

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10

дисциплина: Администрирование локальных сетей

Студент: Каримов Зуфар

Группа: НПИ-01-18

Москва 2021

Оглавление

1. Цель работы.....	3
2. Постановка задачи.....	4
3. Порядок выполнения работы.....	5
4. Выводы	27
5. Контрольные вопросы.....	28

Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

Постановка задачи

1. Требуется настроить следующие правила доступа:

1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;

2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;

3) почтовый сервер: разрешить пользователям работать по протоколам SMTP и POP3 (соответственно через порты 25 и 110 протокола TCP), а для администратора — открыть доступ по протоколам Telnet и FTP;

4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;

5) разрешить icmp-сообщения, направленные в сеть серверов;

6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;

7) разрешить доступ в сеть управления сетевым оборудованием только администратору сети.

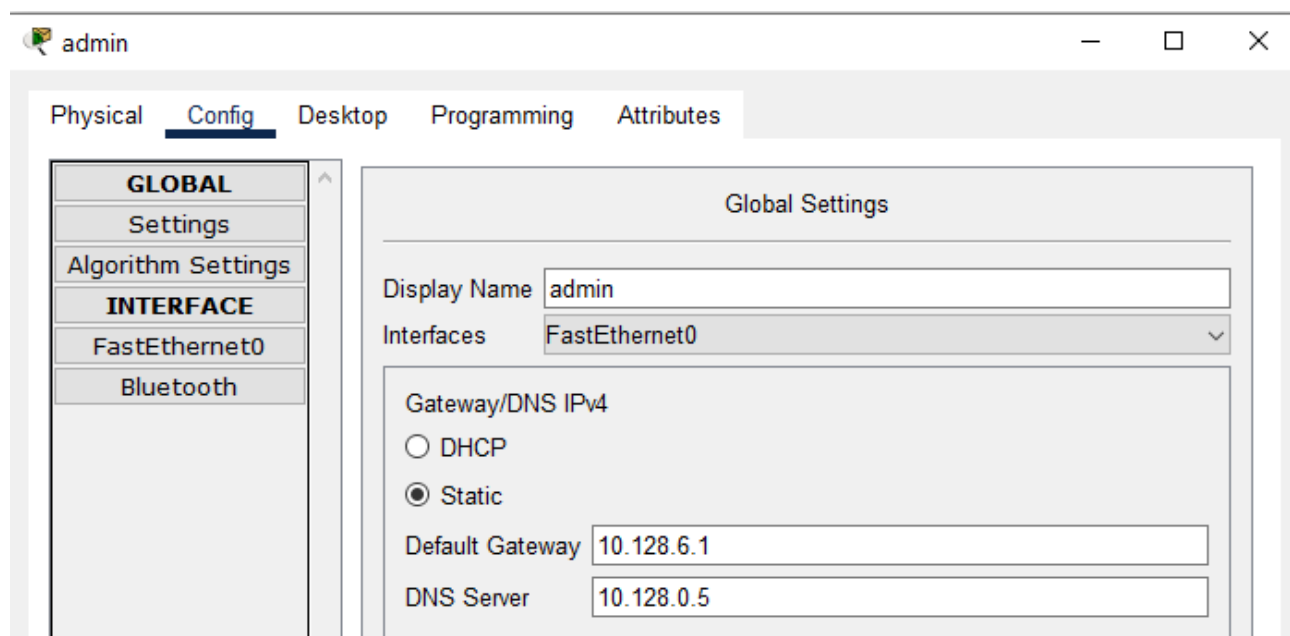
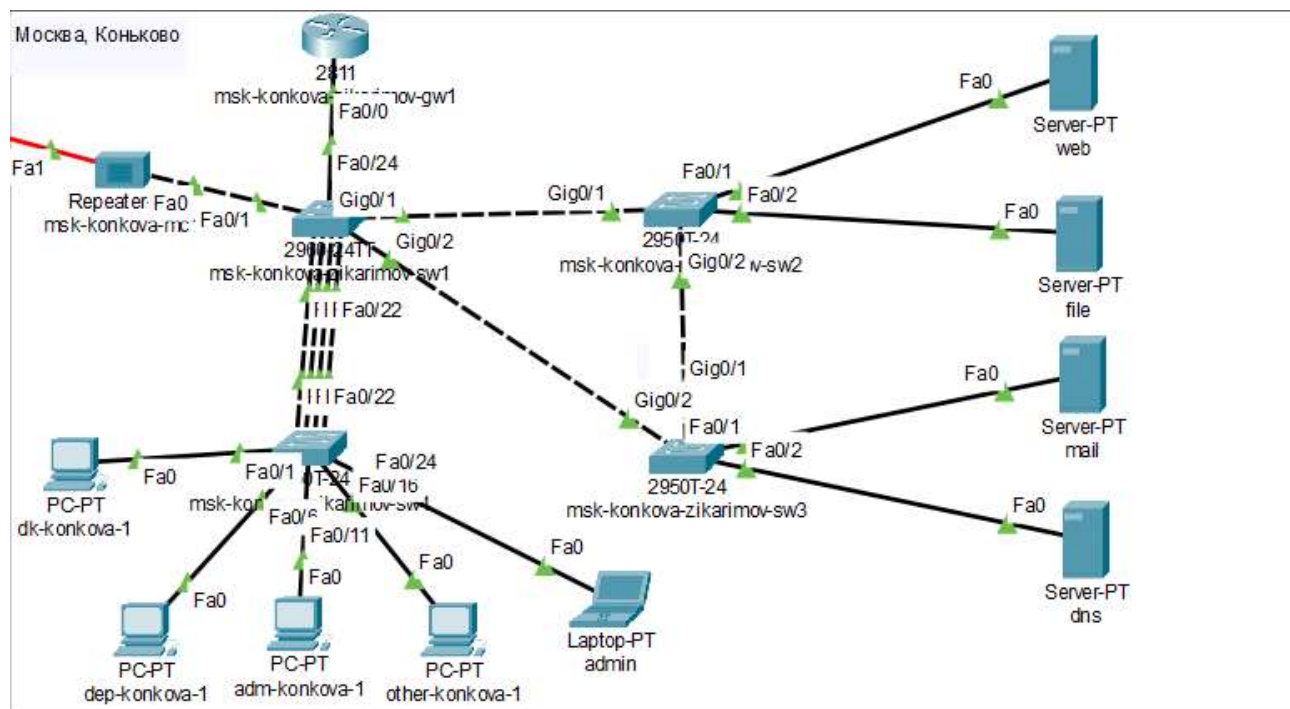
2. Требуется проверить правильность действия установленных правил доступа.

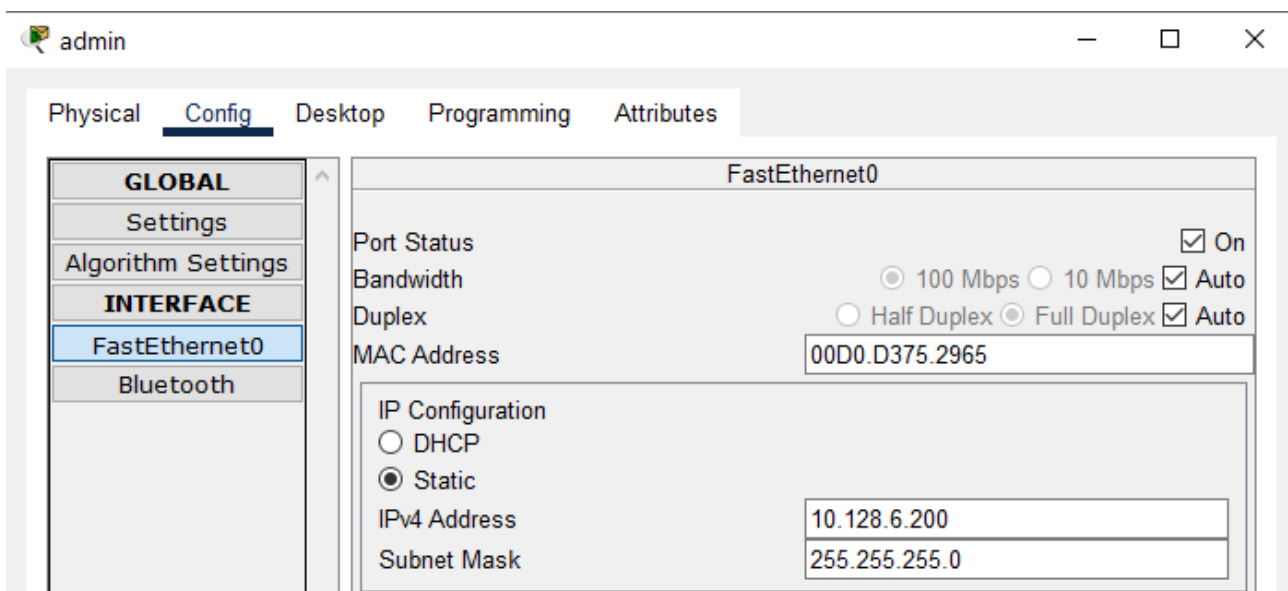
3. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.

4. При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

Последовательность выполнения работы

В рабочей области проекта подключил ноутбук администратора с именем admin к сети к other-donskaya-1 с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоединил ноутбук к порту 24 коммутатора msk-donskaya-sw-4 и присвоил ему статический адрес 10.128.6.200, также указал в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5





1. Настройка доступа к web-серверу по порту tcp 80:

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark web
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp any
host 10.128.0.2 eq 80
```

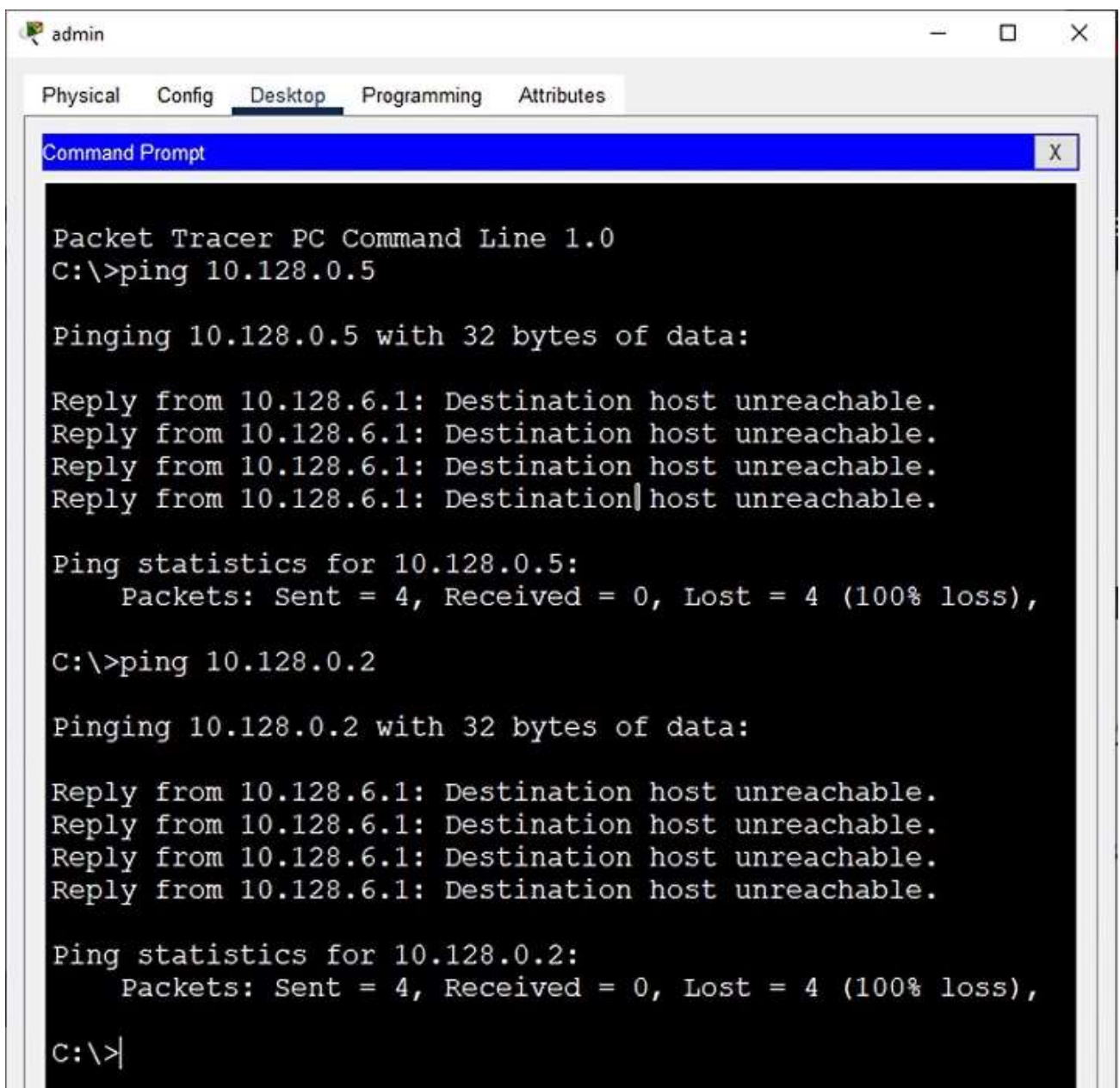
Здесь: создан список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указано (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером; дано разрешение доступа (permit) по протоколу TCP всем (any) пользователям сети (host) на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80.

2. Добавление списка управления доступом к интерфейсу:

```
msk-konkova-zikarimov-gw1(config)#int
msk-konkova-zikarimov-gw1(config)#interface f0/0.3
msk-konkova-zikarimov-gw1(config-subif)#ip ac
msk-konkova-zikarimov-gw1(config-subif)#ip access-group
servers-out out
msk-konkova-zikarimov-gw1(config-subif)#exit
```

Здесь: к интерфейсу f0/0.3 подключается список прав доступа serversout и применяется к исходящему трафику (out). Можно проверить, что доступ к web-

серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера.



The screenshot shows a Packet Tracer PC Command Line window titled "admin". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. Inside the window is a "Command Prompt" window with a blue title bar. The command prompt shows the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

ping демонстрирует недоступность web-сервера как по имени, так и по ip-адресу web-сервера



3. Дополнительный доступ для администратора по протоколам Telnet и FTP:

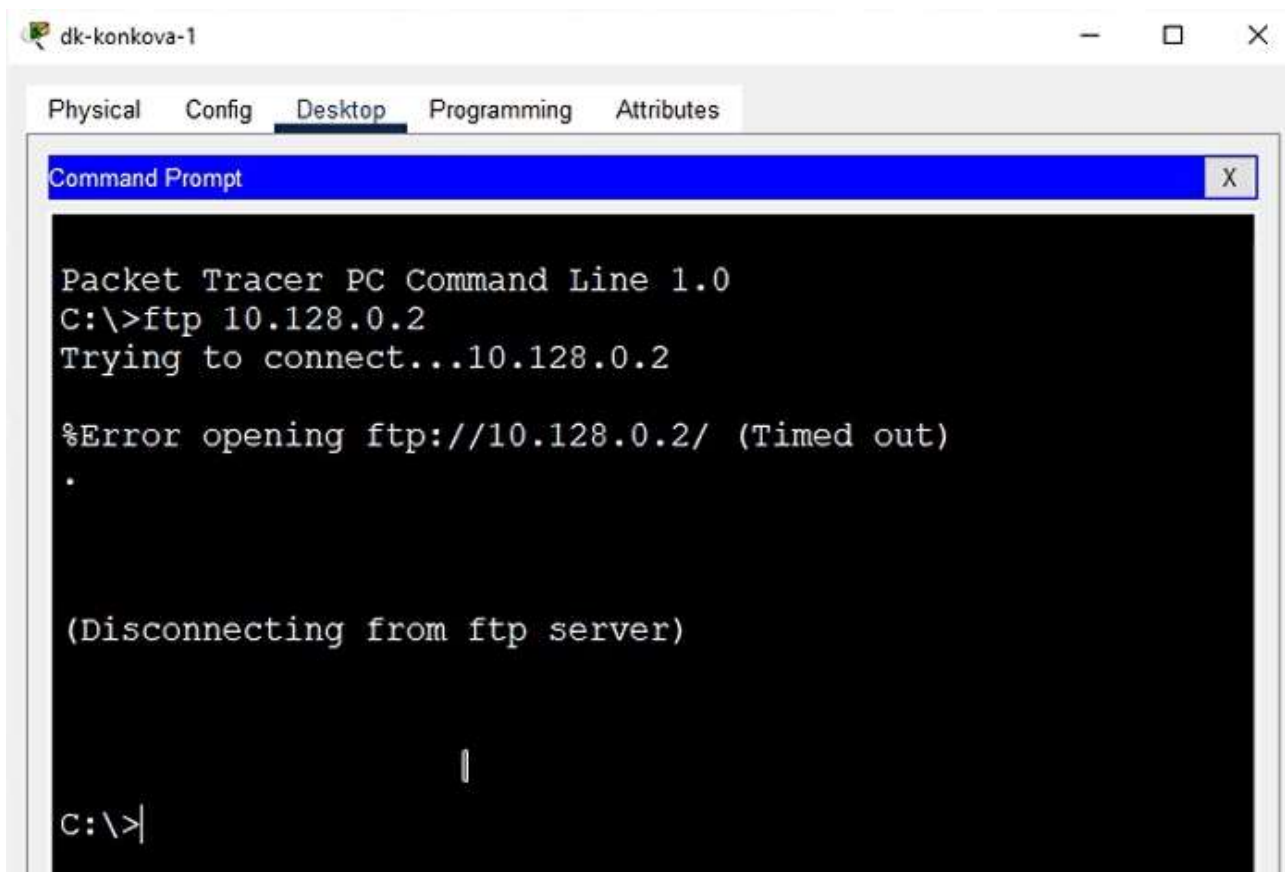
```
msk-konkova-zikarimov-gw1(config)#ip access-list extended servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
host 10.128.6.200 host 10.128.0.2 eq telnet
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
```

Здесь: в список контроля доступа servers-out добавлено правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet. Убедитесь, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введите ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco


```
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2
Connected to 10.128.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>

C:\>
```

Попробуйте провести аналогичную процедуру с другого устройства сети. Убедился в том, что доступ будет запрещён.



The screenshot shows the Packet Tracer interface with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2

%Error opening ftp://10.128.0.2/ (Timed out)
.

(Disconnecting from ftp server)

C:\>
```

4. Настройка доступа к файловому серверу:

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark file
msk-konkova-zikarimov-gw1(config-ext-nacl)#per
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp any
host 10.128.0.3 range 20 ftp
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
```

Здесь: в списке контроля доступа servers-out указано (в качестве комментария-напоминания remark file), что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

5. Настройка доступа к почтовому серверу:

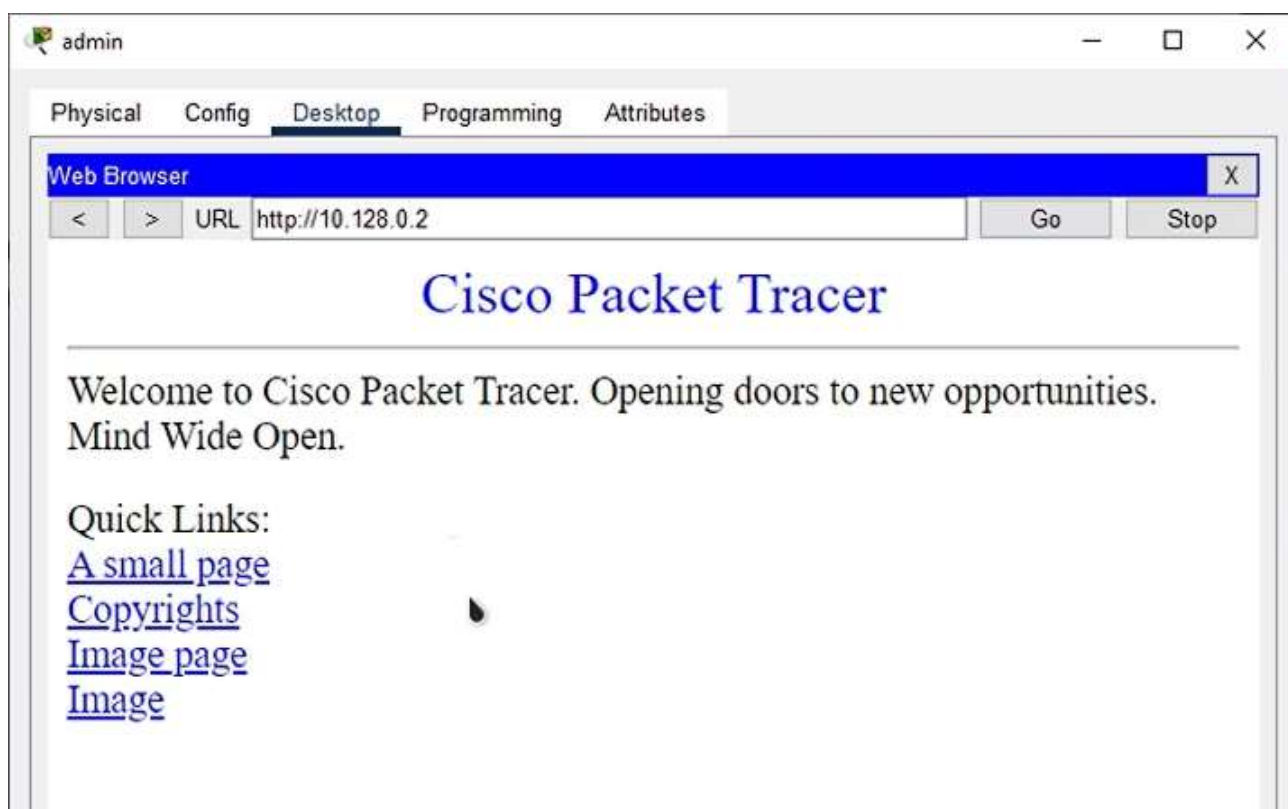
```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark mail
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp any
host 10.128.0.4 eq smtp
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp any
host 10.128.0.4 eq pop3
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
```

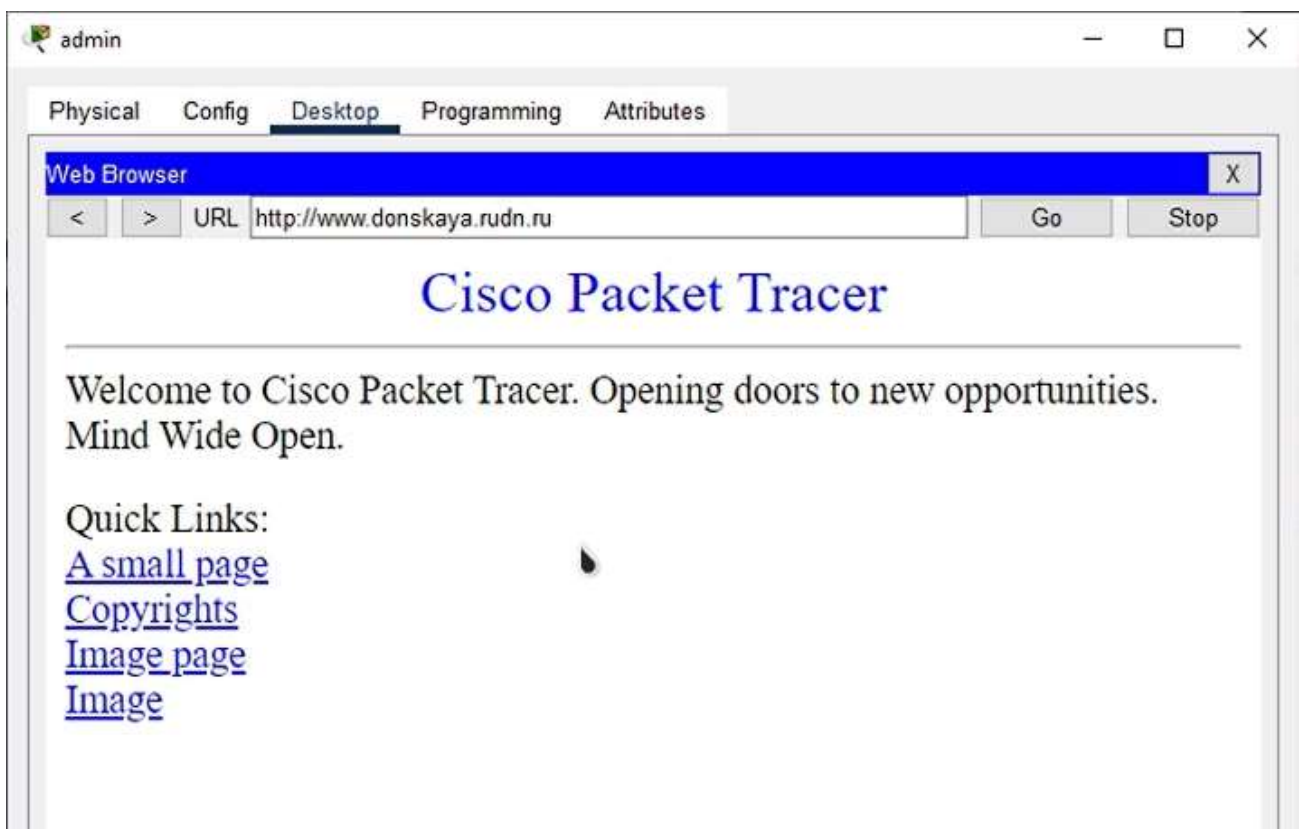
Здесь: в списке контроля доступа servers-out указано (в качестве комментария-напоминания remark mail), что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP.

6. Настройка доступа к DNS-серверу:

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark dns
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit udp
10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
```

Здесь: в списке контроля доступа servers-out указано (в качестве комментария-напоминания remark dns), что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53. Проверьте доступность web-сервера (через браузер) не только по ip-адресу, но и по имени.





Проверил доступность web-сервера (через браузер) не только по ip-адресу, но и по имени.

7. Разрешение icmp-запросов:

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#1 permit icmp
any any
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
```

Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Номера строк правил в списке контроля доступа можно посмотреть с помощью команды.


```

msk-konkova-zikarimov-gw1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#1 permit icmp any any
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
msk-konkova-zikarimov-gw1(config)#exit
msk-konkova-zikarimov-gw1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-konkova-zikarimov-gw1#sh ac
msk-konkova-zikarimov-gw1#sh access-lists
Extended IP access list servers-out
 1 permit icmp any any
10 permit tcp any host 10.128.0.2 eq www (16 match(es))
20 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
30 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
40 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
50 permit tcp any host 10.128.0.3 range 20 ftp
60 permit tcp any host 10.128.0.4 eq smtp
70 permit tcp any host 10.128.0.4 eq pop3
80 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (2 match(es))

msk-konkova-zikarimov-gw1#

```

8. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком):

```

msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
other-in
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark admin
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit ip host
10.128.6.200 any
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
msk-konkova-zikarimov-gw1(config)#int
msk-konkova-zikarimov-gw1(config)#interface f0/0.104
msk-konkova-zikarimov-gw1(config-subif)#ip ac
msk-konkova-zikarimov-gw1(config-subif)#ip access-group
other-in in
msk-konkova-zikarimov-gw1(config-subif)#exit

```

Здесь: в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом

10.128.6.200 на любые действия (any); к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in).

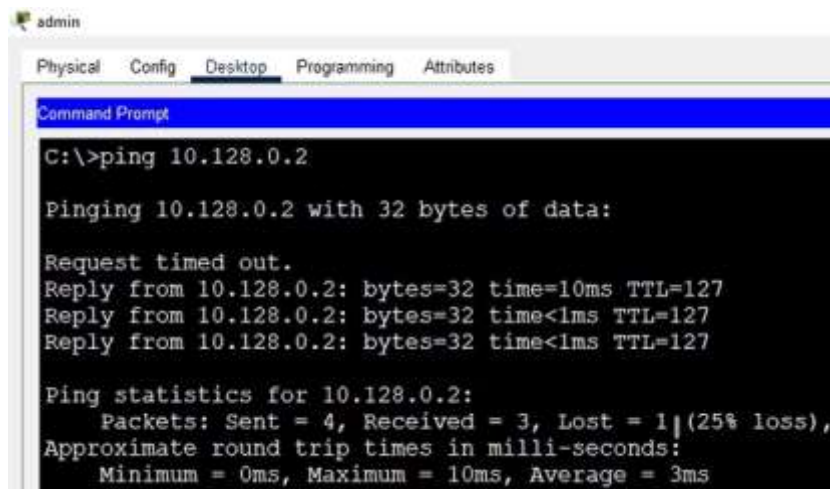
9. Настройка доступа администратора к сети сетевого оборудования:

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list extend
msk-konkova-zikarimov-gw1(config)#ip access-list extended
management-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark admin
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit ip host
10.128.6.200 10.128.1.0 0.0.0.255
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit
msk-konkova-zikarimov-gw1(config)#int
msk-konkova-zikarimov-gw1(config)#interface f0/0.2
msk-konkova-zikarimov-gw1(config-subif)#ip ac
msk-konkova-zikarimov-gw1(config-subif)#ip access-group
management-out out
msk-konkova-zikarimov-gw1(config-subif)#exit
```

Здесь: в списке контроля доступа management-out указано (в качестве комментария-напоминания remark admin), что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключается список прав доступа management-out и применяется к исходящему трафику (out).

Самостоятельная работа

1. Проверьте корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования.



Command Prompt

```
C:\>ping 10.128.0.3
```

```
Pinging 10.128.0.3 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 10.128.0.3: bytes=32 time=12ms TTL=127
```

```
Reply from 10.128.0.3: bytes=32 time=1ms TTL=127
```

```
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.3:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 12ms, Average = 4ms
```

```
C:\>ping 10.128.0.4
```

```
Pinging 10.128.0.4 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.4:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ftp
```


Physical Config Desktop Programming Attributes

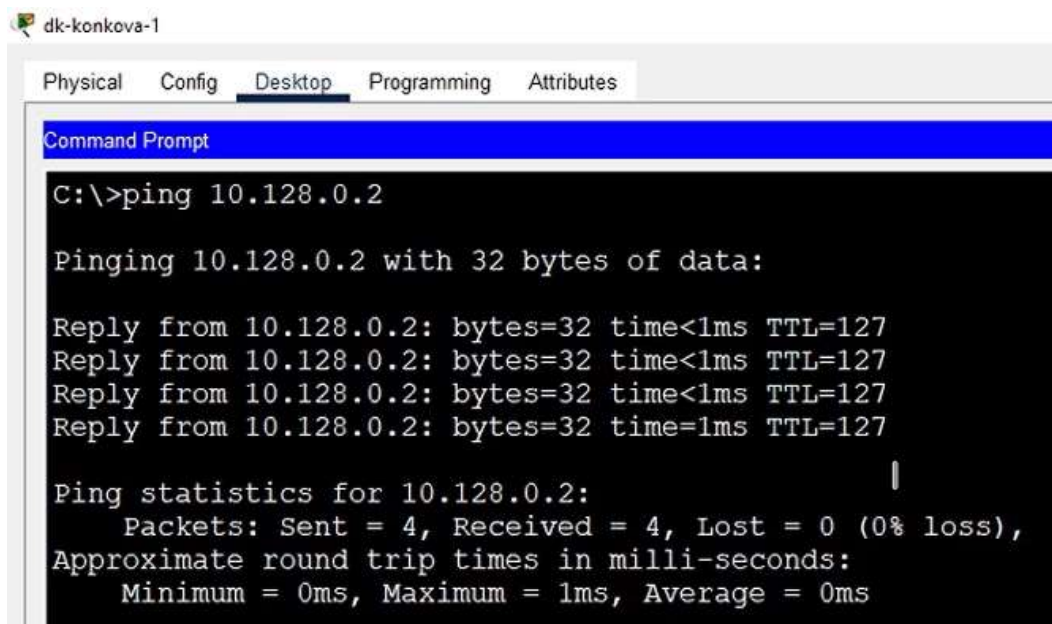
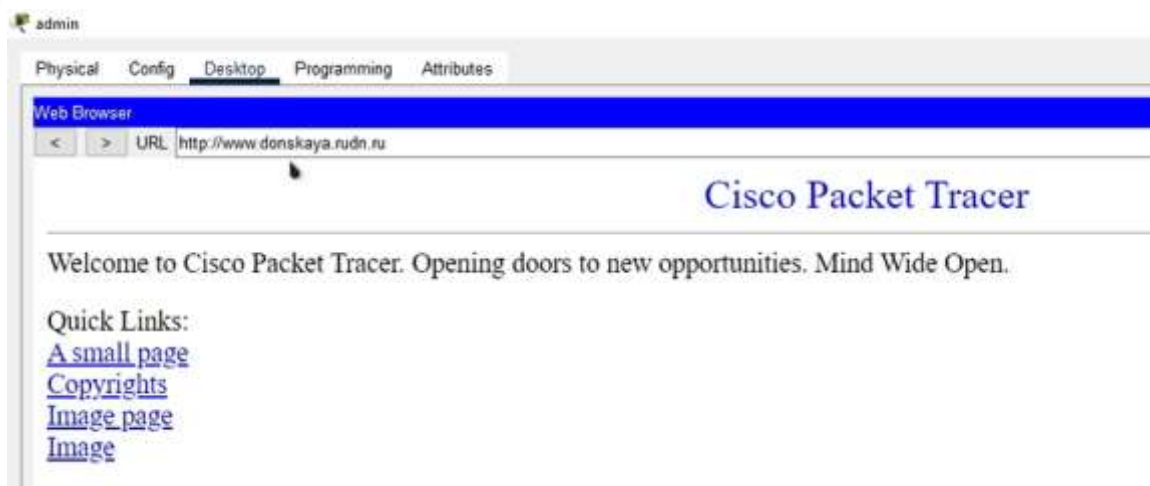
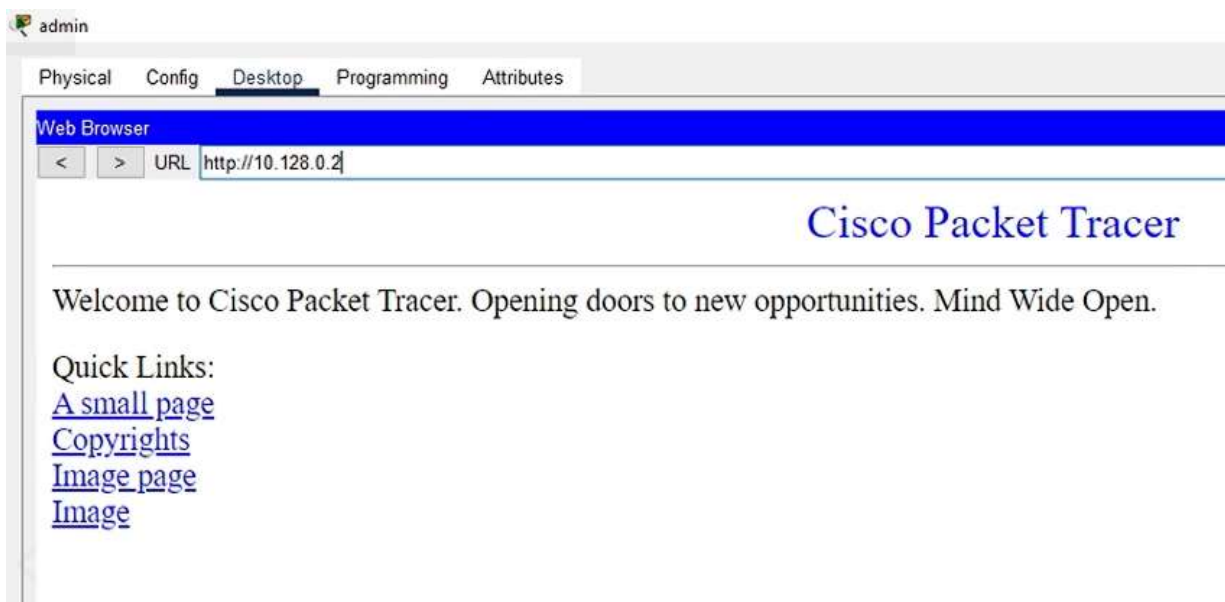
Command Prompt

```
Ping statistics for 10.128.0.4:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ftp 10.128.0.2  
Trying to connect...10.128.0.2  
Connected to 10.128.0.2  
220- Welcome to PT Ftp server  
Username:cisco  
331- Username ok, need password  
Password:  
230- Logged in  
(passive mode On)  
ftp>
```

```
C:\>ftp 10.128.0.3  
Trying to connect...10.128.0.3  
Connected to 10.128.0.3  
220- Welcome to PT Ftp server  
Username:cisco  
331- Username ok, need password  
Password:  
230- Logged in  
(passive mode On)  
ftp>
```

```
C:\>
```

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 10.128.0.3
```

```
Pinging 10.128.0.3 with 32 bytes of data:
```

```
Reply from 10.128.0.3: bytes=32 time=1ms TTL=127
```

```
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.3:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 10.128.0.4
```

```
Pinging 10.128.0.4 with 32 bytes of data:
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.4:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ftp 10.128.0
```

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 10.128.0.4
```

```
Pinging 10.128.0.4 with 32 bytes of data:
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.4:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ftp 10.128.0.3
```

```
Trying to connect...10.128.0.3
```

```
Could not open connection to the host, on port 21: Connect failed
```

```
C:\>ftp 10.128.0.3
```

```
Trying to connect...10.128.0.3
```

```
Connected to 10.128.0.3
```

```
220- Welcome to PT Ftp server
```

```
Username:cisco
```

```
331- Username ok, need password
```

```
Password:
```

```
230- Logged in
```

```
(passive mode On)
```

```
ftp>
```

```
C:\>
```

dk-konkova-1

Physical Config Desktop Programming Attributes

Web Browser

< > URL `http://10.128.0.2`

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:

[A small page](#)

[Copyrights](#)

[Image page](#)

[Image](#)

dk-konkova-1

Physical Config Desktop Programming Attributes

Web Browser

< > URL `http://www.donskaya.rudn.ru`

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:

[A small page](#)

[Copyrights](#)

[Image page](#)

[Image](#)

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 10.128.0.2
```

```
Pinging 10.128.0.2 with 32 bytes of data:
```

```
Reply from 10.128.0.2: bytes=32 time=1ms TTL=127
Reply from 10.128.0.2: bytes=32 time=10ms TTL=127
Reply from 10.128.0.2: bytes=32 time=4ms TTL=127
Reply from 10.128.0.2: bytes=32 time=1ms TTL=127
```

```
Ping statistics for 10.128.0.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

```
C:\>ping 10.128.0.3
```

```
Pinging 10.128.0.3 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 10.128.0.3: bytes=32 time=10ms TTL=127
Reply from 10.128.0.3: bytes=32 time=10ms TTL=127
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.3:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 6ms
```

```
C:\>ping 10.128.0.4
```

Physical Config Desktop Programming Attributes

Command Prompt

```
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 10ms, Average = 6ms
```

```
C:\>ping 10.128.0.4
```

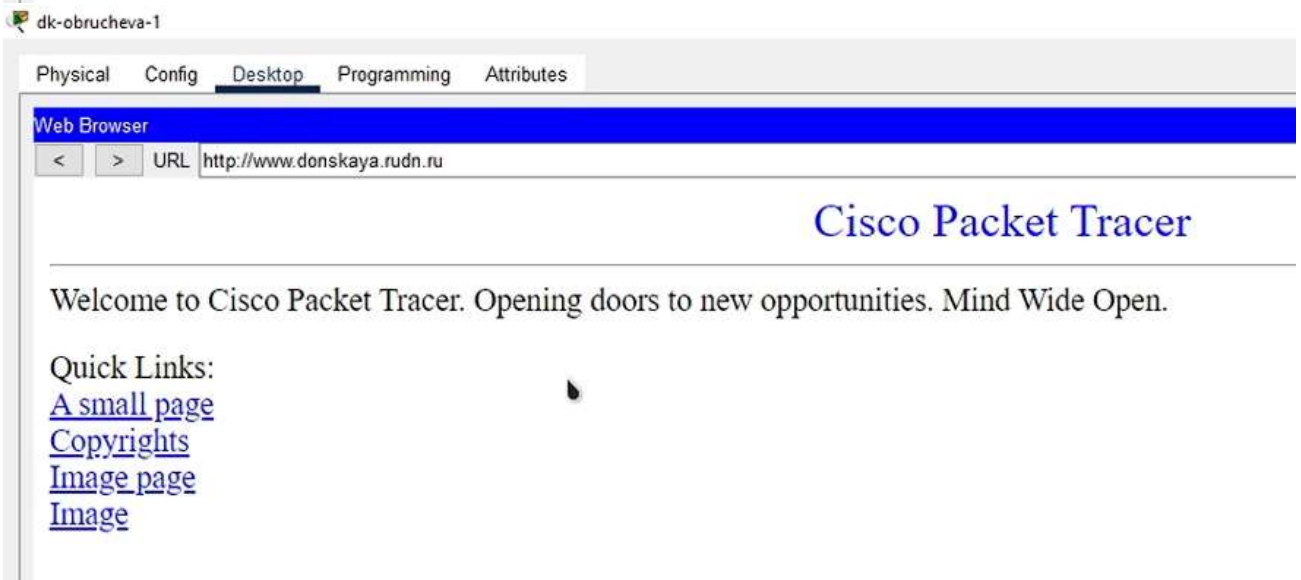
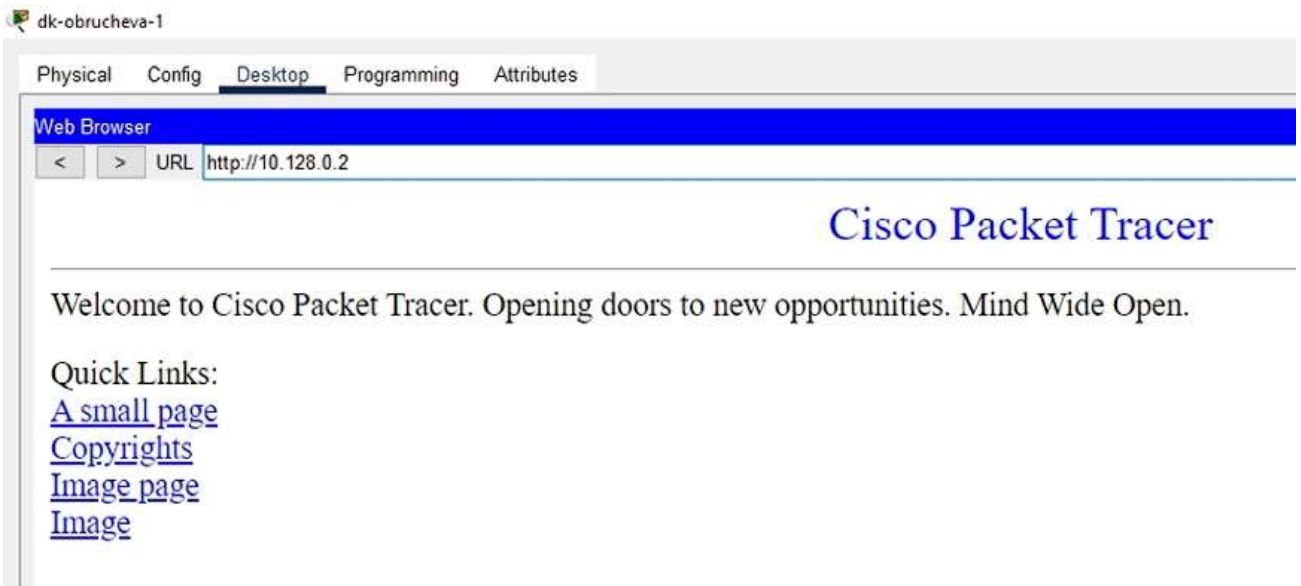
```
Pinging 10.128.0.4 with 32 bytes of data:
```

```
Reply from 10.128.0.4: bytes=32 time=7ms TTL=127  
Reply from 10.128.0.4: bytes=32 time=1ms TTL=127  
Reply from 10.128.0.4: bytes=32 time=1ms TTL=127  
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.128.0.4:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 7ms, Average = 2ms
```

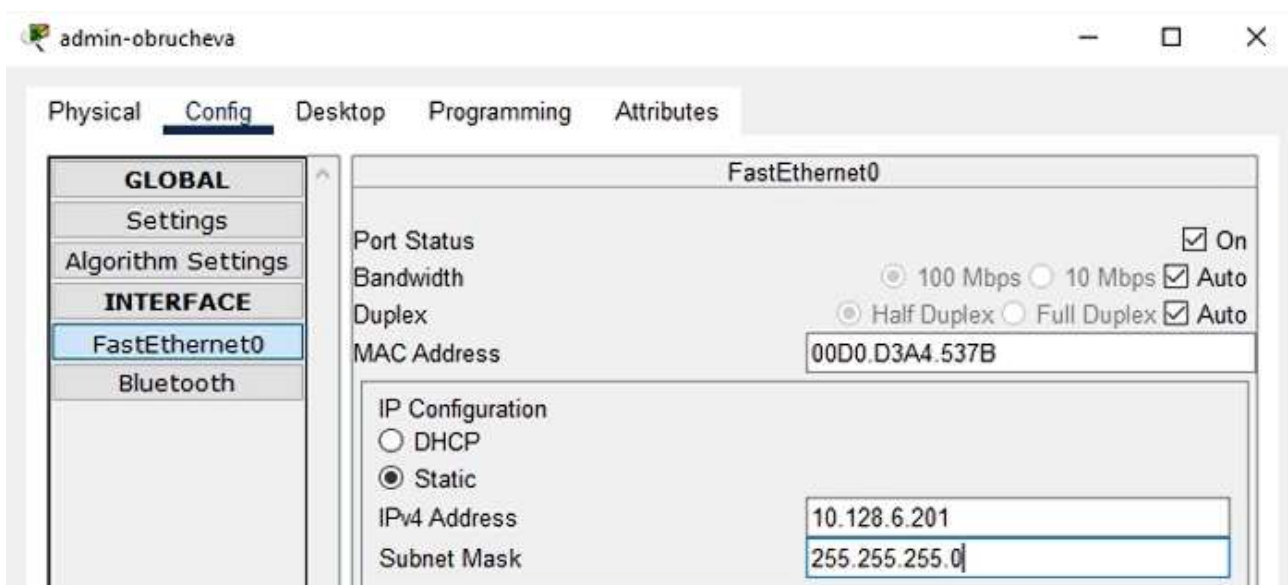
```
C:\>ftp 10.128.0.3  
Trying to connect...10.128.0.3  
Connected to 10.128.0.3  
220- Welcome to PT Ftp server  
Username:cisco  
331- Username ok, need password  
Password:  
230- Logged in  
(passive mode On)  
ftp>
```

```
C:\>
```



2. Разрешите администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.





```
msk-obrucheva-zikarimov-sw1(config)#int f0/23
msk-obrucheva-zikarimov-sw1(config-if)#no sh
msk-obrucheva-zikarimov-sw1(config-if)#no sh
msk-obrucheva-zikarimov-sw1(config-if)#no shutdown
msk-obrucheva-zikarimov-sw1(config-if)#sw
msk-obrucheva-zikarimov-sw1(config-if)#switchport mod
msk-obrucheva-zikarimov-sw1(config-if)#switchport mode ac
msk-obrucheva-zikarimov-sw1(config-if)#switchport mode
access
msk-obrucheva-zikarimov-sw1(config-if)#sw
msk-obrucheva-zikarimov-sw1(config-if)#switchport ac
msk-obrucheva-zikarimov-sw1(config-if)#switchport access
vlan 104
msk-obrucheva-zikarimov-sw1(config-if)#exit
```

```
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
servers-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp host
10.128.6.200 host 10.128.0.2 range 20 ftp
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp host
10.128.6.201 host 10.128.0.2 range 20 ftp
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp host
10.128.6.201 host 10.128.0.2 eq telnet
```



```

msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
other-in
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark admin-
obrucheva
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit ip host
10.128.6.201 any
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
management-out
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark admin-
obrucheva
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit ip host
10.128.6.201 10.128.1.0 0.0.0.255
msk-konkova-zikarimov-gw1(config-ext-nacl)#exit

```

msk-konkova-zikarimov-gw1

Physical Config CLI Attributes

IOS Command Line Interface

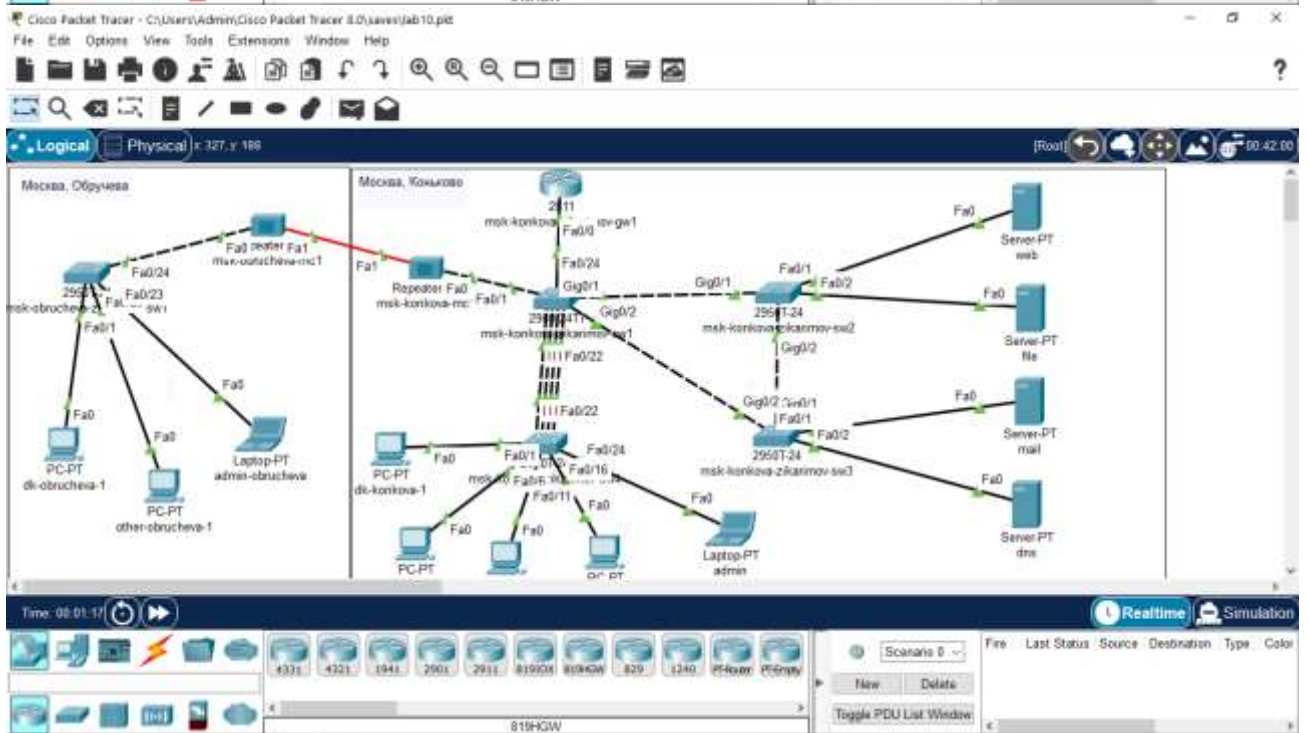
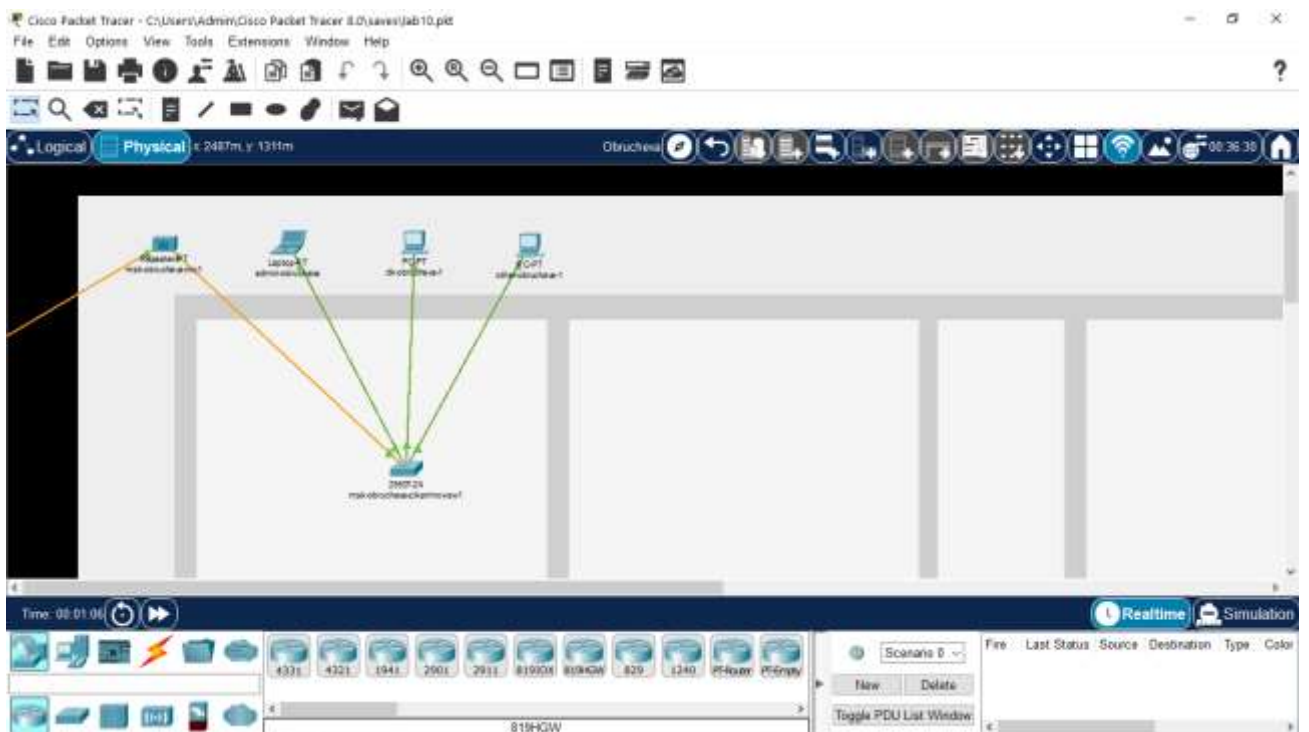
```

network 10.128.0.0 255.255.255.0
default-router 10.128.5.1
dns-server 10.128.0.5
ip dhcp pool other

msk-konkova-zikarimov-gw1#sh ru ac
msk-konkova-zikarimov-gw1#sh ac
msk-konkova-zikarimov-gw1#sh access-lists
Extended IP access list servers-out
  10 permit icmp any any (36 match(es))
  20 permit tcp any host 10.128.0.2 eq www (32 match(es))
  30 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
  40 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (9 match(es))
  50 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
  60 permit tcp any host 10.128.0.3 range 20 ftp (21 match(es))
  70 permit tcp any host 10.128.0.4 eq smtp
  80 permit tcp any host 10.128.0.4 eq pop3
  90 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (6 match(es))
  100 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
  110 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
Extended IP access list other-in
  10 permit ip host 10.128.6.200 any (43 match(es))
  20 permit ip host 10.128.6.201 any
Extended IP access list management-out
  10 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
  20 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255

msk-konkova-zikarimov-gw1#

```



Вывод

Освоил настройку прав доступа пользователей к ресурсам сети.

Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Команда `permit`.

После команды необходимо указать протокол. Он задается в виде номера протокола. Протоколы IP, TCP, UDP, AH, ESP, ICMP, EIGRP, GRE, IGMP, IPINIP, NOS, OSPF, PCP, PIM могут быть заданы собственной аббревиатурой.

2. Как задать действие правила сразу для нескольких портов?

Команда `range` + номера портов

Указывается диапазон портов или один порт [0 ... 65535].

Используется в связке с параметром `operator`. При использовании `operator=range` после него следуют два числа - границы диапазона портов.

3. Как узнать номер правила в списке прав доступа?

`show access-lists`

4. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Добавление новых строк в определенную позицию:

`ip access-list standard LIST1`

номер_строки `permit` ...

Удаление строк:

`ip access-list standard LIST103`

по номер_строки

Перенумерация строк:

`ip access list-resequence LIST 103 10 50`

