

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ БЕЛАРУСЬ**
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики

БОБОВОЗ ВЛАДИСЛАВ СЕРГЕЕВИЧ

Настройка списков контроля доступа на устройствах Cisco

Отчет по лабораторной работе № 14,
вариант 15
(“Компьютерные сети”)
студента 3-го курса 6-ой группы

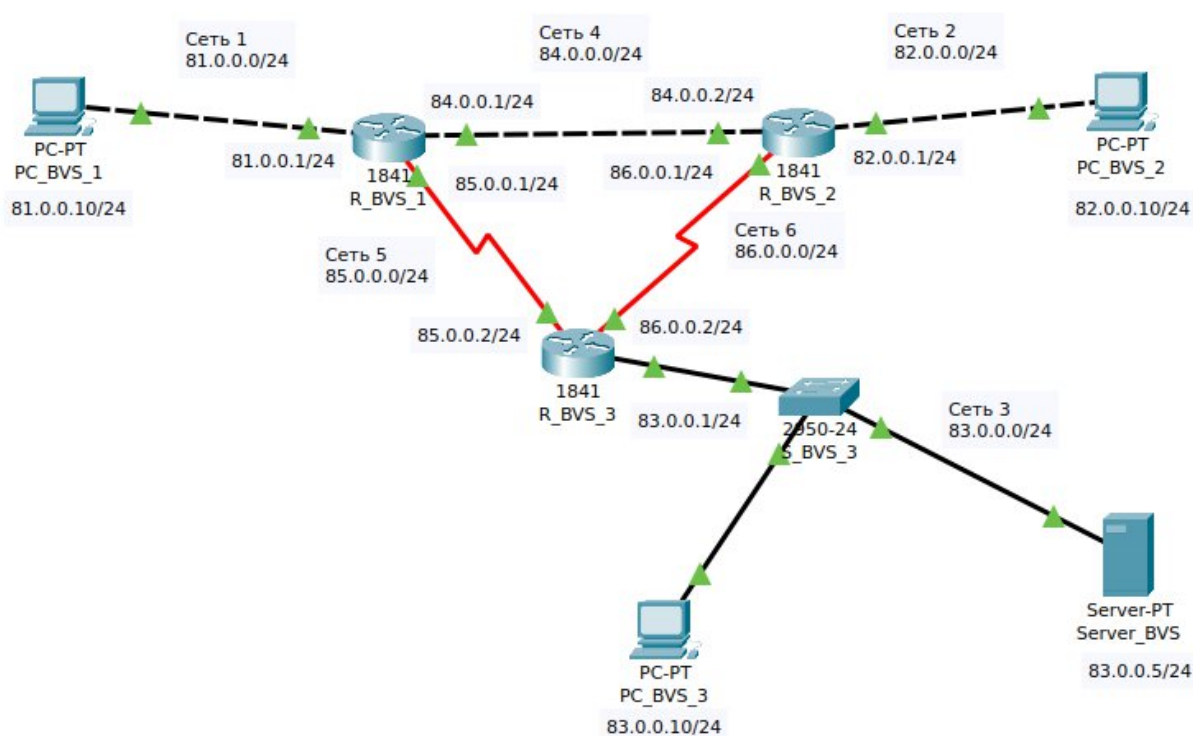
Преподаватель
Каллистратова Ю.А.

Минск 2024

Данные варианта задания:

Вариант	Сеть 1 - 6
15	81.0.0.0/24 82.0.0.0/24 83.0.0.0/24 84.0.0.0/24 85.0.0.0/24 86.0.0.0/24

Схема сети:



Цель работы.

С помощью стандартного и расширенного ACL-листов запретить доступ к некоторым ресурсам сети.

Этапы выполнения работы.

1. Соберите схему сети, приведенную на скриншоте. Согласно Вашему варианту, настройте маршрутизацию между узлами, задав маршруты

по умолчанию. Проверьте взаимодействие с узлами сети с помощью команды ping. (В отчет включить результаты пингов)

PC_BVS_1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 81.0.0.10

Subnet Mask 255.255.255.0

Default Gateway 81.0.0.1

DNS Server 0.0.0.0

PC_BVS_2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 82.0.0.10

Subnet Mask 255.255.255.0

Default Gateway 82.0.0.1

DNS Server 0.0.0.0

PC_BVS_3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

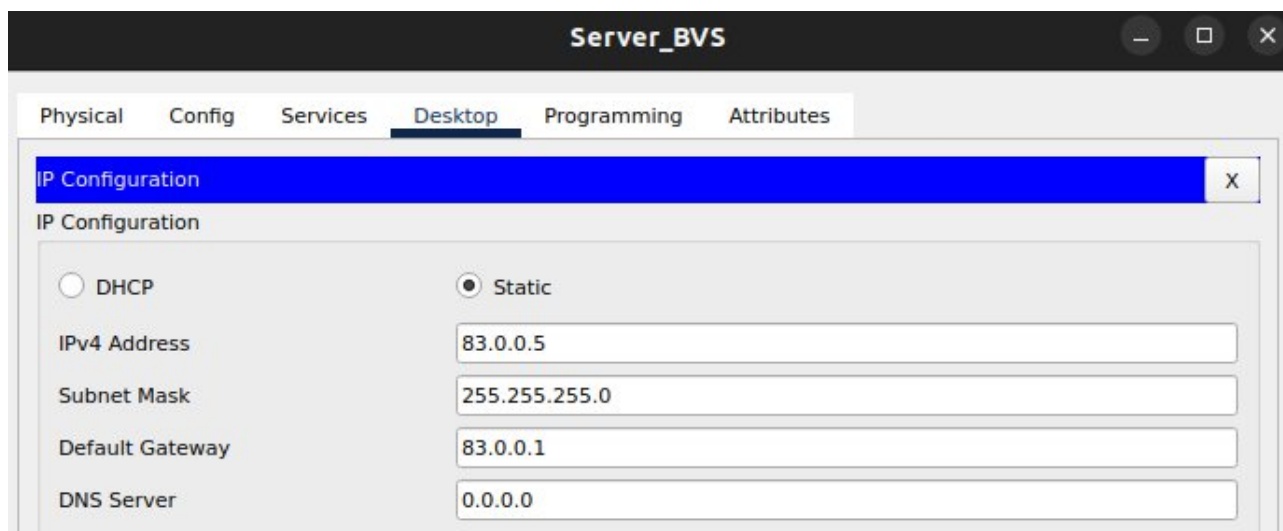
☐ DHCP ☒ Static

IPv4 Address 83.0.0.10

Subnet Mask 255.255.255.0

Default Gateway 83.0.0.1

DNS Server 0.0.0.0



```
R_BVS_1(config)#interface FastEthernet0/0
R_BVS_1(config-if)#ip address 81.0.0.1 255.255.255.0
R_BVS_1(config-if)#interface FastEthernet0/1
R_BVS_1(config-if)#ip address 84.0.0.1 255.255.255.0
R_BVS_1(config-if)#interface Serial0/0/0
R_BVS_1(config-if)#ip address 85.0.0.1 255.255.255.0
```

```
R_BVS_2(config)#interface FastEthernet0/0
R_BVS_2(config-if)#ip address 82.0.0.1 255.255.255.0
R_BVS_2(config-if)#interface FastEthernet0/1
R_BVS_2(config-if)#ip address 84.0.0.2 255.255.255.0
R_BVS_2(config-if)#interface Serial0/0/1
R_BVS_2(config-if)#ip address 86.0.0.1 255.255.255.0
```

```
R_BVS_3(config)#interface FastEthernet0/0
R_BVS_3(config-if)#ip address 83.0.0.1 255.255.255.0
R_BVS_3(config-if)#interface Serial0/0/0
R_BVS_3(config-if)#ip address 85.0.0.2 255.255.255.0
R_BVS_3(config-if)#interface Serial0/0/1
R_BVS_3(config-if)#ip address 86.0.0.2 255.255.255.0
```

Настройка маршрутов по умолчанию

```
R_BVS_1(config)#ip route 0.0.0.0 0.0.0.0 85.0.0.2
R_BVS_1(config)#ip route 0.0.0.0 0.0.0.0 84.0.0.2
```

```
R_BVS_2(config)#ip route 0.0.0.0 0.0.0.0 84.0.0.1
R_BVS_2(config)#ip route 0.0.0.0 0.0.0.0 86.0.0.2
```

```
R_BVS_3(config)#ip route 0.0.0.0 0.0.0.0 85.0.0.1
R_BVS_3(config)#ip route 0.0.0.0 0.0.0.0 86.0.0.1
```

Проверка доступности устройств с помощью инструментов пакета Cisco:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC_BVS_1	PC_BVS_2	IC...		0.000	N	0
	Successful	PC_BVS_1	PC_BVS_3	IC...		0.000	N	1
	Successful	PC_BVS_2	PC_BVS_1	IC...		0.000	N	2
	Successful	PC_BVS_2	PC_BVS_3	IC...		0.000	N	3
	Successful	PC_BVS_3	PC_BVS_1	IC...		0.000	N	4
	Successful	PC_BVS_3	PC_BVS_2	IC...		0.000	N	5

Передача пакетов проходит успешно.

2. Через эмулятор браузера на узлах проверьте доступность HTTP-сервера. В строке браузера введите ip-адрес HTTP-сервера.



Сервер доступен.

3. Настройте на маршрутизаторе R1 стандартный ACL, запрещающий устройству PC1 взаимодействовать с устройствами из других сетей

- 3.1. Зайдите в режим глобальной конфигурации маршрутизатора.

R1>enable

R1#configure terminal

- 3.2. Создайте стандартный ACL.

R1(config)#access-list 1 deny 192.168.1.10 0.0.0.0

R_BVS_1(config)#access-list 1 deny 81.0.0.10 0.0.0.0

access-list	Команда создания ACL
1	Номер ACL
deny	Команда «запретить»
192.168.1.10	Адрес, к которому надо применить команду
0.0.0.0	Wildcard маска

```
R1(config)#access-list 1 permit any
```

```
R_BVS_1(config)#access-list 1 permit any
```

3.3. Установите ACL на интерфейсе fa0/0 маршрутизатора R1.

```
R1(config)#interface fa 0/0
```

```
R1(config-if)#ip access-group 1 in
```

```
R_BVS_1(config)#interface FastEthernet0/0
```

```
R_BVS_1(config-if)#ip access-group 1 in
```

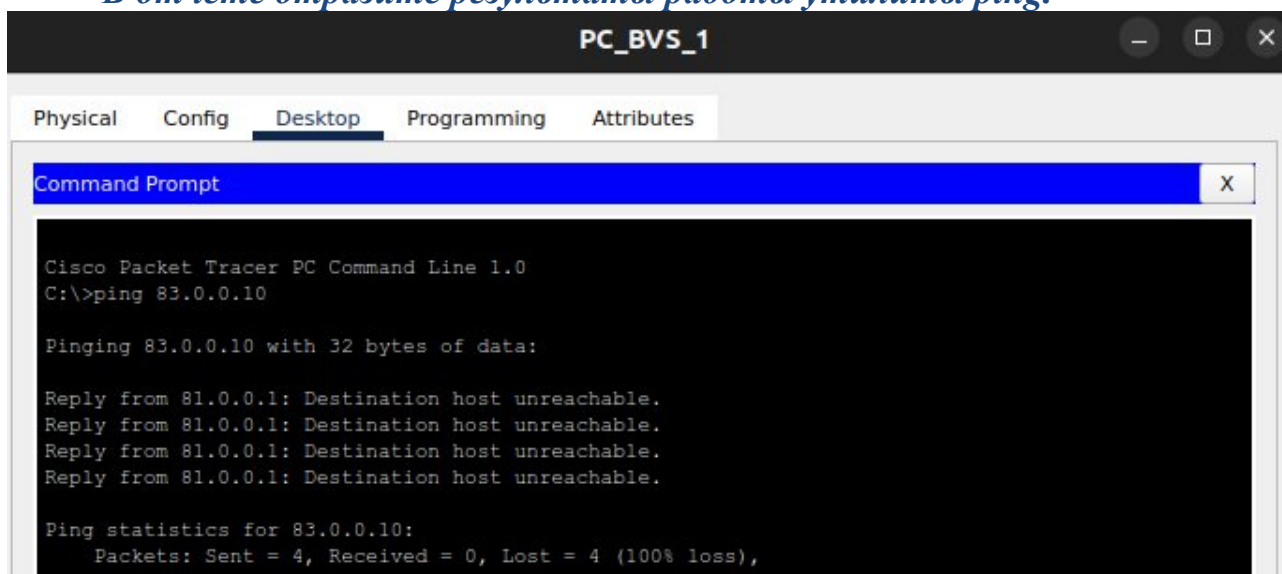
4. Проверьте правильность настройки стандартного ACL.

4.1. Зайдите в эмулятор командной строки на устройстве PC1.

4.2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC1 с

любым конечным устройством сети. Если PC1 не получает эхо ответы от другого устройства, ACL настроен правильно.

В отчёте отразите результаты работы утилиты ping.



Проверка доступности устройств с помощью инструментов пакета Cisco:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC_BVS_1	PC_BVS_2	IC...		0.000	N	0
	Failed	PC_BVS_1	PC_BVS_3	IC...		0.000	N	1
	Failed	PC_BVS_2	PC_BVS_1	IC...		0.000	N	2
	Successful	PC_BVS_2	PC_BVS_3	IC...		0.000	N	3
	Failed	PC_BVS_3	PC_BVS_1	IC...		0.000	N	4
	Successful	PC_BVS_3	PC_BVS_2	IC...		0.000	N	5

Передача пакетов не прошла, значит, ACL настроен правильно.

5. Настройте на маршрутизаторе R3 расширенный ACL, запрещающий устройству PC2 обращаться к веб-серверу по протоколу HTTP.

5.1. Зайдите в режим глобальной конфигурации маршрутизатора.

```
R3>enable
R3#configure terminal
```

5.2. Создайте расширенный ACL.

```
R3(config)#access-list 101 deny tcp 192.168.2.10 0.0.0.0 192.168.3.5 0.0.0.0 eq 80
```

access-list	Команда создания ACL
101	Номер ACL
deny	Команда «запретить»
tcp	Протокол транспортного уровня
192.168.2.10	Адрес источника
0.0.0.0	Wildcard маска для адреса источника
192.168.3.5	Адрес получателя
0.0.0.0	Wildcard маска для адреса получателя
eq 80	Порт назначения, по которому нужно запретить взаимодействие

```
R3(config)#access-list 101 permit ip any any
R3(config)#access-list 101 permit icmp any any
```

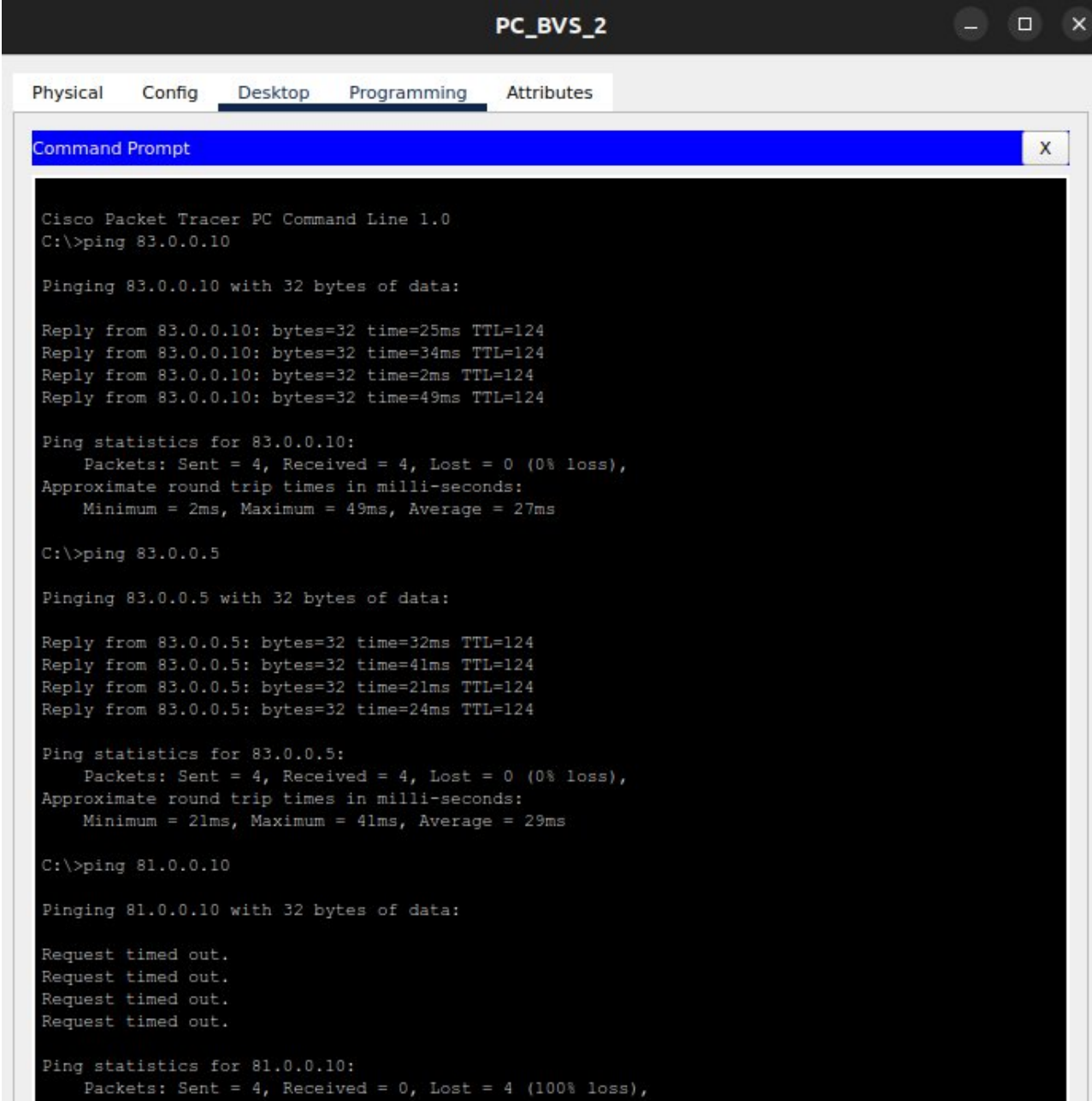
```
R_BVS_3(config)#access-list 101 deny tcp 82.0.0.10 0.0.0.0 83.0.0.5 0.0.0.0 eq 80
R_BVS_3(config)#access-list 101 permit ip any any
R_BVS_3(config)#access-list 101 permit icmp any any
```

5.3. Установите ACL на интерфейсе s0/0/1 маршрутизатора R3.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group 101 in
R_BVS_3(config)#interface serial0/0/1
R_BVS_3(config-if)#ip access-group 101 in
```

6. Проверьте правильность настройки расширенного ACL.

6.1. Зайдите в эмулятор командной строки на устройстве PC2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC2 с любым конечным устройством сети.



The screenshot shows a Command Prompt window titled "PC_BVS_2" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 83.0.0.10

Pinging 83.0.0.10 with 32 bytes of data:

Reply from 83.0.0.10: bytes=32 time=25ms TTL=124
Reply from 83.0.0.10: bytes=32 time=34ms TTL=124
Reply from 83.0.0.10: bytes=32 time=2ms TTL=124
Reply from 83.0.0.10: bytes=32 time=49ms TTL=124

Ping statistics for 83.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 49ms, Average = 27ms

C:\>ping 83.0.0.5

Pinging 83.0.0.5 with 32 bytes of data:

Reply from 83.0.0.5: bytes=32 time=32ms TTL=124
Reply from 83.0.0.5: bytes=32 time=41ms TTL=124
Reply from 83.0.0.5: bytes=32 time=21ms TTL=124
Reply from 83.0.0.5: bytes=32 time=24ms TTL=124

Ping statistics for 83.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 41ms, Average = 29ms

C:\>ping 81.0.0.10

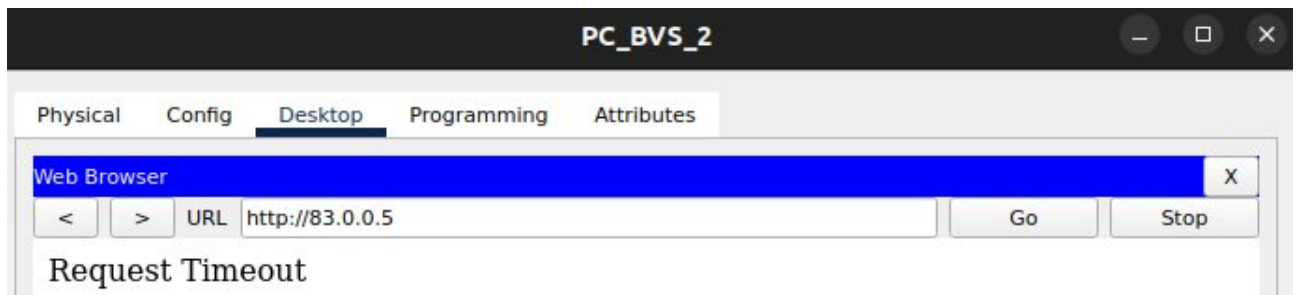
Pinging 81.0.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

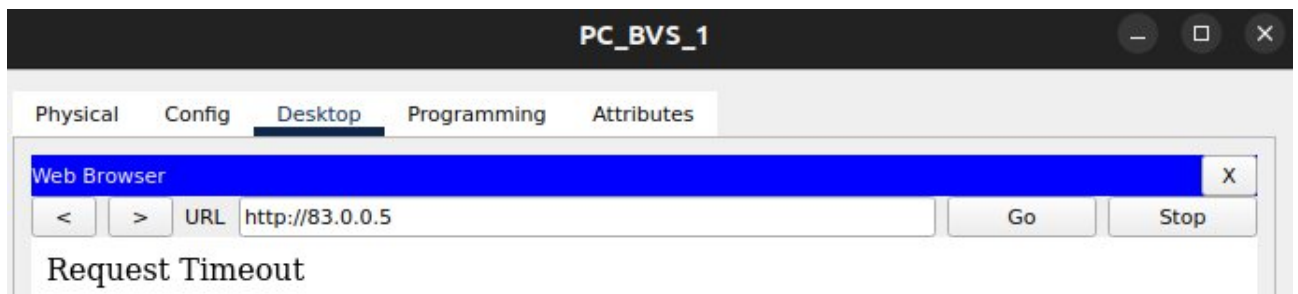
Ping statistics for 81.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Пинги на PC1 не проходят, так как для него был настроен запрет на взаимодействие с устройствами других сетей в задании 3. Эхо-ответы от PC3 и сервера получены.

6.2. С помощью эмулятора браузера попробуйте загрузить страницу HTTP-сервера по его адресу. Если устройство PC2 получает эхо-ответы от сервера, но страницу загрузить не удастся, значит ACL настроен правильно.



Страницу загрузить не удастся, но пинги с PC2 на сервер проходят успешно, значит, ACL настроен правильно.



С PC1 страницу загрузить не удастся, так как он не может взаимодействовать с устройствами других сетей из-за настроенного нами ACL. А у PC3 есть доступ к HTTP –серверу.