Запустите программу Tera Term на PC-A, затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

Часть 4: Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг 1: Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Используйте вопросительный знак (?), чтобы отобразить варианты параметров для команды **ssh**.

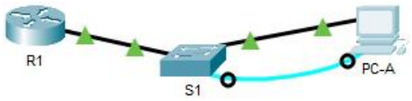
Поиск

16:03
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 399, y: 153 [Root] 08:57:30



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#ssh -l admin 192.168.1.3

% Connection refused by remote host
R1#ssh -l admin 192.168.1.11

Password:
% Login invalid


Password:

This is a secure system. Authorized Access Only!

S1#
```

Top

Time: 00:17:34 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

5 / 7

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 2: Настройте коммутатор для соединения по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

a. Настройте имя устройства, как указано в таблице адресации.

b. Задайте домен для устройства.

```
S1(config)# ip domain-name ccna-lab.com
```


c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Создайте имя пользователя в локальной базе учетных записей.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Активируйте протоколы Telnet и SSH на линиях VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
S1(config-line)# login local
S1(config-line)# end
```

Шаг 3: Установите соединение с коммутатором по протоколу SSH.

Запустите программу Tera Term на PC-A, затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

Часть 4: Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг 1: Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Используйте вопросительный знак (?), чтобы отобразить варианты параметров для команды **ssh**.

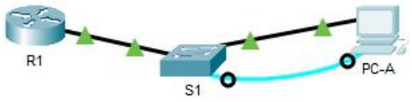
```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
```

Поиск 16:05 09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1230, y: 279 [Root] 09:16:30



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#ssh -l admin 192.168.1.3

% Connection refused by remote host
R1#ssh -l admin 192.168.1.11

Password:
% Login invalid


Password:

This is a secure system. Authorized Access Only!

S1#ssh ?
  -l  Log in using this user name
  -v  Specify SSH Protocol Version
S1#ssh
```

Top

Time: 00:18:11 Realtime Simulation

Console

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

5 / 7

c. Создайте ключ шифрования с указанием его длины.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Создайте имя пользователя в локальной базе учетных записей.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Активируйте протоколы Telnet и SSH на линиях VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

f. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.

```
S1(config-line)# login local
S1(config-line)# end
```

Шаг 3: Установите соединение с коммутатором по протоколу SSH.

Запустите программу Tera Term на PC-A, затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Удалось ли вам установить SSH-соединение с коммутатором?

да

Часть 4: Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Клиент SSH встроен в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 4 вам предстоит установить соединение с маршрутизатором по протоколу SSH, используя интерфейс командной строки коммутатора.

Шаг 1: Посмотрите доступные параметры для клиента SSH в Cisco IOS.

Используйте вопросительный знак (?), чтобы отобразить варианты параметров для команды **ssh**.

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Шаг 2: Установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–l admin**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля **adminpass**

```
S1# ssh -l admin 192.168.1.1
Password:
```

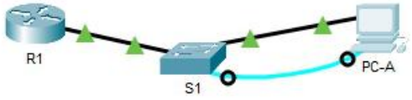

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Поиск 16:06 09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1216, y: 517 [Root] 09:36:30



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#ssh -l admin 192.168.1.3

% Connection refused by remote host
R1#ssh -l admin 192.168.1.11

Password:
% Login invalid


Password:

This is a secure system. Authorized Access Only!

S1#ssh ?
  -l  Log in using this user name
  -v  Specify SSH Protocol Version
S1#ssh -l admin 192.168.1.1

Password:

This is a secure system. Authorized Acccess Only!

R1#
```

Top

Time: 00:18:49 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

6 / 7

```
  -b    Specify Options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Шаг 2: Установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду **–l admin**. Это позволит вам войти в систему под именем **admin**. При появлении приглашения введите в качестве пароля **adminpass**

```
S1# ssh -l admin 192.168.1.1
Password:
```


Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

```
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************

R1#
```

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1, нажмите комбинацию клавиш **Ctrl+Shift+6**. Отпустите клавиши **Ctrl+Shift+6** и нажмите **x**. Отображается приглашение привилегированного режима EXEC коммутатора.

```
R1#
S1#
```

c. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду **exit**.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

Вопросы для повторения

Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

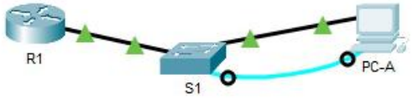
Поиск

16:07
09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1143, y: 447 [Root] 09:49:30



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#ssh -l admin 192.168.1.3

% Connection refused by remote host
R1#ssh -l admin 192.168.1.11

Password:
% Login invalid


Password:

This is a secure system. Authorized Access Only!

S1#ssh ?
  -l  Log in using this user name
  -v  Specify SSH Protocol Version
S1#ssh -l admin 192.168.1.1

Password:

This is a secure system. Authorized Acccess Only!

R1#exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Top

Time: 00:19:14 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

6 / 7

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

```
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************

R1#
```

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1, нажмите комбинацию клавиш **Ctrl+Shift+6**. Отпустите клавиши **Ctrl+Shift+6** и нажмите **x**. Отображается приглашение привилегированного режима EXEC коммутатора.

```
R1#
S1#
```

c. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду **exit**.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

Вопросы для повторения

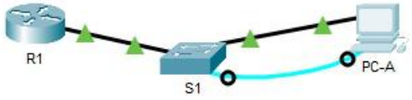
Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

Поиск 16:07 09.10.2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1218, y: 298 [Root] 10:31:00



PC-A

Physical Config Desktop Programming Attributes

Command Prompt X

```
C:\>ssh -l admin 192.168.1.1

Password:
% Login invalid


Password:

This is a secure system. Authorized Acccess Only!

R1#ssh -l admin 192.168.1.3

% Connection refused by remote host
R1#ssh -l admin 192.168.1.11

Password:
% Login invalid


Password:

This is a secure system. Authorized Access Only!

S1#ssh ?
  -l  Log in using this user name
  -v  Specify SSH Protocol Version
S1#ssh -l admin 192.168.1.1

Password:

This is a secure system. Authorized Acccess Only!

R1#^Z
R1#exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Top

Time: 00:20:36 Realtime Simulation

Scenario 0 New Delete Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec)

Console

netacad.sadlab.su/le

Расписание 231-351 ОСТ Личный кабинет CTF tutorials CTF map

6 / 7

```
R1#
```

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1, нажмите комбинацию клавиш **Ctrl+Shift+6**. Отпустите клавиши **Ctrl+Shift+6** и нажмите **x**. Отображается приглашение привилегированного режима EXEC коммутатора.

```
R1#
S1#
```

c. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду **exit**.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Какие версии протокола SSH поддерживаются при использовании интерфейса командной строки?

ip ssh version 1
ip ssh version 2

Вопросы для повторения

Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

Создать в локальной базе учетных записей несколько пользователей, каждой учетной записи присвоить пароль (и при необходимости - уровень доступных привилегий)

Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

Сводная таблица по интерфейсам маршрутизаторов

Поиск

16:09
09.10.2024