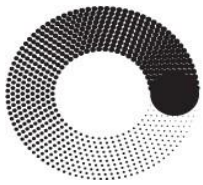
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



московский политех

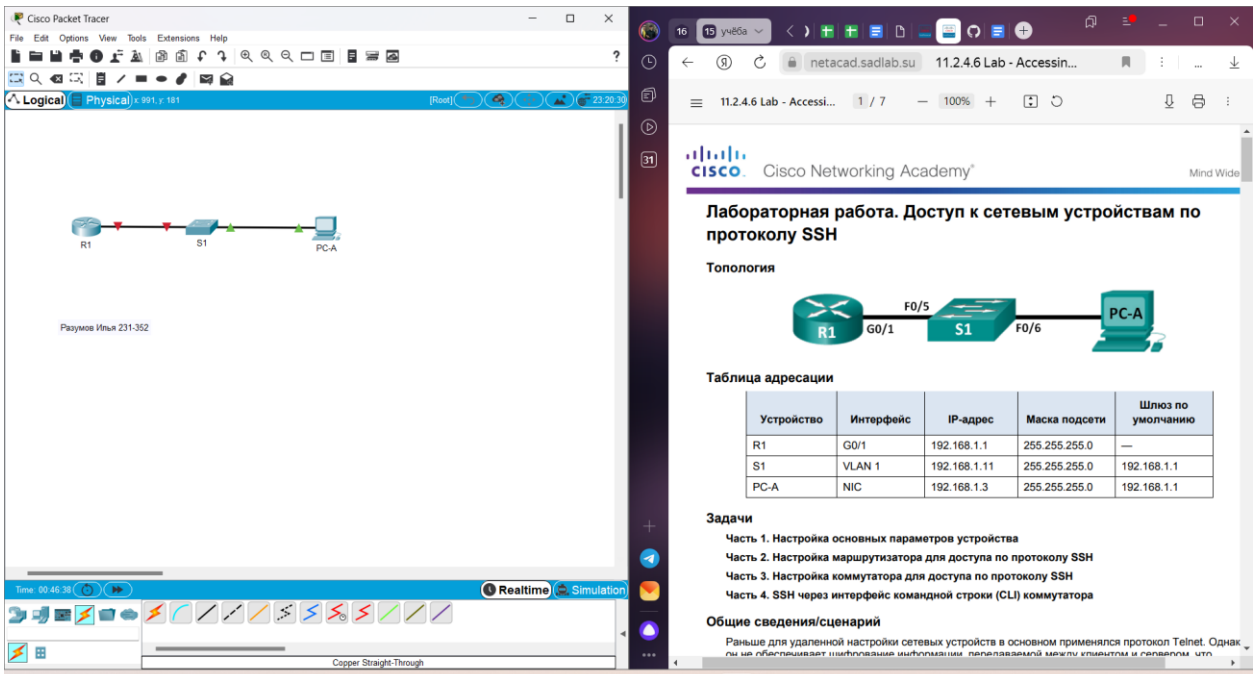
ЛАБОРАТОРНАЯ РАБОТА №3

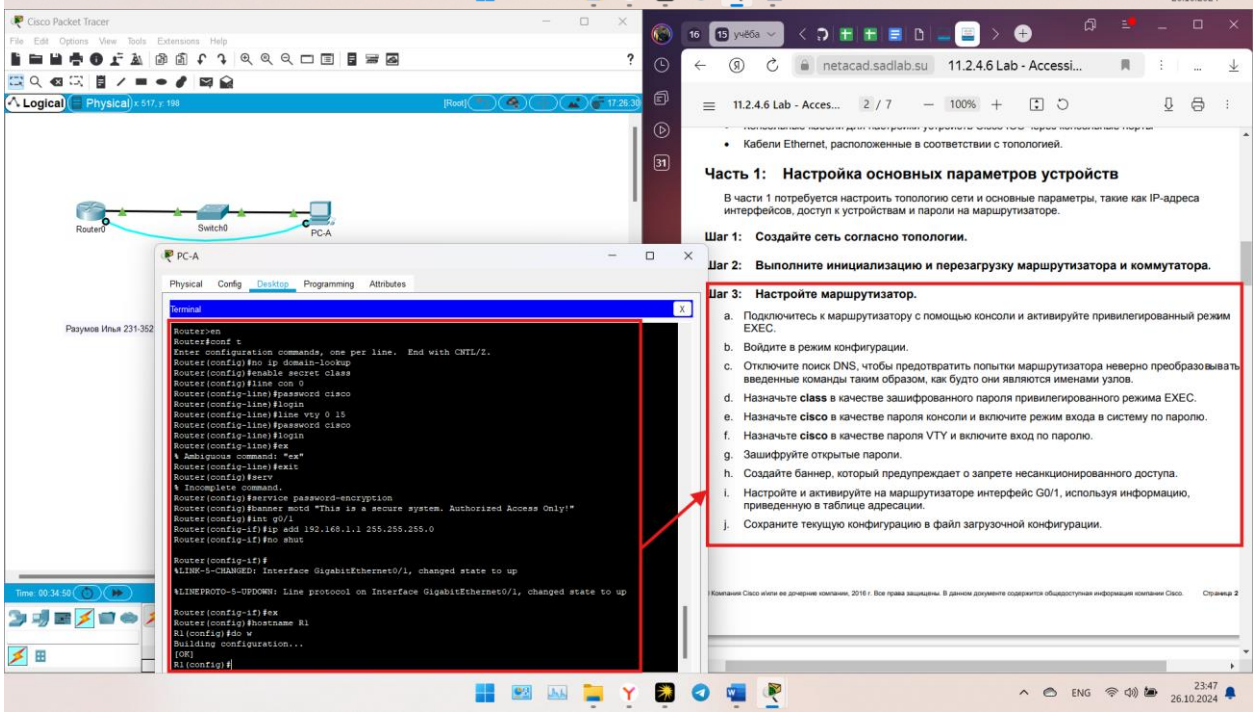
«Настройка основных параметров коммутации»

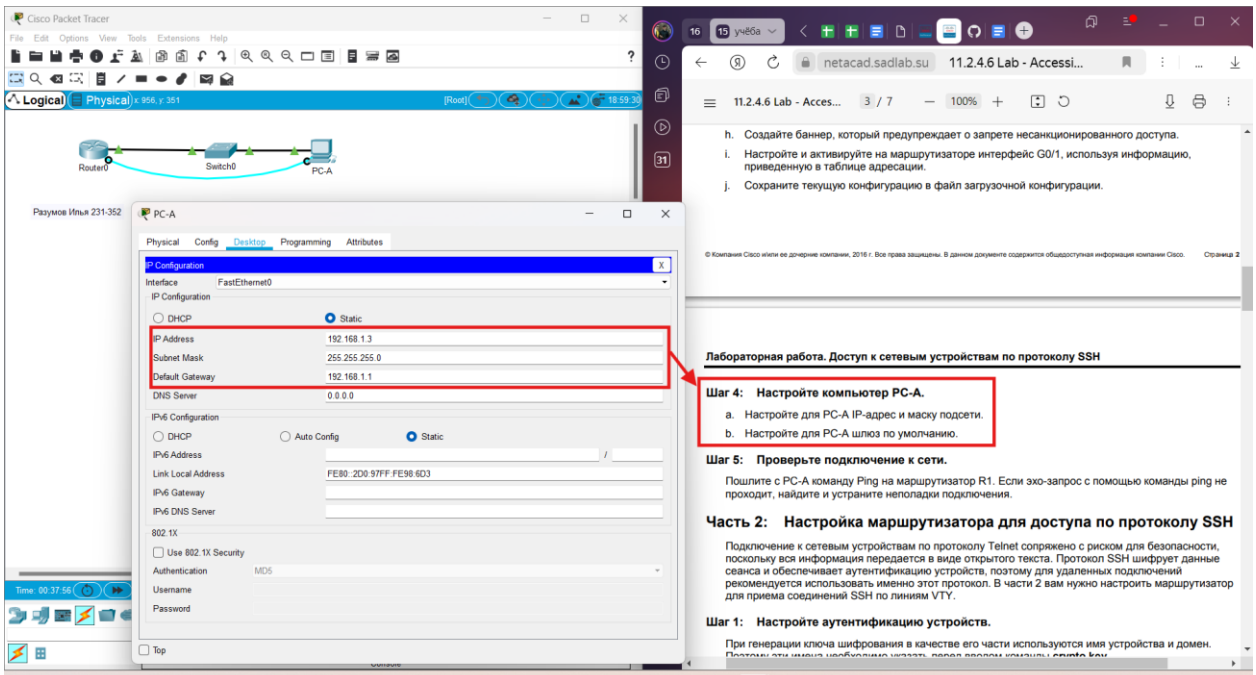
по дисциплине
«Сети и системы передачи информации»

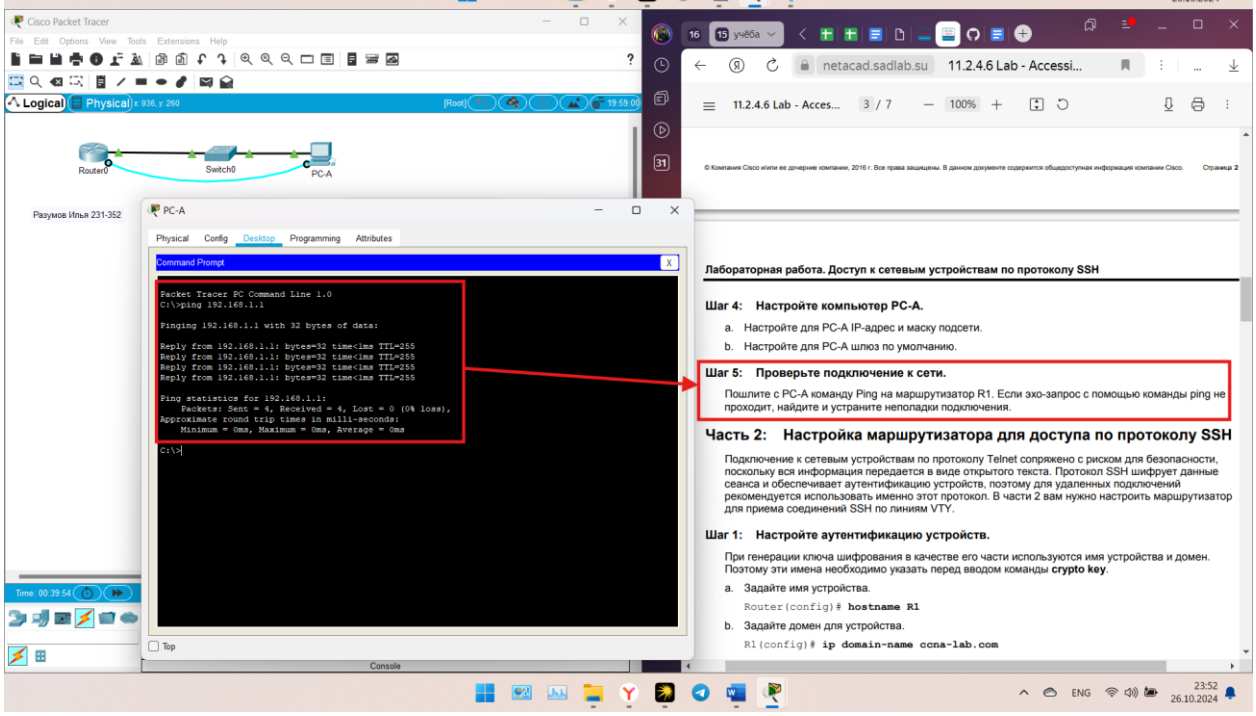
Группа 231-352
Студент Разумов И. М.
Преподаватель Дорофеев О.В.

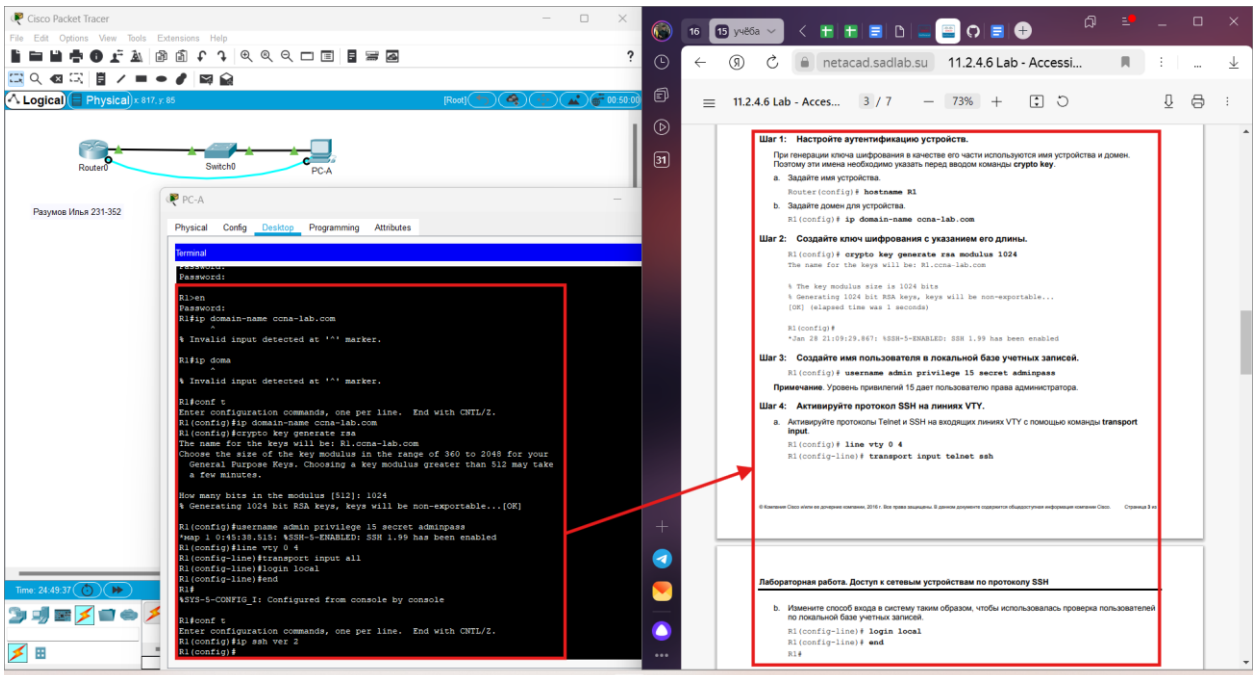
Москва 2024

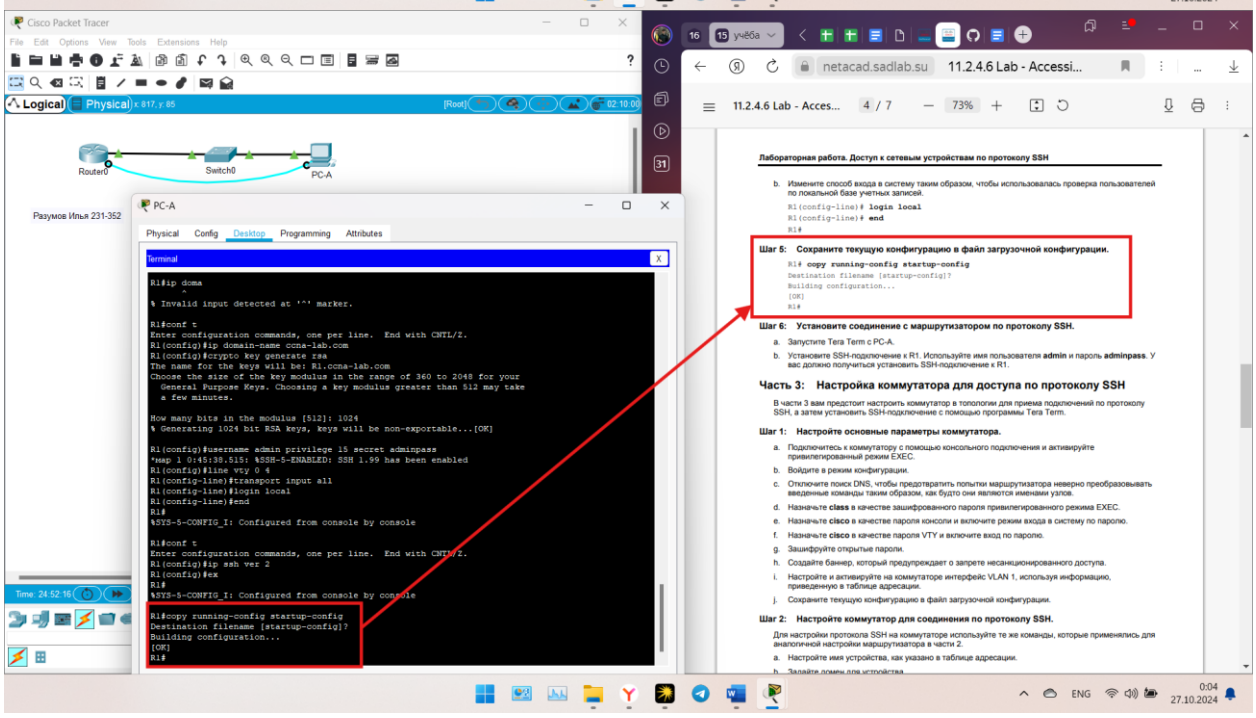

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical Physical
R1
S1
PC-A
Разумов Илья 231-352
Realtime Simulation
Copper Straight-Through
netacad.sadlab.su
11.2.4.6 Lab - Accessin...
Cisco Networking Academy
Mind Wide
Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH
Топология
F0/5
G0/1
F0/6
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. Однак
22:57
26.10.2024

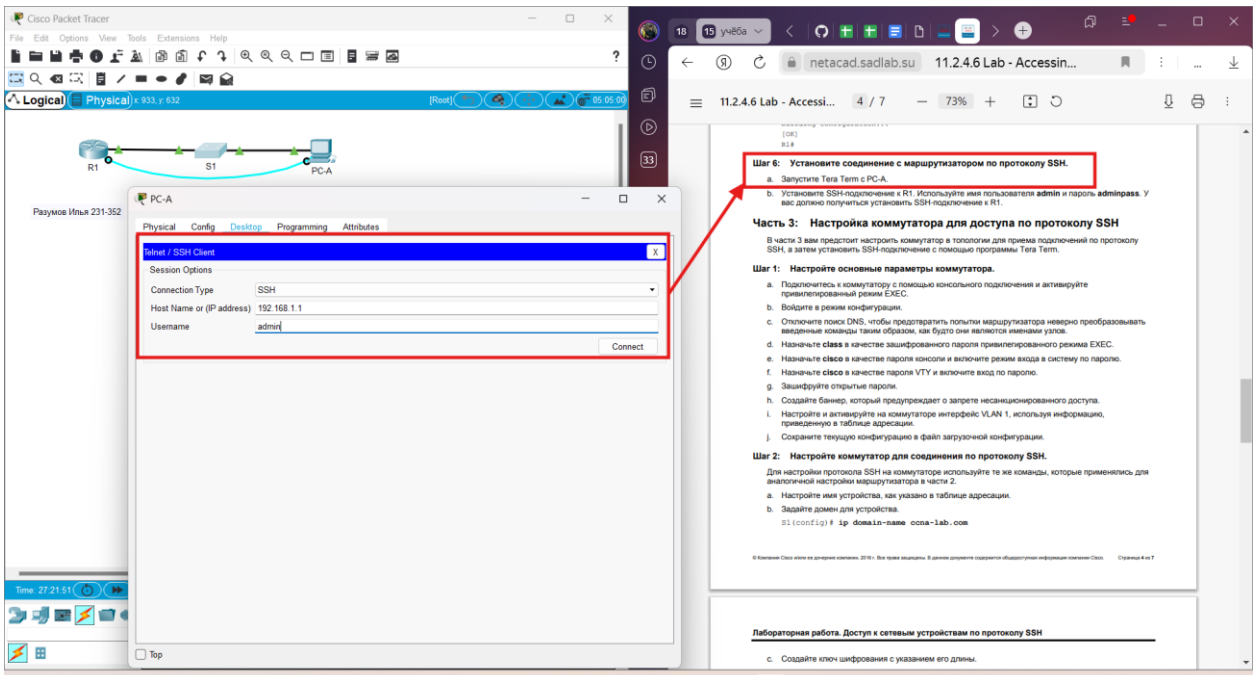

Cisco Packet Tracer
Logical Physical
Router0
Switch0
PC-A
Разумов Илья 231-352
PC-A
Physical Config Desktop Programming Attributes
Terminal
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#line 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)#ex
% Ambiguous command: "ex"
Router(config-line)#exit
Router(config)#serv
% Incomplete command.
Router(config)#service password-encryption
Router(config)#banner motd "This is a secure system. Authorized Access Only!"
Router(config)#int g0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
%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)#
netacad.sadlab.su
11.2.4.6 Lab - Accessi...
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.
Страница 2
23:47
26.10.2024

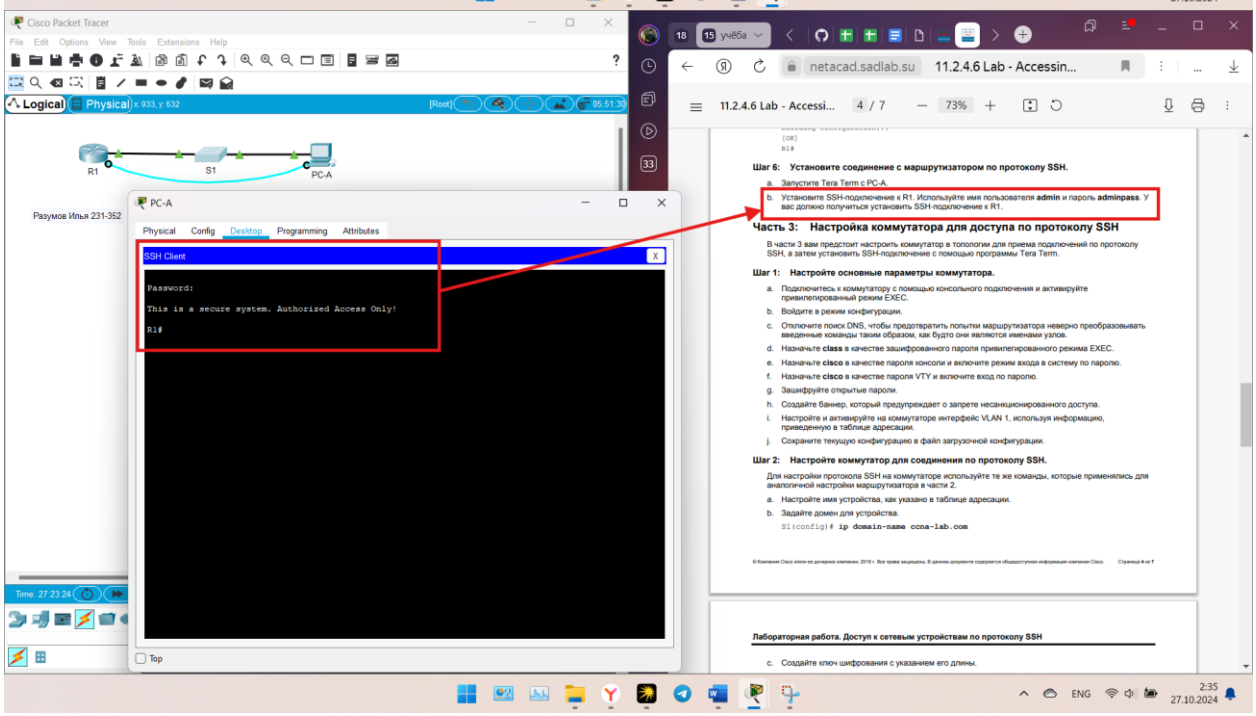

Cisco Packet Tracer
Logical
Physical
Router0
Switch0
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
IPv6 Address
Link Local Address
FE80::2D0:97FF:FE98:6D3
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
Username
Password
Top
netacad.sadlab.su
11.2.4.6 Lab - Accessi...
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.

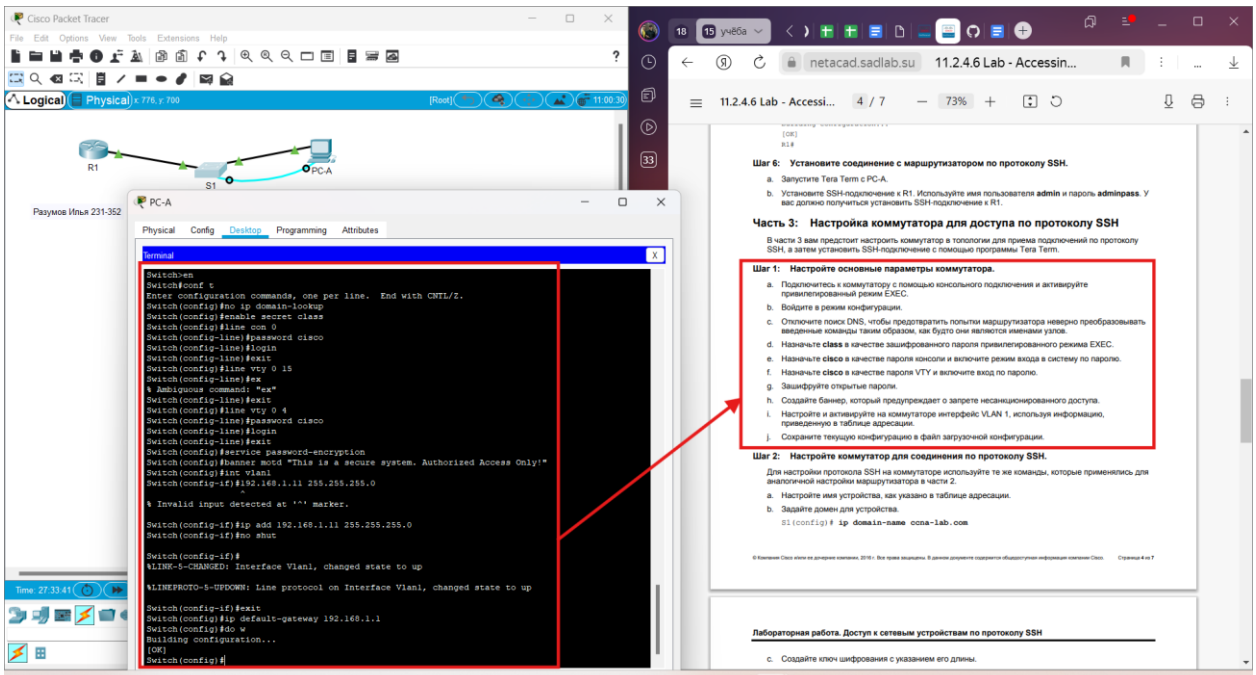

Cisco Packet Tracer
Logical
Physical
Router0
Switch0
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 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<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
netacad.sadlab.su
11.2.4.6 Lab - Accessi...
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

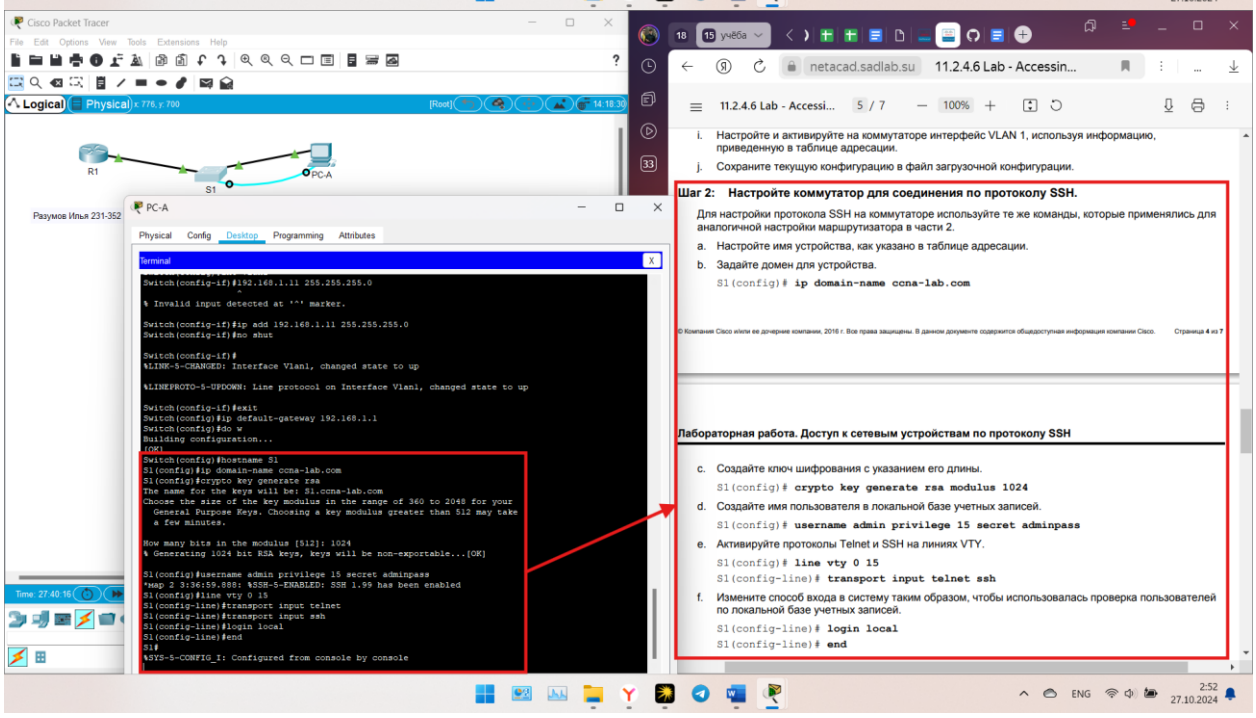

Cisco Packet Tracer
Router0
Switch0
PC-A
Разумов Илья 231-352
PC-A
Physical Config Desktop Programming Attributes
Terminal
R1>en
Password:
R1#ip domain-name ccna-lab.com
% Invalid input detected at '^' marker.
R1#ip doma
% Invalid input detected at '^' marker.
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 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
*map 1 0:45:38.515: %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/Z.
R1(config)#ip ssh ver 2
R1(config)#
netacad.sadlab.su
11.2.4.6 Lab - Accessi...
11.2.4.6 Lab - Acces...
3 / 7
73%
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
Лабораторная работа. Доступ к сетевым устройствам по протоколу 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#
ENG
0:01
27.10.2024

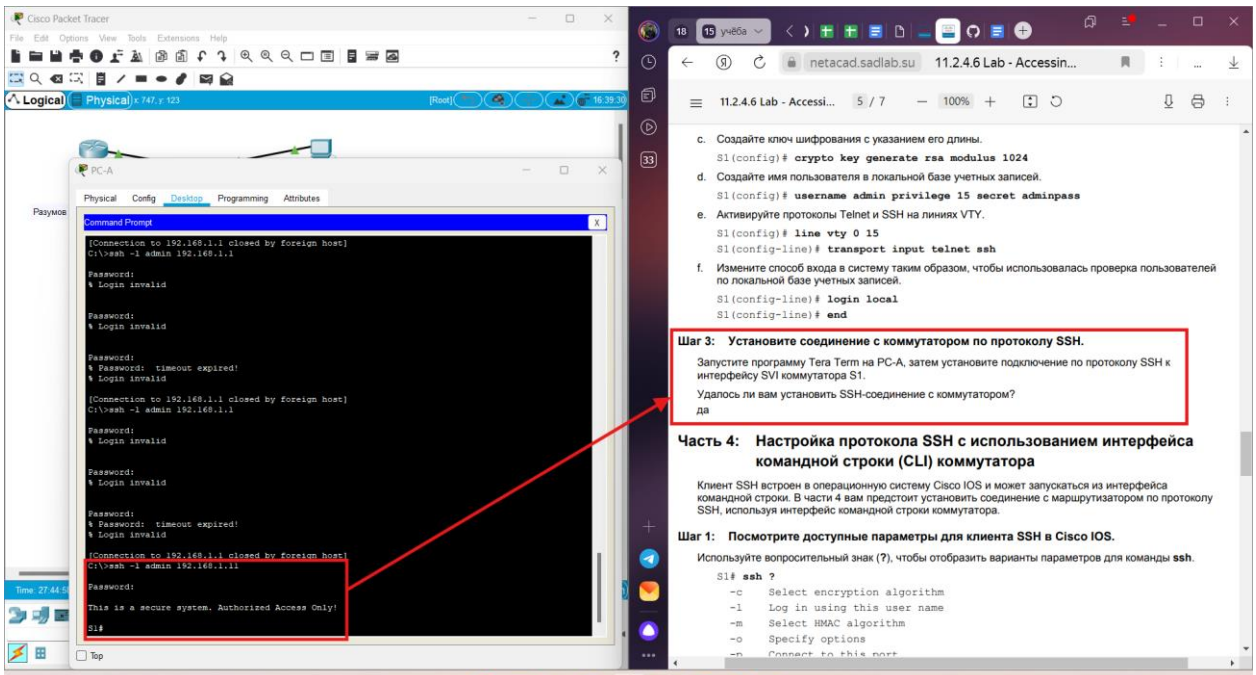

Cisco Packet Tracer
Router0
Switch0
PC-A
Разумов Илья 231-352
PC-A
Physical Config Desktop Programming Attributes
Terminal
R1#ip doma
% Invalid input detected at '^' marker.
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto 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 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
*map 1 0:45:38.515: %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/Z.
R1(config)#ip ssh ver 2
R1(config)#ex
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
netacad.sadlab.su
11.2.4.6 Lab - Accessi...
11.2.4.6 Lab - Acces...
4 / 7
73%
Лабораторная работа. Доступ к сетевым устройствам по протоколу 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#
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.
ENG
0:04
27.10.2024

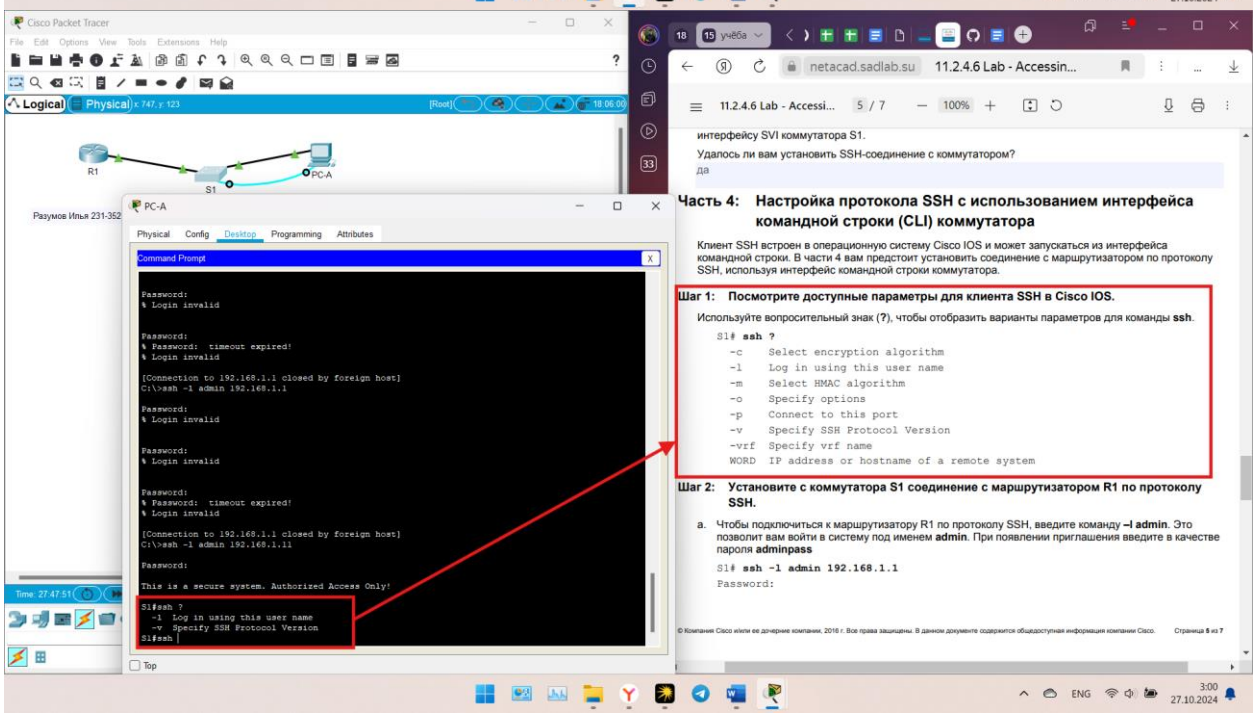

Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
Telnet / SSH Client
Session Options
Connection Type
SSH
Host Name or (IP address)
192.168.1.1
Username
admin
Connect
Top
11.2.4.6 Lab - Accessin...
Шаг 6: Установите соединение с маршрутизатором 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
Шаг 1: Настройте основные параметры коммутатора.
Шаг 2: Настройте коммутатор для соединения по протоколу SSH.
Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

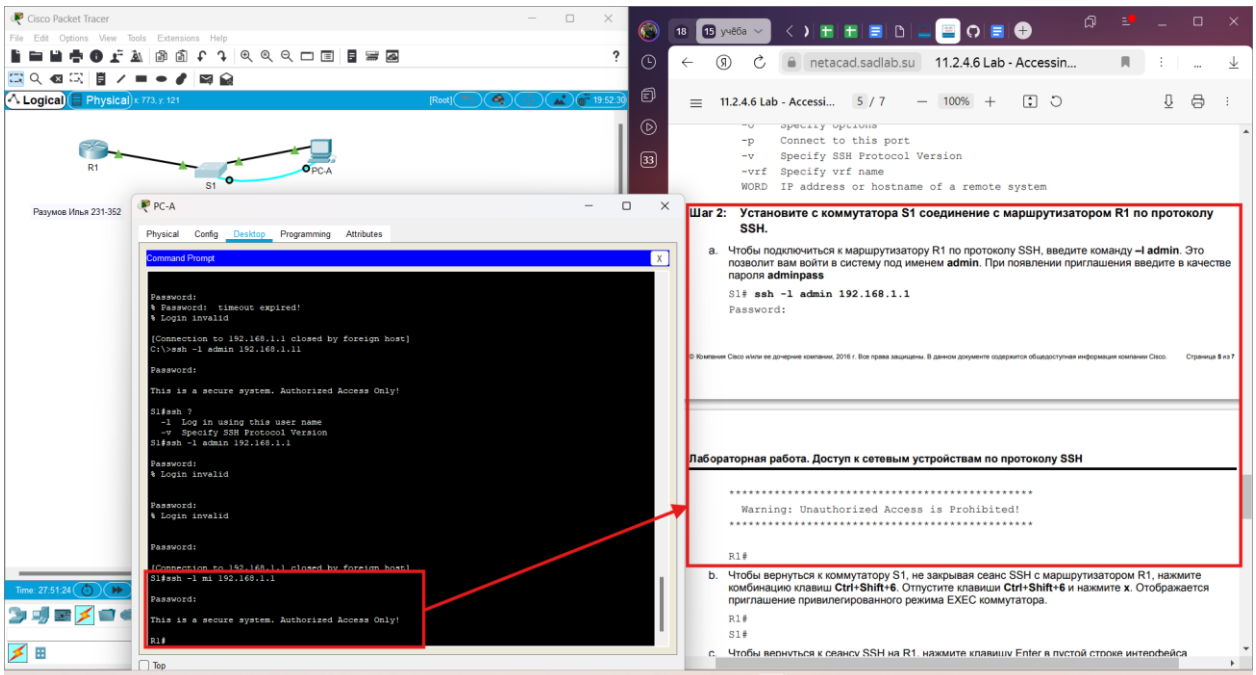

Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
SSH Client
Password:
This is a secure system. Authorized Access Only!
R1#
Top
11.2.4.6 Lab - Accessin...
Шаг 6: Установите соединение с маршрутизатором по протоколу SSH.
a. Запустите 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
Шаг 1: Настройте основные параметры коммутатора.
Шаг 2: Настройте коммутатор для соединения по протоколу SSH.
Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH

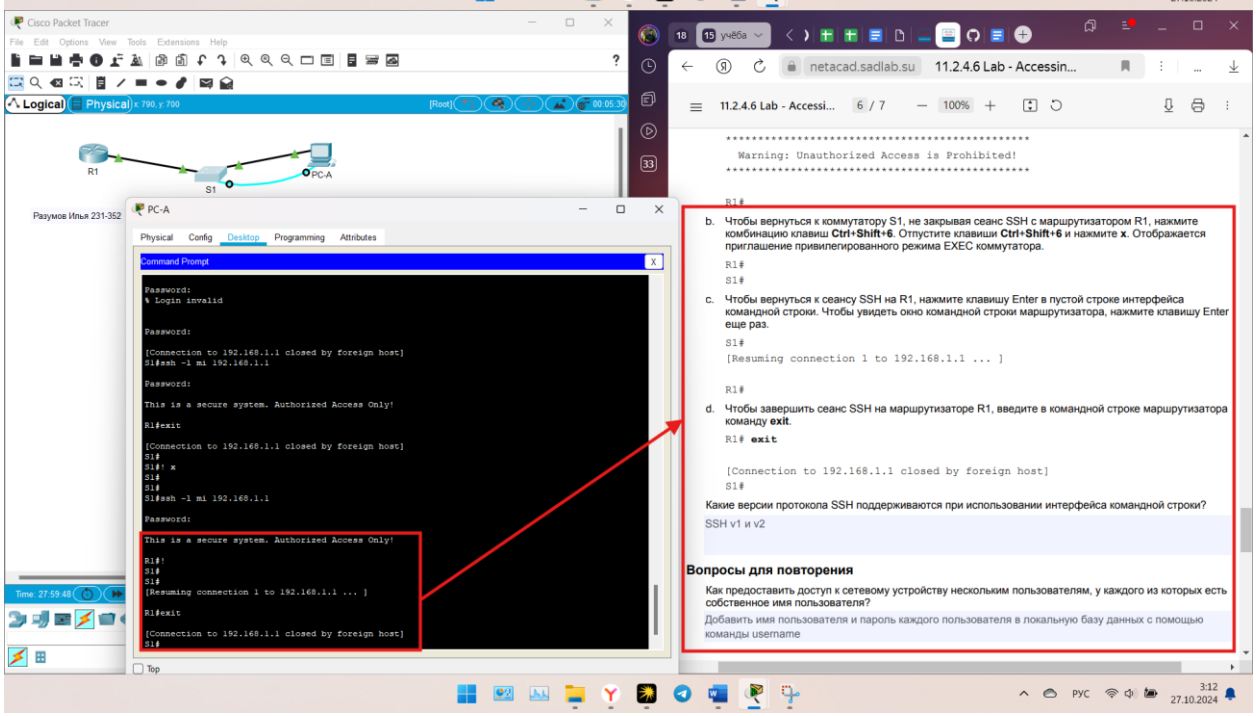

Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
Terminal
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#enable secret class
Switch(config)#line con 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#ex
% Ambiguous command: "ex"
Switch(config-line)#exit
Switch(config)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
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 default-gateway 192.168.1.1
Switch(config)#do w
Building configuration...
[OK]
Switch(config)#
netacad.sadlab.su
11.2.4.6 Lab - Accessin...
11.2.4.6 Lab - Accessi...
4 / 7
73%
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
Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH
c. Создайте ключ шифрования с указанием его длины.


Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
Разумов Илья 231-352
PC-A
Physical
Config
Desktop
Programming
Attributes
Terminal
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 default-gateway 192.168.1.1
Switch(config)#do w
Building configuration...
[OK]
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 2 3:36:59.888: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
netacad.sadlab.su
11.2.4.6 Lab - Accessin...
11.2.4.6 Lab - Accessi...
5 / 7
100%
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
Лабораторная работа. Доступ к сетевым устройствам по протоколу SSH
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


Cisco Packet Tracer
PC-A
Command Prompt
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.1
Password:
% Login invalid
% Password: timeout expired!
This is a secure system. Authorized Access Only!
S1#
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


Cisco Packet Tracer
PC-A
Command Prompt
S1#ssh ?
-l Log in using this user name
-v Specify SSH Protocol Version
S1#ssh |
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:


Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Password:
% Password: timeout expired!
% Login invalid
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.11
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:
% Login invalid
Password:
% Login invalid
Password:
[Connection to 192.168.1.1 closed by foreign host]
S1#ssh -l mi 192.168.1.1
Password:
This is a secure system. Authorized Access Only!
R1#
Top
Разумов Илья 231-352
11.2.4.6 Lab - Accessin...
-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


Cisco Packet Tracer
Logical
Physical
R1
S1
PC-A
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Password:
% Login invalid
Password:
[Connection to 192.168.1.1 closed by foreign host]
S1#ssh -l mi 192.168.1.1
Password:
This is a secure system. Authorized Access Only!
R1#exit
[Connection to 192.168.1.1 closed by foreign host]
S1#
S1#! x
S1#
S1#
S1#ssh -l mi 192.168.1.1
Password:
This is a secure system. Authorized Access Only!
R1#!
S1#
S1#
[Resuming connection 1 to 192.168.1.1 ...]
R1#exit
[Connection to 192.168.1.1 closed by foreign host]
S1#
Top
Разумов Илья 231-352
11.2.4.6 Lab - Accessin...
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?
SSH v1 и v2
Вопросы для повторения
Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?
Добавить имя пользователя и пароль каждого пользователя в локальную базу данных с помощью команды username