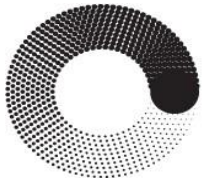
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

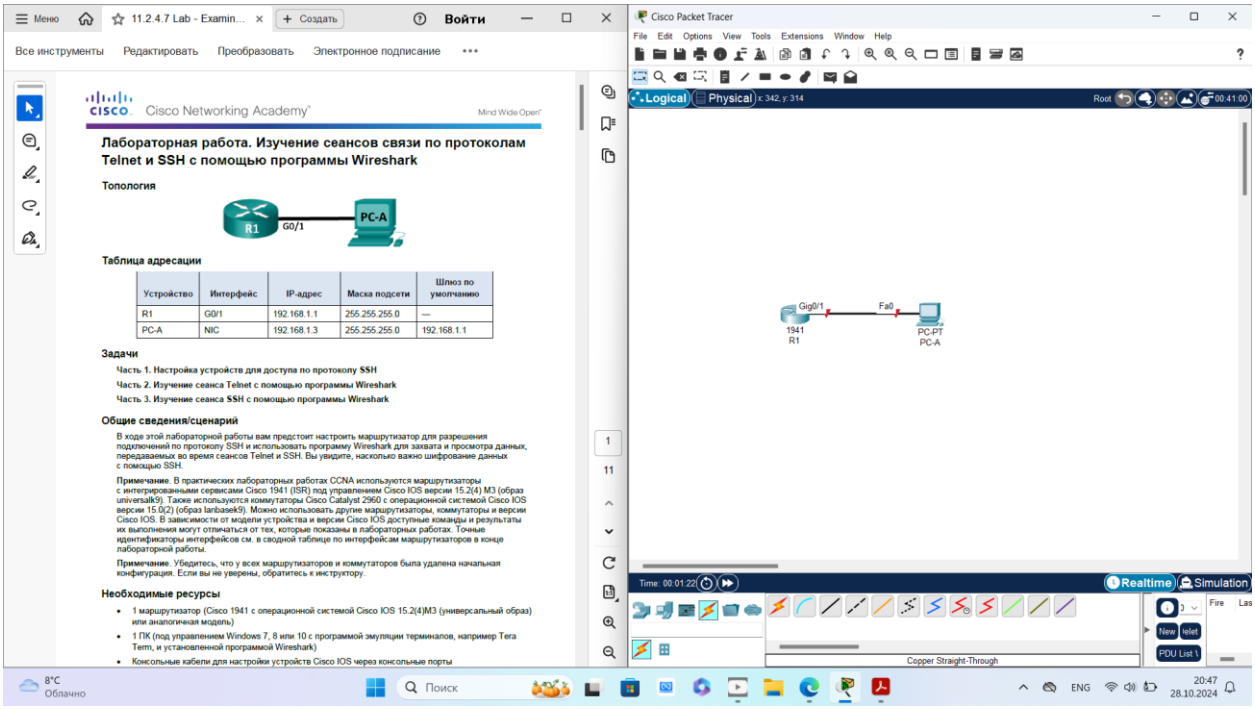


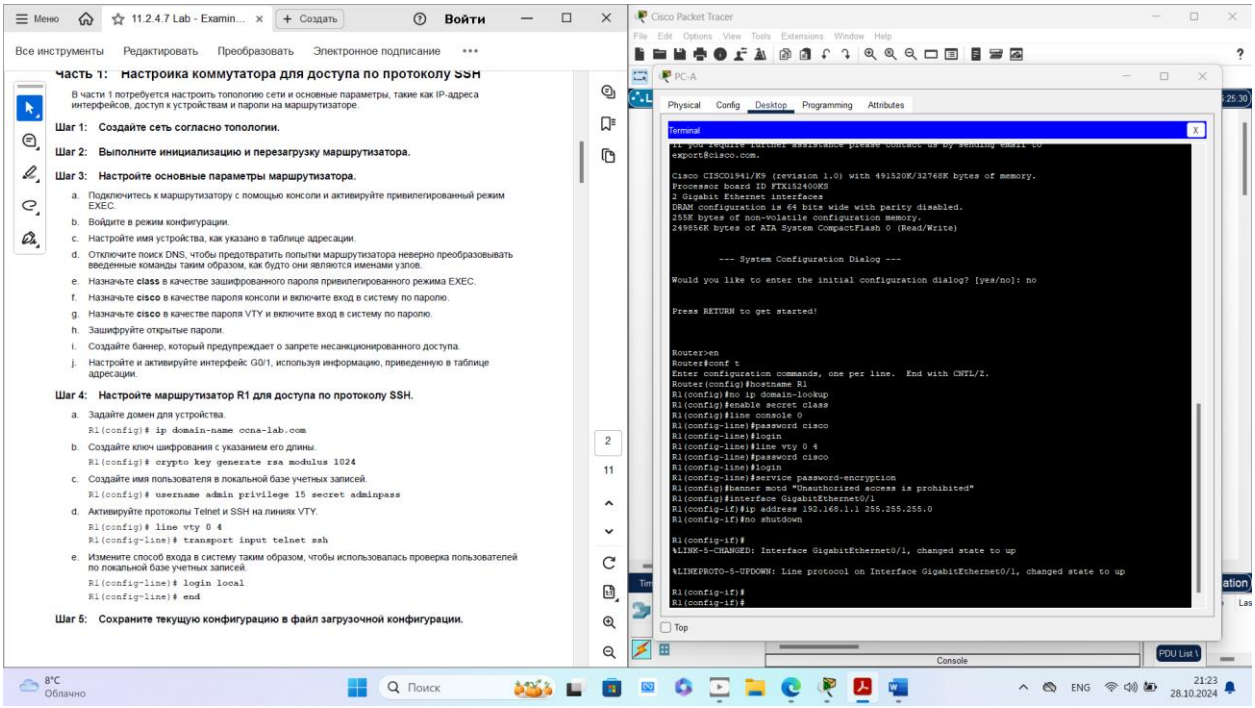
московский политех

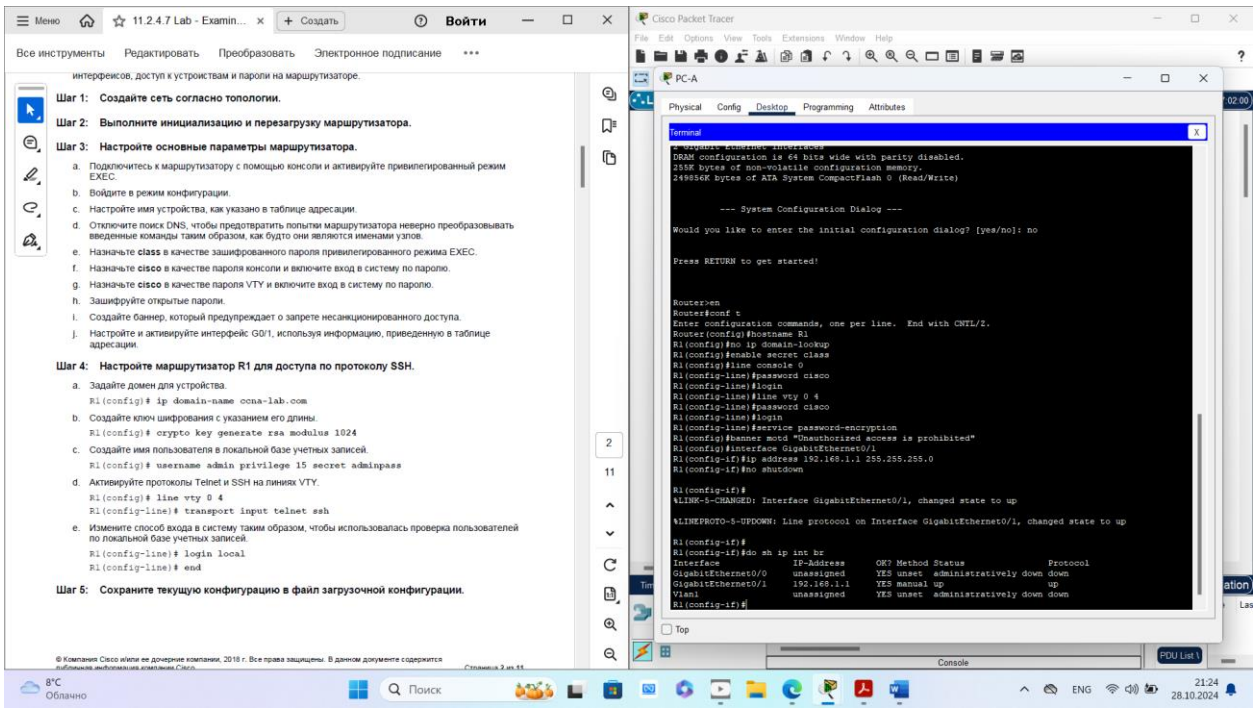
ЛАБОРАТОРНАЯ РАБОТА №4

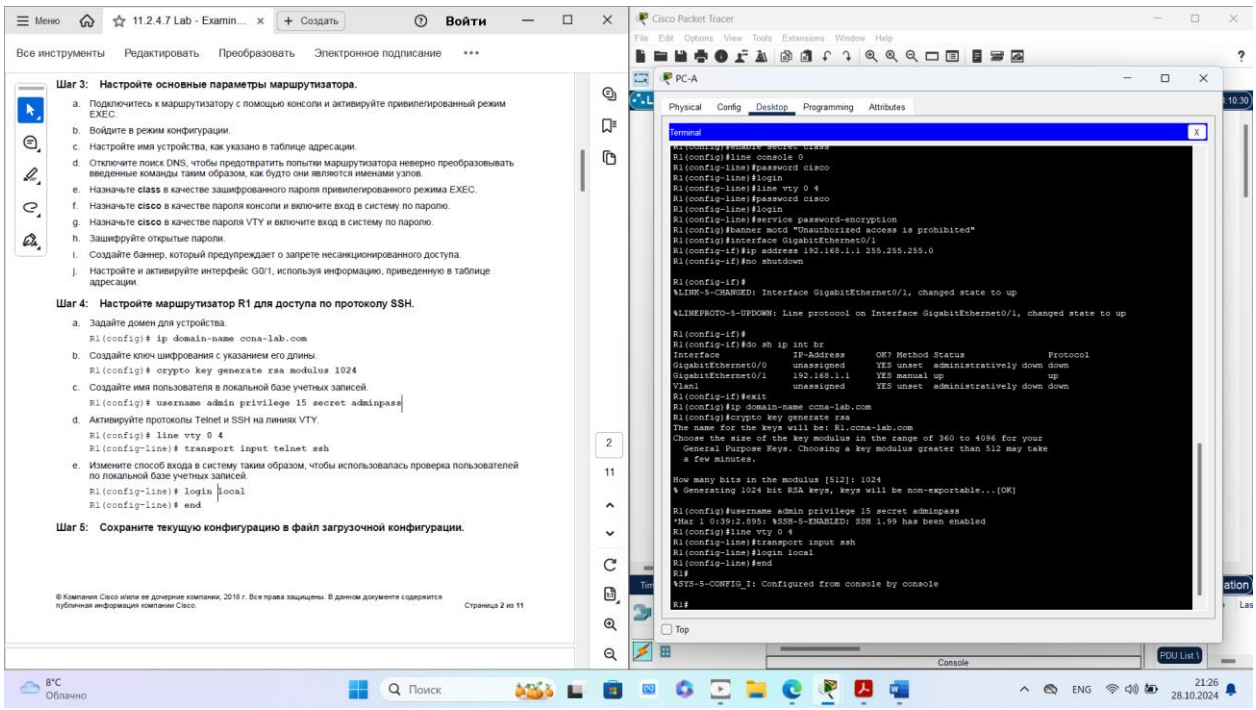
Группа 231-351
Студент Пономарева А.Е

Москва – 2024


Меню
11.2.4.7 Lab - Examin...
Создать
Войти
Все инструменты
Редактировать
Преобразовать
Электронное подписание
Cisco Networking Academy
Mind Wide Open
Лабораторная работа. Изучение сеансов связи по протоколам Telnet и SSH с помощью программы Wireshark
Топология
R1
G0/1
PC-A
Таблица адресации
Устройство
Интерфейс
IP-адрес
Маска подсети
Шлюз по умолчанию
R1
G0/1
192.168.1.1
255.255.255.0
—
PC-A
NIC
192.168.1.3
255.255.255.0
192.168.1.1
Задачи
Часть 1. Настройка устройств для доступа по протоколу SSH
Часть 2. Изучение сеанса Telnet с помощью программы Wireshark
Часть 3. Изучение сеанса SSH с помощью программы Wireshark
Общие сведения/сценарий
В ходе этой лабораторной работы вам предстоит настроить маршрутизатор для разрешения подключений по протоколу SSH и использовать программу Wireshark для захвата и просмотра данных, передаваемых во время сеансов Telnet и SSH. Вы увидите, насколько важно шифрование данных с помощью SSH.
Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты 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 ПК (под управлением Windows 7, 8 или 10 с программой эмуляции терминалов, например Tera Term, и установленной программой Wireshark)
Консольные кабели для настройки устройств Cisco IOS через консольные порты
Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
Gig0/1
Fa0
1941
R1
PC-PT
PC-A
Time: 00:01:22
Realtime
Simulation
Copper Straight-Through
8°C
Облачно
Поиск
ENG
20:47
28.10.2024


Меню
11.2.4.7 Lab - Examin...
Создать
Войти
Все инструменты
Редактировать
Преобразовать
Электронное подписание
Часть 1: Настроика коммутатора для доступа по протоколу SSH
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.
Шаг 3: Настройте основные параметры маршрутизатора.
a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Настройте имя устройства, как указано в таблице адресации.
d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
e. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
f. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
g. Назначьте cisco в качестве пароля VTY и включите вход в систему по паролю.
h. Зашифруйте открытые пароли.
i. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
j. Настройте и активируйте интерфейс G0/1, используя информацию, приведенную в таблице адресации.
Шаг 4: Настройте маршрутизатор R1 для доступа по протоколу SSH.
a. Задайте домен для устройства.
R1(config)# ip domain-name ccna-lab.com
b. Создайте ключ шифрования с указанием его длины.
R1(config)# crypto key generate rsa modulus 1024
c. Создайте имя пользователя в локальной базе учетных записей.
R1(config)# username admin privilege 15 secret adminpass
d. Активируйте протоколы Telnet и SSH на линиях VTY.
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
e. 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
Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.
Cisco Packet Tracer
PC-A
Physical
Config
Desktop
Programming
Attributes
Terminal
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400K5
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd "Unauthorized access is prohibited"
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(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
R1(config-if)#
R1(config-if)#
Top
Console
8°C
Облачно
Поиск
ENG
21:23
28.10.2024


Меню
11.2.4.7 Lab - Examin...
Создать
Войти
Все инструменты
Редактировать
Преобразовать
Электронное подписание
интерфейсов, доступ к устройствам и пароли на маршрутизаторе.
Шаг 1: Создайте сеть согласно топологии.
Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора.
Шаг 3: Настройте основные параметры маршрутизатора.
a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Настройте имя устройства, как указано в таблице адресации.
d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
e. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
f. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
g. Назначьте cisco в качестве пароля VTY и включите вход в систему по паролю.
h. Зашифруйте открытые пароли.
i. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
j. Настройте и активируйте интерфейс G0/1, используя информацию, приведенную в таблице адресации.
Шаг 4: Настройте маршрутизатор R1 для доступа по протоколу SSH.
a. Задайте домен для устройства.
R1(config)# ip domain-name ccna-lab.com
b. Создайте ключ шифрования с указанием его длины.
R1(config)# crypto key generate rsa modulus 1024
c. Создайте имя пользователя в локальной базе учетных записей.
R1(config)# username admin privilege 15 secret adminpass
d. Активируйте протоколы Telnet и SSH на линиях VTY.
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
e. 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
Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.
© Компания Cisco и/или ее дочерние компании, 2018 г. Все права защищены. В данном документе содержится публичная информация компании Cisco.
Страница 3 из 11
Cisco Packet Tracer
PC-A
Physical
Config
Desktop
Programming
Attributes
Terminal
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/2.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd "Unauthorized access is prohibited"
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(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
R1(config-if)#
R1(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
R1(config-if)#
Top
Console
PDU List
8°C
Облачно
Поиск
ENG
21:24
28.10.2024


Меню
11.2.4.7 Lab - Examin...
Создать
Войти
Все инструменты
Редактировать
Преобразовать
Электронное подписание
Шаг 3: Настройте основные параметры маршрутизатора.
a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
b. Войдите в режим конфигурации.
c. Настройте имя устройства, как указано в таблице адресации.
d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
e. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
f. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
g. Назначьте cisco в качестве пароля VTY и включите вход в систему по паролю.
h. Зашифруйте открытые пароли.
i. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
j. Настройте и активируйте интерфейс G0/1, используя информацию, приведенную в таблице адресации.
Шаг 4: Настройте маршрутизатор R1 для доступа по протоколу SSH.
a. Задайте домен для устройства.
R1(config)# ip domain-name ccna-lab.com
b. Создайте ключ шифрования с указанием его длины.
R1(config)# crypto key generate rsa modulus 1024
c. Создайте имя пользователя в локальной базе учетных записей.
R1(config)# username admin privilege 15 secret adminpass
d. Активируйте протоколы Telnet и SSH на линиях VTY.
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
e. 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
Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.
© Компания Cisco и/или ее дочерние компании, 2018 г. Все права защищены. В данном документе содержится публичная информация компании Cisco.
Страница 2 из 11
Cisco Packet Tracer
PC-A
Physical
Config
Desktop
Programming
Attributes
Terminal
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd "Unauthorized access is prohibited"
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(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
R1(config-if)#
R1(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
R1(config-if)#exit
R1(config)#ip domain-name ccna-lab.com
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 4096 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 0:39:2.895: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
Top
Console
PDU List
8°C
Облачно
Поиск
ENG
21:26
28.10.2024

Меню | 11.2.4.7 Lab - Examin... | Создать | Войти

Все инструменты | Редактировать | Преобразовать | Электронное подписание | •••

Лабораторная работа. Изучение сеансов связи по протоколам Telnet и SSH с помощью программы Wireshark

Шаг 6: Настройте компьютер PC-A.

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

b. Настройте для PC-A шлюз по умолчанию.

Шаг 7: 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: Изучение сеанса Telnet с помощью программы Wireshark

В части 2 вам нужно воспользоваться программой Wireshark для захвата и просмотра данных, передаваемых во время сеанса связи с маршрутизатором по протоколу Telnet. С помощью программы Tera Term вы должны подключиться к маршрутизатору R1 по протоколу Telnet, войти в систему и ввести на маршрутизаторе команду **show run**.

Примечание. Если на компьютере не установлено программное обеспечение клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTY (www.putty.org).

Примечание. По умолчанию доступ к Telnet из командной строки в Windows 7 отключен. Чтобы активировать подключение по протоколу Telnet из окна командной строки, выберите **Пуск** > **Панель управления** > **Программы** > **Программы и компоненты** > **Включение или отключение компонентов Windows.** Установите флажок **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Выполните захват данных.

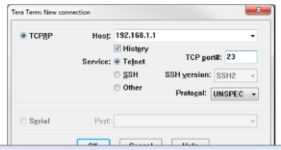
a. Запустите программу Wireshark.

b. Запустите захват данных на интерфейсе локальной сети.

Примечание. Если захват данных на интерфейсе локальной сети запустить не удается, попробуйте открыть программу Wireshark с использованием опции **Запуск от имени администратора**.

Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле Host введите **192.168.1.1**.



Cisco Packet Tracer

PC-A

Physical | Config | Desktop | Programming | Attributes

IP Configuration

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::203:E4FF:FEEE:E1EC

Default Gateway:

DNS Server:

802.1X

Use 802.1X Security

Authentication: MD5

Username:

Password:

Top

Console

PDU List

8°C Облачно | Поиск | ENG | 21:27 28.10.2024

Меню | 11.2.4.7 Lab - Examin... | Создать | Войти

Все инструменты | Редактировать | Преобразовать | Электронное подписание | •••

Шаг 6: Настройте компьютер PC-A.

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

b. Настройте для PC-A шлюз по умолчанию.

Шаг 7: 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: Изучение сеанса Telnet с помощью программы Wireshark

В части 2 вам нужно воспользоваться программой Wireshark для захвата и просмотра данных, передаваемых во время сеанса связи с маршрутизатором по протоколу Telnet. С помощью программы Tera Term вы должны подключиться к маршрутизатору R1 по протоколу Telnet, войти в систему и ввести на маршрутизаторе команду **show run**.

Примечание. Если на компьютере не установлено программное обеспечение клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTY (www.putty.org).

Примечание. По умолчанию доступ к Telnet из командной строки в Windows 7 отключен. Чтобы активировать подключение по протоколу Telnet из окна командной строки, выберите **Пуск** > **Панель управления** > **Программы** > **Программы и компоненты** > **Включение или отключение компонентов Windows.** Установите флажок **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Выполните захват данных.

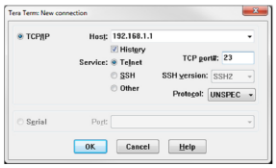
a. Запустите программу Wireshark.

b. Запустите захват данных на интерфейсе локальной сети.

Примечание. Если захват данных на интерфейсе локальной сети запустить не удается, попробуйте открыть программу Wireshark с использованием опции **Запуск от имени администратора**.

Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле Host введите **192.168.1.1**.



Cisco Packet Tracer

PC-A

Physical | Config | Desktop | Programming | Attributes

Command Prompt

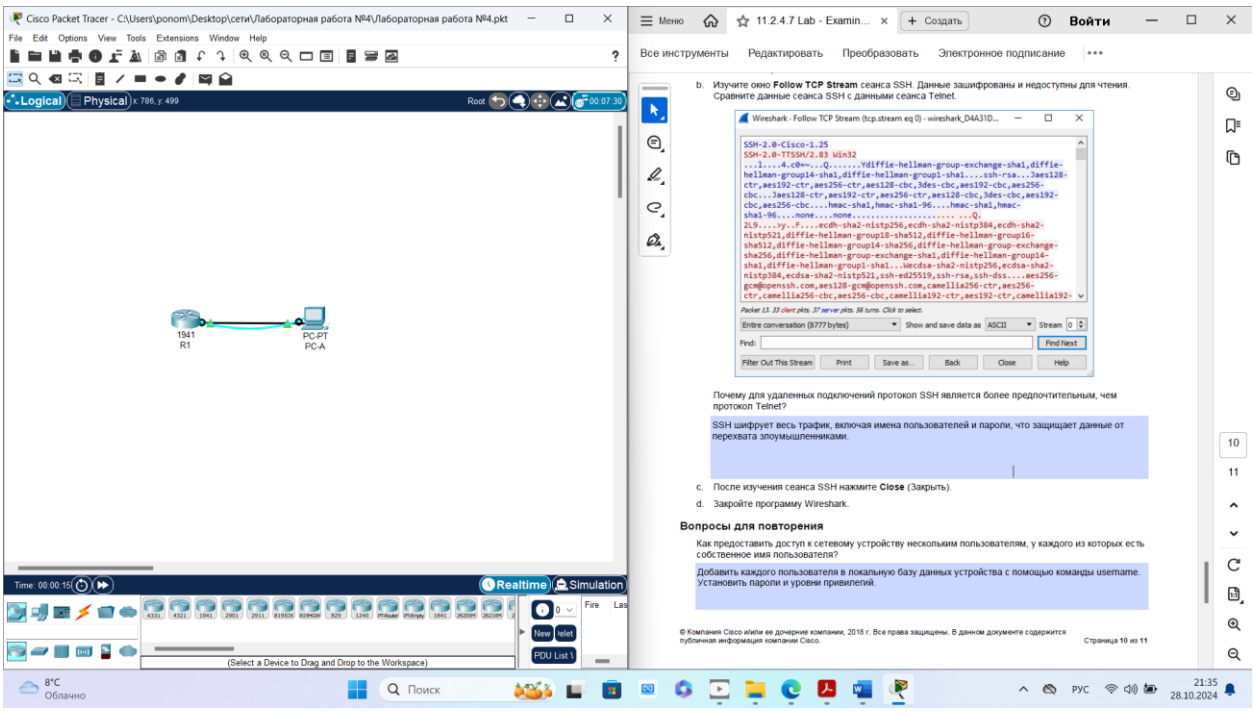
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

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<1ms 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 = 0ms, Average = 0ms

C:\>
```

Top

Console

PDU List

8°C Облачно | Поиск | ENG | 21:29 28.10.2024


Cisco Packet Tracer - C:\Users\ponom\Desktop\сети\Лабораторная работа №4\Лабораторная работа №4.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 786, y: 499
Root 00:07:30
1941
R1
PC-PT
PC-A
Time: 00:00:15
Realtime Simulation
(Select a Device to Drag and Drop to the Workspace)
Меню
11.2.4.7 Lab - Examin...
Создать
Войти
Все инструменты Редактировать Преобразовать Электронное подписание
b. Изучите окно Follow TCP Stream сеанса SSH. Данные зашифрованы и недоступны для чтения. Сравните данные сеанса SSH с данными сеанса Telnet.
Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_D4A31D...
SSH-2.0-Cisco-1.25
SSH-2.0-TTSSH/2.83 Win32
Entire conversation (8777 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Почему для удаленных подключений протокол SSH является более предпочтительным, чем протокол Telnet?
SSH шифрует весь трафик, включая имена пользователей и пароли, что защищает данные от перехвата злоумышленниками.
c. После изучения сеанса SSH нажмите Close (Закрыть).
d. Закройте программу Wireshark.
Вопросы для повторения
Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?
Добавить каждого пользователя в локальную базу данных устройства с помощью команды username. Установить пароли и уровни привилегий.
© Компания Cisco и/или ее дочерние компании, 2018 г. Все права защищены. В данном документе содержится публичная информация компании Cisco.
Страница 10 из 11
10
11
8°C
Облачно
Поиск
РУС
21:35
28.10.2024