

## Таблица VLAN

VLAN	Имя	Назначенный интерфейс
20	Management	S2: F0/5
30	Operations	S1: F0/6
40	Sales	S2: F0/18
999	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2
1000	Native	—

## Задачи

**Часть 1. Создание сети и настройка основных параметров устройства**

**Часть 2. Настройка сетей VLAN на коммутаторе**

**Часть 3. Настройка магистральных каналов**

**Часть 4. Настройка маршрутизации**

**Часть 5. Настройка удаленного доступа**

**Часть 6. Проверка связи**

**Часть 7. Настройка и проверка списков расширенного контроля доступа**

## Общие сведения и сценарий

В этом задании в режиме симуляции физического оборудования (PTPM) вам было поручено настроить списки управления доступом (ACL) в сети небольшой компании. ACL являются одним из самых простых и прямых средств управления трафиком уровня 3. R1 будет размещать интернет-соединение и делиться информацией о маршруте по умолчанию с R2. После завершения первоначальной настройки у компании есть некоторые особые требования к безопасности трафика, за выполнение которых вы будете нести ответственность.

**Примечание:** В этом задании было набрано более 100 баллов. Таким образом Packet Tracer будет отображать количество баллов в режиме реального времени вместо процентного балла.

## Инструкции

**Часть 1. Создание сети и настройка основных параметров устройства**

**Шаг 1. Создайте сеть согласно топологии.**

- a. Подключите устройства в соответствии с топологией и подсоедините соответствующие кабели. Используйте консольный кабель для подключения PC к каждому коммутатору или маршрутизатору при их настройке. Чтобы получить доступ к коммутатору или маршрутизатору, необходимо подключить консольный кабель между PC и устройством, которое вы хотите настроить. Мы рекомендуем подключить PC-A к R1 и PC-B к R2.
- b. Затем при настройке коммутаторов подключите PC-A к S1 и PC-B к S2. После подключения консольного кабеля выберите PC > Desktop tab > Terminal и нажмите кнопку «OK», чтобы открыть командную строку.

При замене консольного кабеля на новое устройство, например между маршрутизатором и коммутатором, легче нажать на конец консольного кабеля и перетащить его обратно на панель для кабелей, чем пытаться подключить кабель напрямую к другому устройству. После подключения консольного кабеля к другому устройству необходимо закрыть и снова открыть окно терминала, чтобы установить новое подключение.

**Шаг 2. Произведите базовую настройку маршрутизаторов.**

- a. Назначьте маршрутизатору имя устройства.
- b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- c. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
- d. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
- e. Установите cisco в качестве пароля vty. Вы включите вход (login) позже в этом задании.
- f. Зашифруйте открытые пароли.
- g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
- h. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain?
domain  domain-lookup  domain-name
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#exit
R1(config)#service password-encryptions
^
% Invalid input detected at '^' marker.

R1(config)#service password-encryption
R1(config)#banner motd "Some"
R1(config)#|
```

```
Router>enable
Router#config 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)#exit
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#banner motd "Some"
Router(config)#w
^
% Invalid input detected at '^' marker.

Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#w
Building configuration...
[OK]
Router#
```

### Шаг 3. Настройте базовые параметры каждого коммутатора.

- a. Присвойте коммутатору имя устройства.
- b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- c. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
- d. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
- e. Установите cisco в качестве пароля vty. Вы включите вход (login) позже в этом задании.
- f. Зашифруйте открытые пароли.
- g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
- h. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#exit
S1(config)#banner motd "Some"
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
w
Building configuration...
[OK]
S1#
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd "Some"
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#w
Building configuration...
[OK]
S2#|
```

## Часть 2. Настройка сетей VLAN на коммутаторах.

### Шаг 1. Создайте сети VLAN на коммутаторах.

- Создайте необходимые VLAN и назовите их на каждом коммутаторе из приведенной выше таблицы.

```
S1>#
S1(config)#vlan 20
S1(config-vlan)#name Management
S1(config-vlan)#vlan 30
S1(config-vlan)#Operations
^
% Invalid input detected at '^' marker.

S1(config-vlan)#name Operations
S1(config-vlan)#vlan 40
S1(config-vlan)#name Sales
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#vlan 1000
S1(config-vlan)#name Native
S1(config-vlan)#[
```

```
S2>enable
Password:
Password:
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 20
S2(config-vlan)#name Management
S2(config-vlan)#vlan 30
S2(config-vlan)#name Operations
S2(config-vlan)#vlan 40
S2(config-vlan)#name Sales
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#vlan 1000
S2(config-vlan)#Native
^
% Invalid input detected at '^' marker.

S2(config-vlan)#name Native
S2(config-vlan)#[
```

- b. Настройте интерфейс управления и шлюз по умолчанию на каждом коммутаторе, используя информацию об IP-адресе в таблице адресации.

```
S1(config)#int vlan 20
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

S1(config-if)#ip address 10.20.0.2 255.255.255.0
S1(config-if)#ip default-gateway 10.20.0.1
S1(config)#[
```

```
S2(config-if)#ip address 10.20.0.3 255.255.255.0
S2(config-if)#ip default-gateway 10.20.0.1
S2(config)#[
```

- c. Назначьте все неиспользуемые порты коммутатора во VLAN Parking Lot. Настройте их в статический режима доступа и административно деактивируйте их.

```

S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 20
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

S1(config-if)#ip address 10.20.0.2 255.255.255.0
S1(config-if)#ip default-gateway 10.20.0.1
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int range f0/2-4, f0/7-24. g0/1-2
^
% Invalid input detected at '^' marker.

S1(config-if)#int range f0/2-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown

```

```

S2>enable
Password:
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/5
S2(config-if)#switchport ?
  access          Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  nonegotiate    Device will not engage in negotiation protocol on this
                  interface
  port-security   Security related command
  priority        Set appliance 802.1p priority
  protected       Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
  voice           Voice appliance attributes
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 40
S2(config-if)#int range f0/2-4, f0/6-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown

```

**Примечание:** Команда `interface range` помогает выполнить эту задачу с помощью минимального количества команд, если это необходимо.

## Шаг 2. Назначьте сети VLAN соответствующим интерфейсам коммутатора.

- Назначьте используемые порты соответствующей VLAN (указанной в таблице VLAN выше) и настройте их в режим статического доступа.
- Выполните команду `show vlan brief`, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

## Часть 3. ·Настройте транки (магистральные каналы).

## Шаг 1. Вручную настройте магистральный интерфейс F0/1.

- Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать магистральную связь. Не забудьте сделать это на обоих коммутаторах.
- В рамках конфигурации транка установите для native vlan значение 1000 на обоих коммутаторах. Вы можете временно видеть сообщения об ошибках, пока два интерфейса настроены для разных native VLAN.
- В качестве другой части конфигурации транка укажите, что VLAN 10, 20, 30 и 1000 разрешены в транке.

```
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#int f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

S1(config-if)#switchport trunk native vlan 1000
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1000), with FastEthernet0/1 (1).

S1(config-if)#switchport trunk allowed vlan 10,20,30,1000
S1(config-if)#

```

```
S2>enable
Password:
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S
FastEthernet0/1 (1000).

S2(config)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 1000
S2(config-if)##%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN1000. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency restored.

S2(config-if)#switchport trunk allowed vlan 10,20,30,1000
S2(config-if)#

```

- Выполните команду show interfaces trunk для проверки портов магистрали, собственной VLAN и разрешенных VLAN через магистраль.

```
S1#show interfaces trunk
Port      Mode       Encapsulation  Status        Native vlan
Fa0/1     on         802.1q          trunking    1000

Port      Vlans allowed on trunk
Fa0/1     10,20,30,1000

Port      Vlans allowed and active in management domain
Fa0/1     20,30,1000

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     20,30,1000

```

```

S2#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1    on        802.1q        trunking    1000

Port      Vlans allowed on trunk
Fa0/1    10,20,30,1000

Port      Vlans allowed and active in management domain
Fa0/1    20,30,1000

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    none

```

## Шаг 2. Вручную настройте магистральный интерфейс F0/5 на коммутаторе S1.

- Настройте интерфейс S1 F0/5 с теми же параметрами транка, что и F0/1. Это магистральное соединение до R1.
- Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```

S1#
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1000
S1(config-if)#switchport trunk allowed 10,20,30,1000
                           ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport trunk allowed vlan 10,20,30,1000
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#w
Building configuration...
[OK]
S1#

```

## Часть 4. Настройте маршрутизацию.

### Шаг 1. Настройка маршрутизации между сетями VLAN на R1.

- Активируйте интерфейс G0/0/1 на маршрутизаторе.
- Настройте подинтерфейсы для каждой VLAN, как указано в таблице IP-адресации. Все подинтерфейсы используют инкапсуляцию 802.1Q. Убедитесь, что подинтерфейс для собственной VLAN не имеет назначенного IP-адреса. Включите описание для каждого подинтерфейса.
- Настройте интерфейс G0/0/1 на R1 с адресацией из таблицы адресации.

```

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit
R1(config)#int g0/0/1.20
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20, changed state to up

R1(config-subif)#ip address 10.20.0.1 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.20.0.1 255.255.255.0
R1(config-subif)#description "VLAN 20 Management"
R1(config-subif)#exit
R1(config)#int g0/0/1.30
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to up

R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.30.0.1 255.255.255.0
R1(config-subif)#description "VLAN 30 Operations"
R1(config-subif)#exit
R1(config)#int g0/0/1.40
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.40, changed state to up

R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#description "VLAN 40 Salse"
R1(config-subif)#ip address 10.40.0.1 255.255.255.0
R1(config-subif)#

```

```

R1(config-subif)#encapsulation dot1Q 1000
R1(config-subif)#description "VLAN 1000 Native"
R1(config-subif)#int g0/0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#end

```

- e. С помощью команды show ip interface brief проверьте конфигурацию подынтерфейса.

```

R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0 172.16.1.1    YES manual administratively down down
GigabitEthernet0/0/1  unassigned     YES unset   up           up
GigabitEthernet0/0/1.20 10.20.0.1   YES manual up           up
GigabitEthernet0/0/1.30 10.30.0.1   YES manual up           up
GigabitEthernet0/0/1.40 10.40.0.1   YES manual up           up
GigabitEthernet0/0/1.100  unassigned YES unset   up           up
Vlan1              unassigned     YES unset   administratively down down
R1#

```

**Шаг 2. Настройка интерфейса R2 g0/0/1 с использованием адреса из таблицы и маршрута по умолчанию с адресом следующего перехода 10.20.0.1**

```
Router configuration commands, one per line, end with Ctrl-Z.  
Router(config)#int g0/0/1  
Router(config-if)#ip address 10.20.0.4 255.255.255.0  
Router(config-if)#
```

## Часть 5. Настройте удаленный доступ

### Шаг 1. Настройте все сетевые устройства для базовой поддержки SSH.

- Создайте локального пользователя с именем пользователя SSHadmin и зашифрованным паролем \$cisco123!
- Используйте ccna-lab.com в качестве доменного имени.
- Генерируйте криптоключи с помощью 1024 битного модуля.
- Настройте первые пять линий VTY на каждом устройстве, чтобы поддерживать только SSH-соединения и с локальной аутентификацией.

```
R1(config)#username SSHadmin secret $cisco123!  
R1(config)#ip domain-name ccna-lab.com  
R1(config)#crypto ?  
  dynamic-map   Specify a dynamic crypto map template  
  ipsec        Configure IPSEC policy  
  isakmp       Configure ISAKMP policy  
  key          Long term key operations  
  map          Enter a crypto map  
R1(config)#crypto key generate rsa  
% You already have RSA keys defined named R1.ccna.lab .  
% Do you really want to replace them? [yes/no]: y  
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)#line vty 0 4  
*Mar 1 1:25:46.413: %SSH-5-ENABLED: SSH 1.99 has been enabled  
R1(config-line)#transport input ssh  
R1(config-line)#login local  
R1(config-line)#+
```

```
Router(config)#username SSHadmin secret $cisco123!  
Router(config)#ip domain-name ccna-lab.com  
Router(config)#crypto key generate rsa  
% Please define a hostname other than Router.  
Router(config)#hostname R2  
R2(config)#crypto key generate rsa  
% You already have RSA keys defined named R2.ccna.com .  
% Do you really want to replace them? [yes/no]: y  
The name for the keys will be: R2.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]  
  
R2(config)#line vty 0 4  
*Mar 1 1:29:8.676: %SSH-5-ENABLED: SSH 1.99 has been enabled  
R2(config-line)#transport input ssh  
R2(config-line)#login local  
R2(config-line)#+
```

```

S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#username SSHadmin secret $cisc0123!
S1(config)#ip domain-name ccna-lab.com
S1(config)#crypto key generate rsa
% You already have RSA keys defined named S1.ccna.com .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: S1.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]

S1(config)#line vty 0 4
*Mar 1 10:45:40.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#

S2>enable
Password:
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#username SSHadmin secret $cisc0123!
S2(config)#ip domain ccna-lab.com
^
% Invalid input detected at '^' marker.

S2(config)#ip domain-name ccna-lab.com
S2(config)#crypto key generate rsa
% You already have RSA keys defined named S2.ccna.com .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: S2.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]

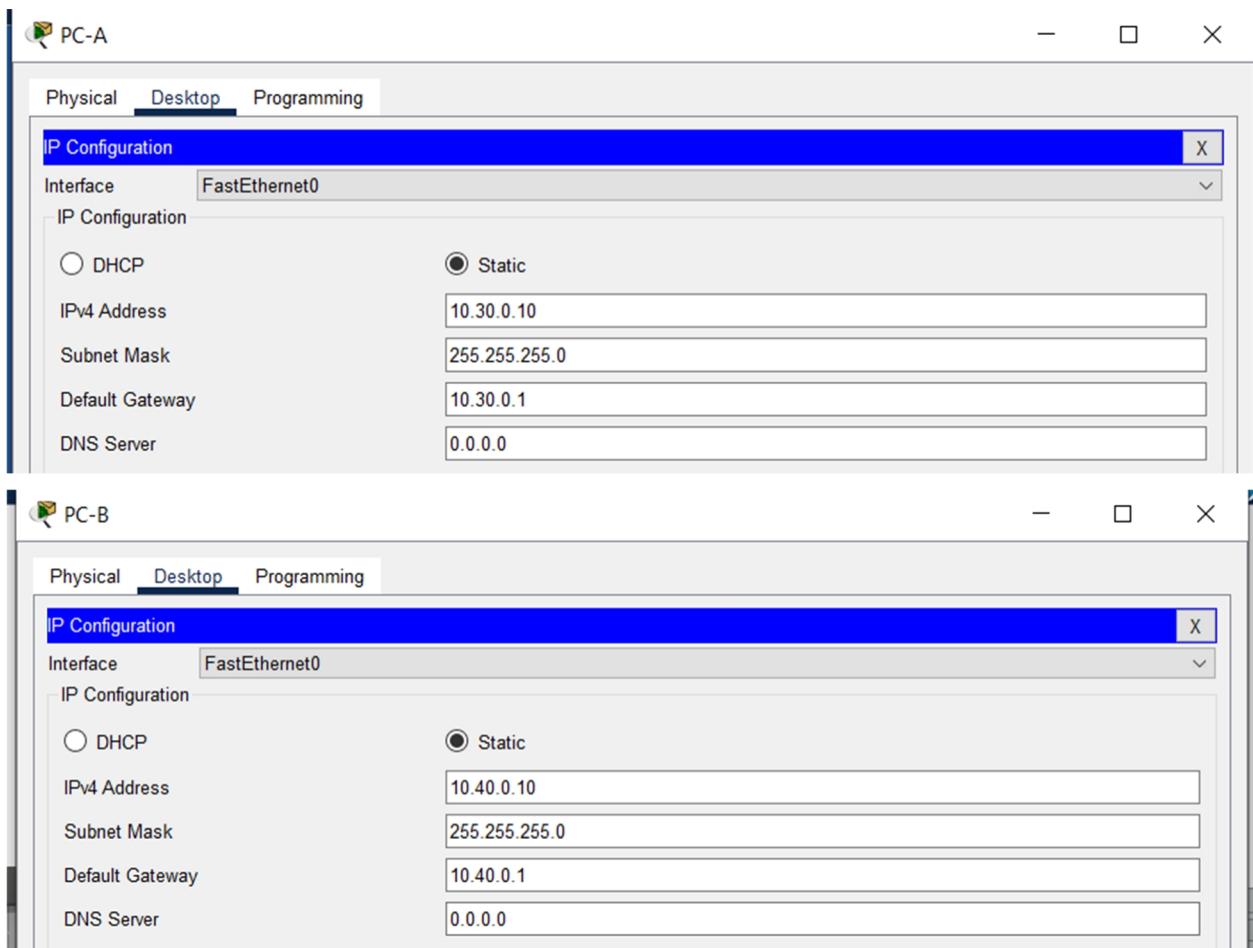
S2(config)#line vty 0 4
*Mar 1 10:48:12.158: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#

```

## Часть 6. Проверка подключения

### Шаг 1. Настройте узлы ПК.

Адреса ПК можно посмотреть в таблице адресации.



## Шаг 2. Выполните следующие тесты. Эхозапрос должен пройти успешно.

**Примечание.** Если вы нажмете кнопку Check Results, вы увидите, что пять выделенных Connectivity Tests отображаются как неправильные. Это связано с тем, что вы еще не реализовали списки ACL. После реализации списков ACL эти пять выделенных Connectivity Tests должны успешно завершиться неудачей.

От	Протокол	Назначение	Результат
PC-A	Ping	10.40.0.10	Успех
PC-A	Ping	10.20.0.1	Успех
PC-B	Ping	10.30.0.10	Успех
PC-B	Ping	10.20.0.1	Успех
PC-B	Ping	172.16.1.1	Успех
PC-B	HTTPS	172.16.1.2	Успех
PC-A	HTTPS	172.16.1.2	Успех
PC-B	SSH	10.20.0.4	Успех
PC-B	SSH	172.16.1.1	Успех

## Часть 7. Настройка и проверка списков расширенного контроля доступа

При проверке базового подключения компания требует реализации следующих политик безопасности:

**Политика 1:** Сеть Sales не может использовать SSH в сети Management (но в другие сети SSH разрешен).

**Политика 2:** Сеть Sales не имеет доступа к server -A с помощью любого веб-протокола (HTTP/HTTPS). Весь остальной веб-трафик должен быть разрешен.

**Политика 3:** Сеть Sales не может отправлять эхо-запросы ICMP в сети Operations или Management. Разрешены эхо-запросы ICMP к другим адресатам.

**Политика 4:** Сеть Operations не может отправлять ICMP эхозапросы в сеть Sales. Разрешены эхо-запросы ICMP к другим адресатам.

```
R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list extended 101
R1(config-ext-nacl)#deny tcp 10.40.0.0 0.0.0.255 10.20.0.1
% Incomplete command.
R1(config-ext-nacl)#deny tcp 10.40.0.0 0.0.0.255 10.20.0.1 eq 22
^
% Invalid input detected at '^' marker.

R1(config-ext-nacl)#deny tcp 10.40.0.0 0.0.0.255 10.20.0.1 0.0.0.255 eq 22
R1(config-ext-nacl)#permit any any
^
% Invalid input detected at '^' marker.

R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended 102
R1(config-ext-nacl)#deny tcp 10.40.0.0 0.0.0.255 host 172.16.1.2 eq 80
R1(config-ext-nacl)#deny tcp 10.40.0.0 0.0.0.255 host 172.16.1.2 eq 443
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended 103
R1(config-ext-nacl)#deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255
R1(config-ext-nacl)#deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended 104
R1(config-ext-nacl)#deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#

```

**Шаг 1. Разработка и применение расширенных списков доступа, которые будут соответствовать требованиям политики безопасности.**

```

R1(config)#int g0/0/0
R1(config-if)#ip access-group 102 out
R1(config-if)#exit
R1(config)#int g0/0/1.40
R1(config-subif)#ip access-group 101
% Incomplete command.
R1(config-subif)#ip ?
  access-group      Specify access control for packets
  address          Set the IP address of an interface
  authentication   authentication subcommands
  flow             NetFlow Related commands
  hello-interval  Configures IP-EIGRP hello interval
  helper-address   Specify a destination address for UDP broadcasts
  mtu              Set IP Maximum Transmission Unit
  nat               NAT interface commands
  ospf              OSPF interface commands
  proxy-arp        Enable proxy ARP
  split-horizon    Perform split horizon
  summary-address  Perform address summarization
R1(config-subif)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
R1(config-subif)#ip access-group 101
% Incomplete command.
R1(config-subif)#ip access-group 101 out
R1(config-subif)#exit
R1(config)#int g0/0/1.20
R1(config-subif)#ip access-group 103 out
R1(config-subif)#int g0/0/1.30
R1(config-subif)#ip access-group 103 out
R1(config-subif)#int g0/0/1.40
R1(config-subif)#ip access-group 104 out
R1(config-subif)#

```

**Шаг 2. Убедитесь, что политики безопасности применяются расширенными списками доступа.**

Выполните следующие тесты. Ожидаемые результаты показаны в таблице:

**Примечание.** Нажмите кнопку Check Results, чтобы заставить Packet Tracer снова запустить все Connectivity Tests.

От	Протокол	Назначение	Результат
PC-A	Ping	10.40.0.10	Сбой
PC-A	Ping	10.20.0.1	Успех
PC-B	Ping	10.30.0.10	Сбой
PC-B	Ping	10.20.0.1	Сбой
PC-B	Ping	172.16.1.1	Успех
PC-B	HTTPS	172.16.1.2	Сбой
PC-A	HTTPS	172.16.1.2	Успех
PC-B	SSH	10.20.0.4	Сбой
PC-B	SSH	172.16.1.1	Успех