

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10

Настройка списков управления доступом (ACL)

дисциплина: Администрирование локальных сетей

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

МОСКВА

2022 г.

Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

Выполнение работы

1. В рабочей области проекта подключите ноутбук администратора с именем admin к сети к other-donskaya-1 с тем (Рис. 1), чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоедините ноутбук к порту 24 коммутатора msk-donskaya-sw-4 и присвойте ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (Рис. 2).

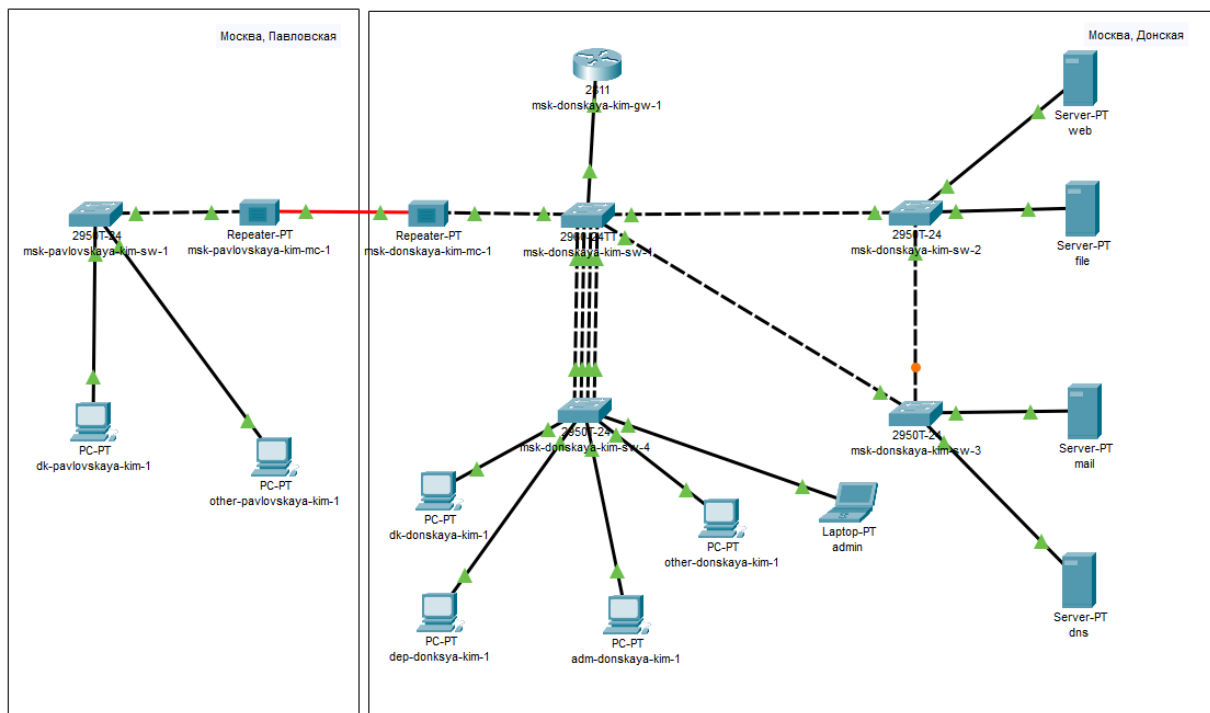


Рисунок 1

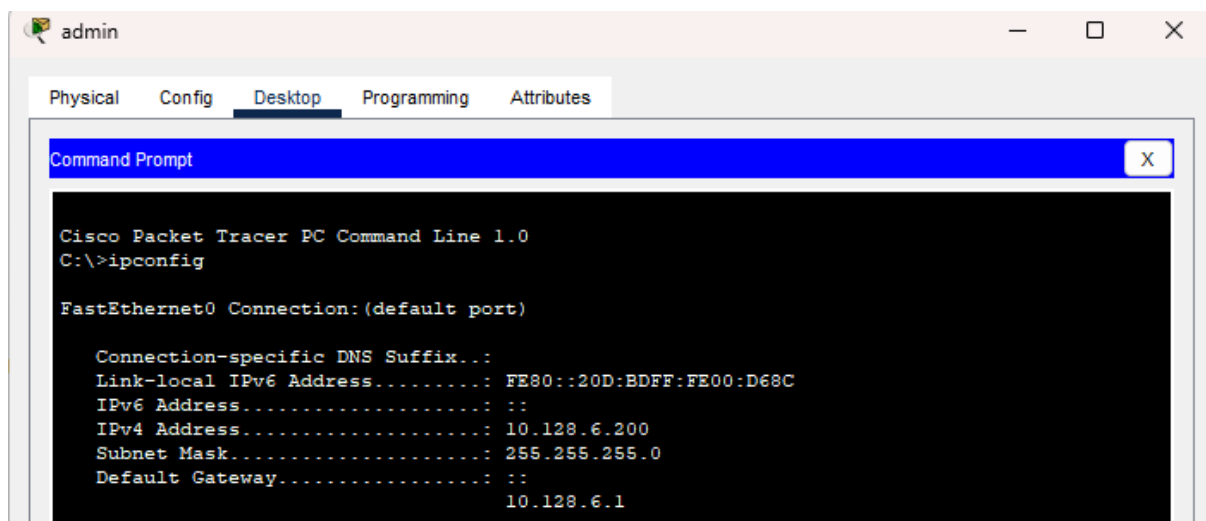


Рисунок 2

2. Настройка доступа к web-серверу по порту tcp 80 (Рис. 3):

```
msk-donskaya-kim-gw-1>en
Password:
msk-donskaya-kim-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark web
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
```

Рисунок 3

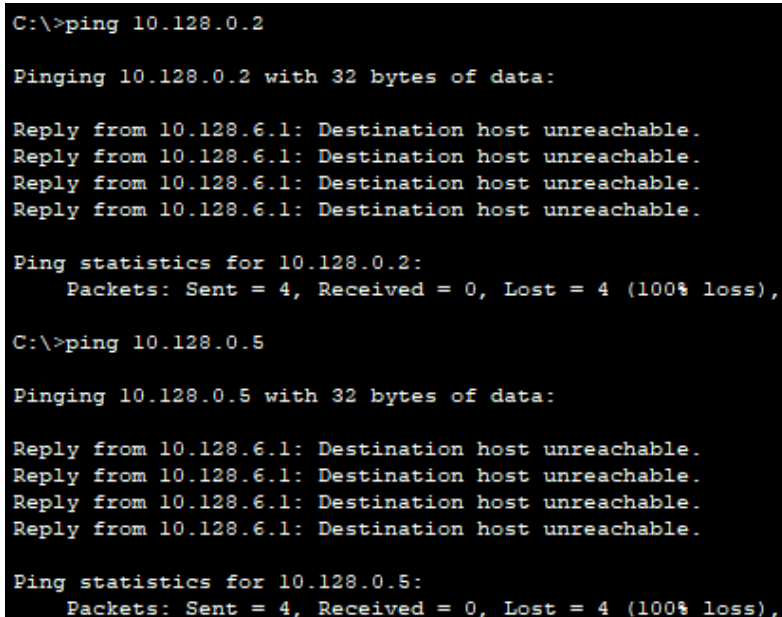
3. Добавление списка управления доступом к интерфейсу (Рис. 4):

```
msk-donskaya-kim-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#interface f0/0.3
msk-donskaya-kim-gw-1(config-subif)#ip access-group servers-out out
```

Рисунок 4

Здесь: к интерфейсу f0/0.3 подключается список прав доступа servers-out 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 (Рис. 5-6).



```
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 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),
```

Рисунок 5

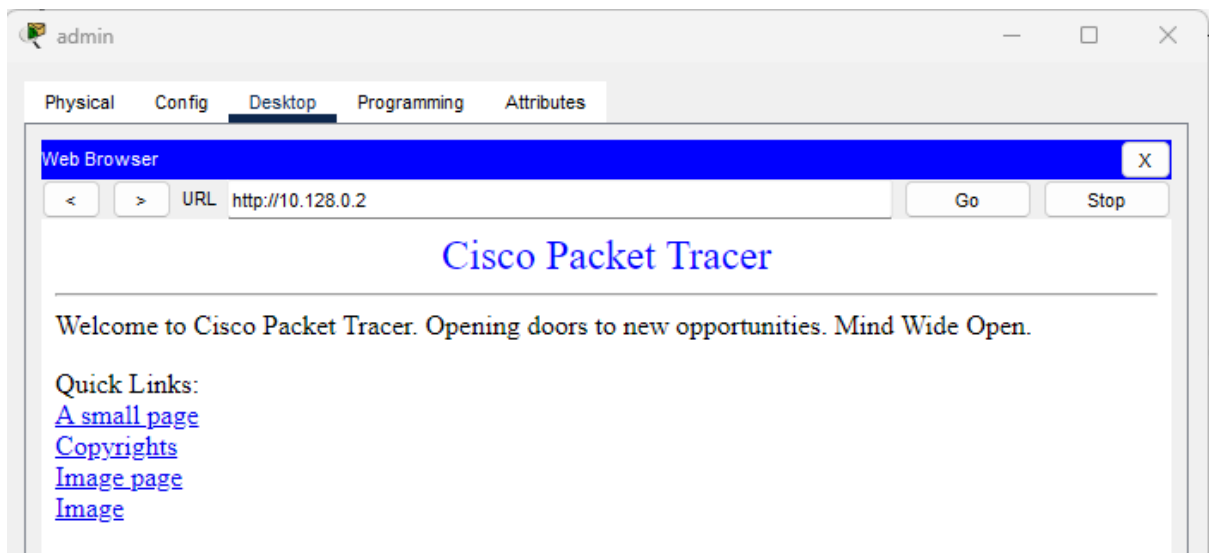


Рисунок 6

4. Дополнительный доступ для администратора по протоколам Telnet и FTP (Рис. 7):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
```

Рисунок 7

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 (Рис. 8).

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

Рисунок 8

Попробуйте провести аналогичную процедуру с другого устройства сети (dk-donskaya-kim-1). Убедитесь, что доступ будет запрещён (Рис. 9).

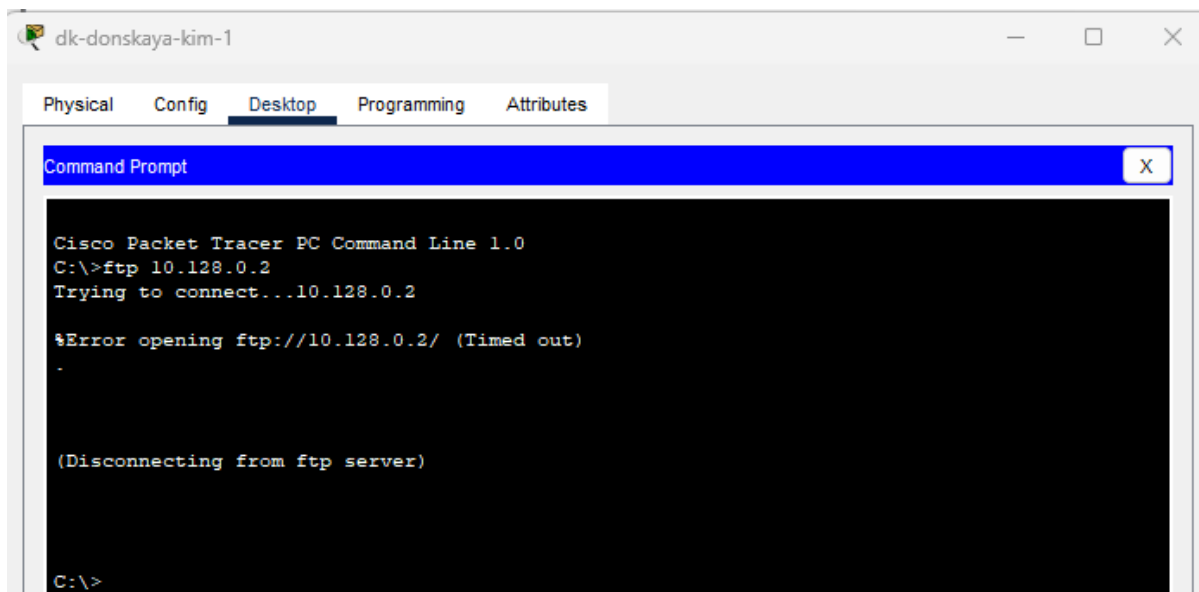


Рисунок 9

5. Настройка доступа к файловому серверу (рис. 10):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark file
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
```

Рисунок 10

6. Настройка доступа к почтовому серверу (рис. 11):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark mail
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
```

Рисунок 11

7. Настройка доступа к DNS-серверу (рис. 12):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark dns
msk-donskaya-kim-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
```

Рисунок 12

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 (рис. 13-14).

```
C:\>ping www.donskaya.rudn.ru

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:\>
```

Рисунок 13

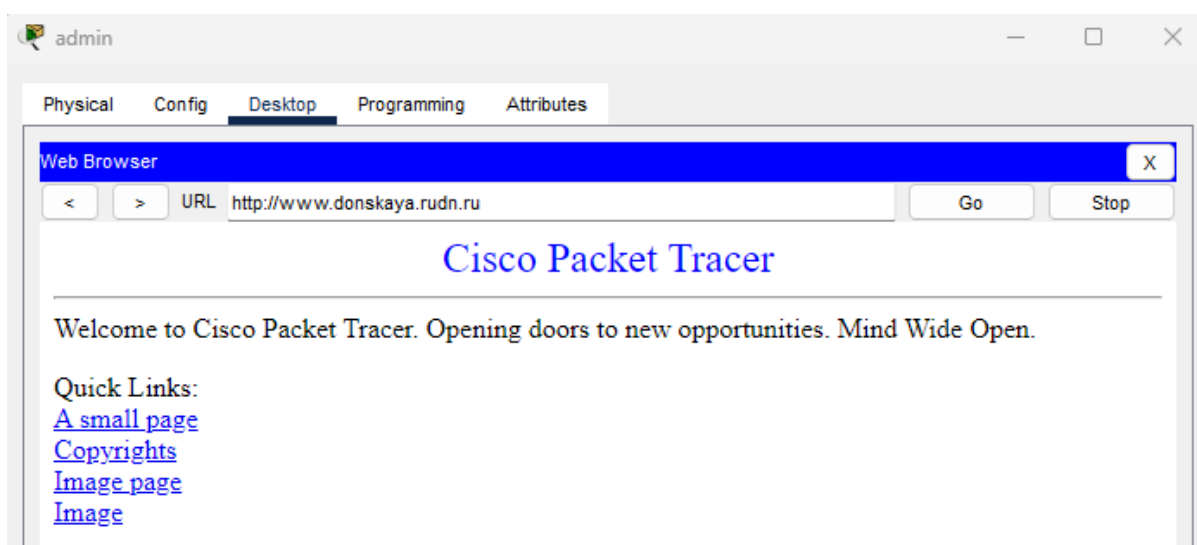


Рисунок 14

8. Разрешение icmp-запросов:

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#1 permit icmp any any
```

Рисунок 15

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 (рис. 16):

```
msk-donskaya-kim-gw-1#show access -lists
```

```
msk-donskaya-kim-gw-1#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 (10 match(es))
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
30 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
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))
```

Рисунок 16

9. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-kim-gw-1 является входящим трафиком) (рис. 17):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended other-in
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.104
msk-donskaya-kim-gw-1(config-subif)#ip access-group other-in in
```

Рисунок 17

10. Настройка доступа администратора к сети сетевого оборудования (рис. 18):

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended management-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.2
msk-donskaya-kim-gw-1(config-subif)#ip access-group management-out out
```

Рисунок 18

11. Схемы L1, таблицы IP и VLAN:

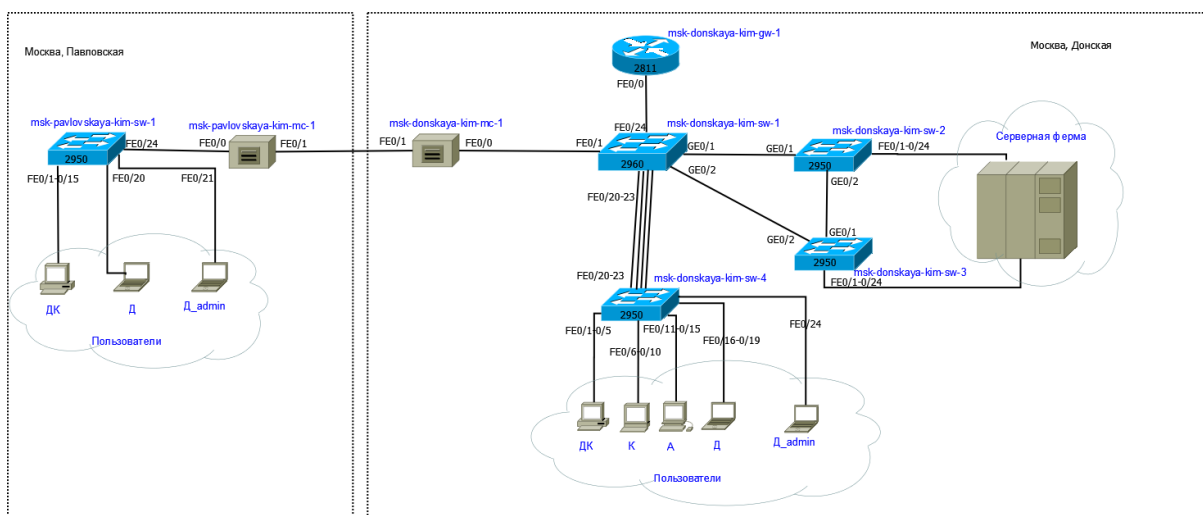


Рисунок 19: Layer 1

Таблица IP

IP-адреса	Примечание	VLAN
10.128.0.0/16	Вся сеть	
10.128.0.0/24	Серверная ферма	3
10.128.0.1	Шлюз	
10.128.0.2	Web	
10.128.0.3	File	
10.128.0.4	Mail	
10.128.0.5	Dns	
10.128.0.6-10.128.0.254	Зарезервировано	
10.128.1.0/24	Управление	2
10.128.1.1	Шлюз	
10.128.1.2	msk-donskaya-kim-sw-1	
10.128.1.3	msk-donskaya-kim-sw-2	
10.128.1.4	msk-donskaya-kim-sw-3	
10.128.1.5	msk-donskaya-kim-sw-4	
10.128.1.6	msk-pavlovskaya-kim-sw-1	
10.128.1.7-10.128.1.254	Зарезервировано	
10.128.2.0/24	Сеть Point-to-Point	
10.128.2.1	Шлюз	
10.128.2.2-10.128.2.254	Зарезервировано	
10.128.3.0/24	Дисплейные классы (ДК)	101
10.128.3.1	Шлюз	
10.128.3.2-10.128.3.254	Пул для пользователей	
10.128.4.0/24	Кафедры (К)	102
10.128.4.1	Шлюз	
10.128.4.2-10.128.4.254	Пул для пользователей	
10.128.5.0/24	Администрация (А)	103
10.128.5.1	Шлюз	
10.128.5.2-10.128.5.254	Пул для пользователей	
10.128.6.0/24	Другие пользователи (Д)	104
10.128.6.1	Шлюз	
10.128.6.2-10.128.6.199	Пул для пользователей	
10.128.6.200	admin-donskaya-kim-1	
10.128.6.201	admin-pavlovskaya-kim-1	

Таблица VLAN

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4-100		Зарезервировано

101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей
104	admin	

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.

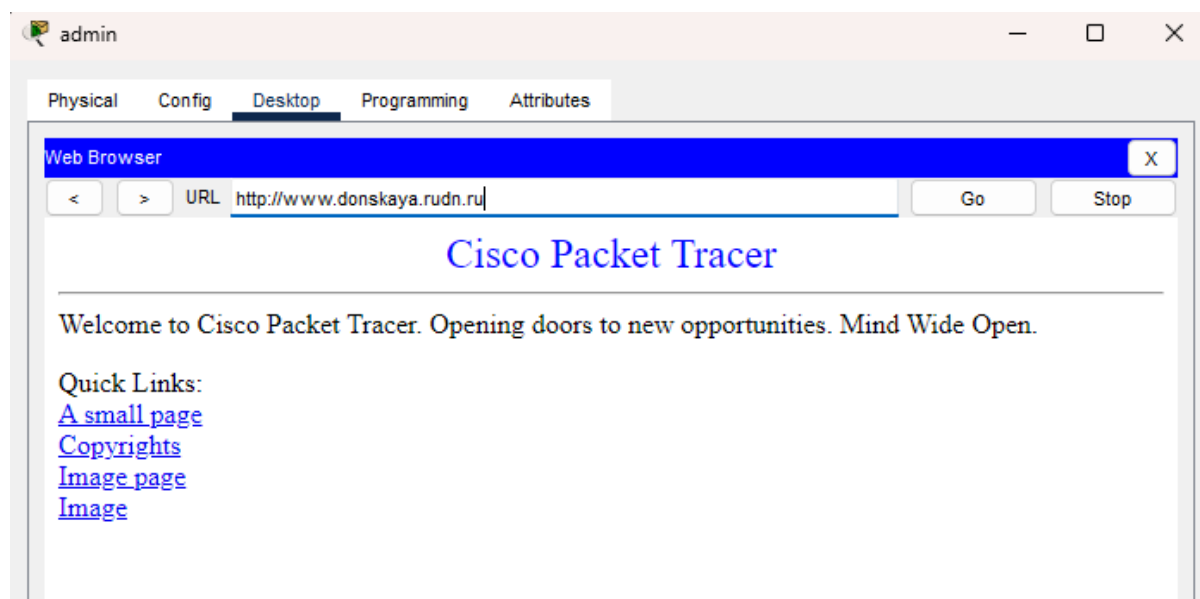


Рисунок 20

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

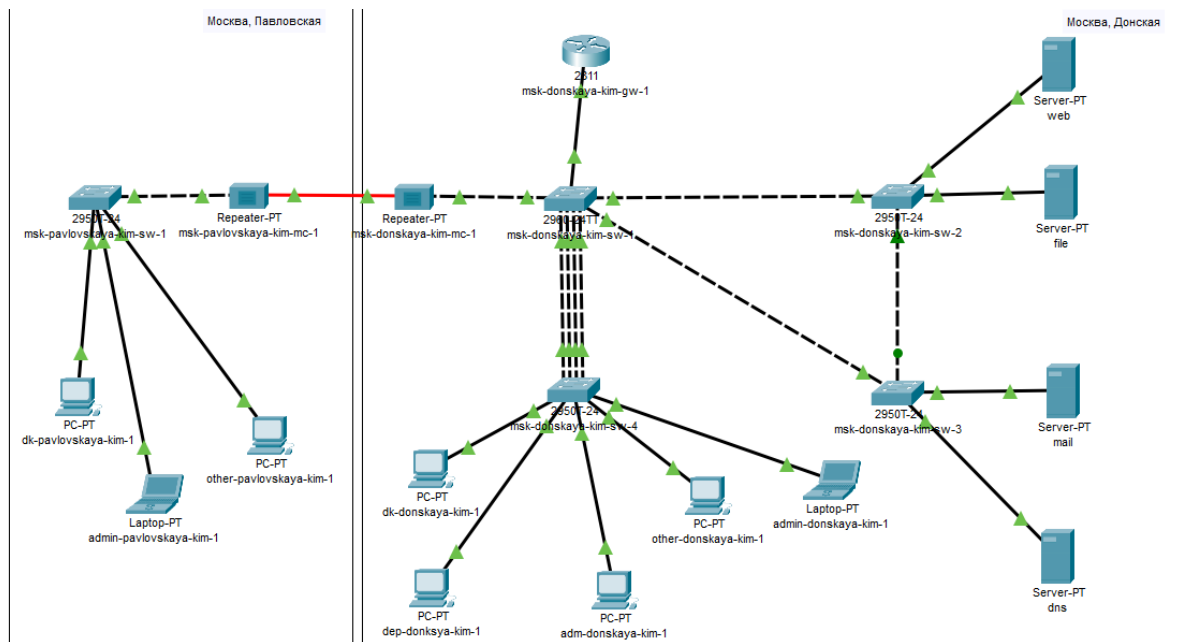


Рисунок 21

```
msk-donskaya-kim-gw-1>en
Password:
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#ip access-list extended other-in
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.104
msk-donskaya-kim-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-kim-gw-1(config-subif)#exit
msk-donskaya-kim-gw-1(config)#ip access-list extended management-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.2
msk-donskaya-kim-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-kim-gw-1(config-subif)#^Z
msk-donskaya-kim-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-kim-gw-1#wr m
```

Рисунок 22

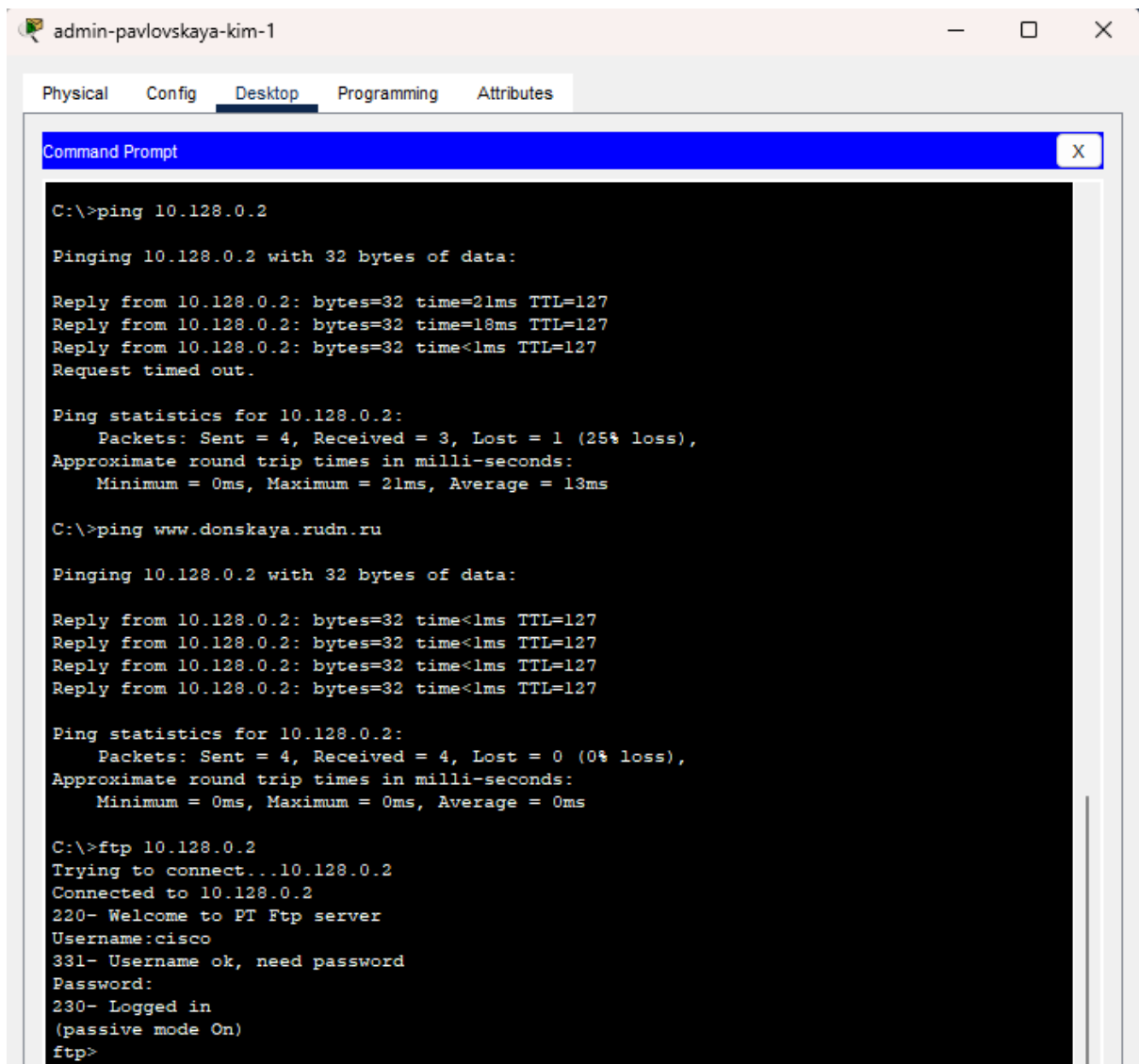


Рисунок 23

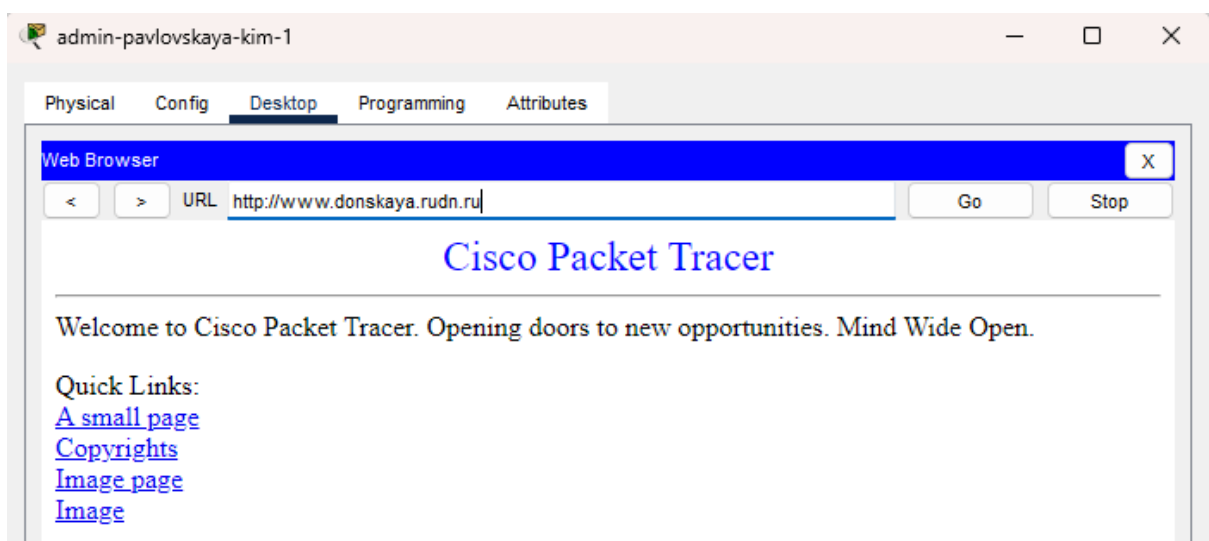


Рисунок 24

Конфигурации оборудования

- **msk-donskaya-kim-gw-1**

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname msk-donskaya-kim-gw-1

!

!

!

enable secret 5 \$1\$mERr\$hx5rVt7rPNoS4wqbXKX7m0

!

!

ip dhcp excluded-address 10.128.3.1 10.128.3.29

ip dhcp excluded-address 10.128.3.200 10.128.3.254

ip dhcp excluded-address 10.128.4.1 10.128.4.29

ip dhcp excluded-address 10.128.4.200 10.128.4.254

ip dhcp excluded-address 10.128.5.1 10.128.5.29

ip dhcp excluded-address 10.128.5.200 10.128.5.254

ip dhcp excluded-address 10.128.6.1 10.128.6.29

ip dhcp excluded-address 10.128.6.200 10.128.6.254

!

ip dhcp pool dk

network 10.128.3.0 255.255.255.0

default-router 10.128.3.1

dns-server 10.128.0.5

ip dhcp pool departments

network 10.128.4.0 255.255.255.0

default-router 10.128.4.1

dns-server 10.128.0.5

ip dhcp pool adm

network 10.128.5.0 255.255.255.0

default-router 10.128.5.1

```
dns-server 10.128.0.5
ip dhcp pool other
network 10.128.6.0 255.255.255.0
default-router 10.128.6.1
dns-server 10.128.0.5
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
license udi pid CISCO2811/K9 sn FTX1017LG55-
!
!
!
!
!
!
!
!
!
!
ip domain-name dons kaya.rudn.edu
ip name-server 10.128.0.5
!
!
spanning-tree mode pvst
!
!
!
```

!

!

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

!

interface FastEthernet0/0.2

description management

encapsulation dot1Q 2

ip address 10.128.1.1 255.255.255.0

ip access-group management-out out

!

interface FastEthernet0/0.3

description servers

encapsulation dot1Q 3

ip address 10.128.0.1 255.255.255.0

ip access-group servers-out out

!

interface FastEthernet0/0.101

description dk

encapsulation dot1Q 101

ip address 10.128.3.1 255.255.255.0

!

interface FastEthernet0/0.102

description departments

encapsulation dot1Q 102

ip address 10.128.4.1 255.255.255.0

!

interface FastEthernet0/0.103

description adm

encapsulation dot1Q 103

ip address 10.128.5.1 255.255.255.0

```
!  
interface FastEthernet0/0.104  
  description other  
  encapsulation dot1Q 104  
  ip address 10.128.6.1 255.255.255.0  
  ip access-group other-in in  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
ip access-list extended servers-out  
  remark web  
  permit icmp any any  
  permit tcp any host 10.128.0.2 eq www  
  permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp  
  permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet  
  remark file  
  permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445  
  permit tcp any host 10.128.0.3 range 20 ftp  
  remark mail  
  permit tcp any host 10.128.0.4 eq smtp  
  permit tcp any host 10.128.0.4 eq pop3
```

```
remark dns
permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain
ip access-list extended other-in
remark admin
permit ip host 10.128.6.200 any
ip access-list extended management-out
remark admin
permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
!
!
!
!
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
transport input ssh
!
!
!
end
```

Ответы на контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Использовать команду permit.

2. Как задать действие правила сразу для нескольких портов?

Задать в команде диапазон портов с помощью range.

3. Как узнать номер правила в списке прав доступа?

Команда show access-list

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

Команда `ip access-list resequence`.

Вывод

Освоила настройку прав доступа пользователей к ресурсам сети.