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: Саргсян Арам Грачьяевич

Группа: НПИбд 02-20

МОСКВА

2023 г.

ЦЕЛЬ РАБОТЫ

Освоить настройку прав доступа пользователей к ресурсам сети.

ХОД РАБОТЫ

1. В рабочей области проекта подключил ноутбук администратора с именем admin к сети к other-donskaya-1, присвоил ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5, переместил его поближе в физтческой области (Рис. 1-3).

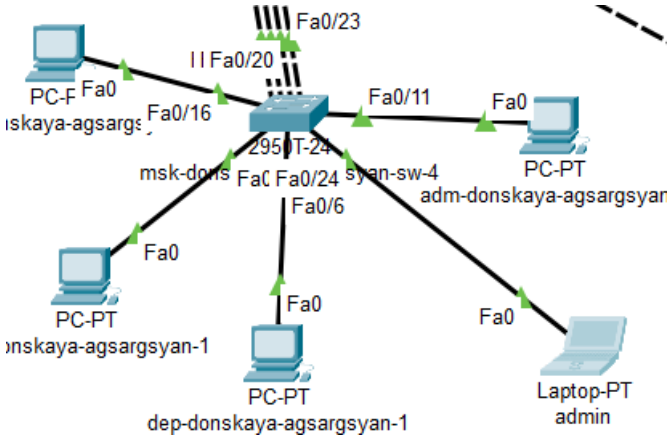

Рис. 1

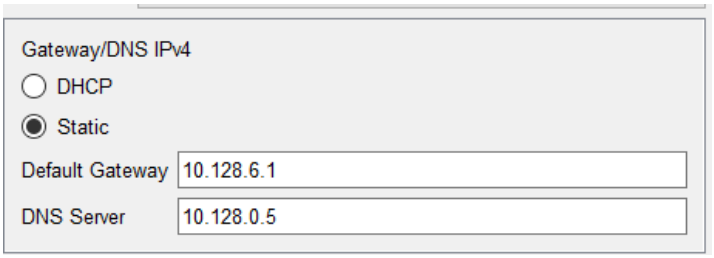

Рис. 2

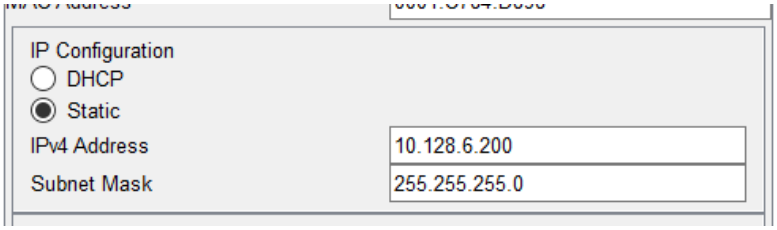

Рис. 3

2. Настроил доступ к web-серверу по порту tcp 80 (Рис. 4).

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

Рис. 4

3. Добавил список управления доступом к интерфейсу (Рис. 5).

```
msk-donskaya-agsargsyan-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#int f0/0.3
msk-donskaya-agsargsyan-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-agsargsyan-gw-1(config-subif)#exit
msk-donskaya-agsargsyan-gw-1(config)#exit
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 5

4. Дополнительно настроил доступ для администратора по протоколам Telnet и FTP (Рис. 6).

```
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended servers-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 6

5. Проверил доступ админа сети other к ДНС по протоколу ftp, разрешение есть только у администратора сети (Рис. 7).

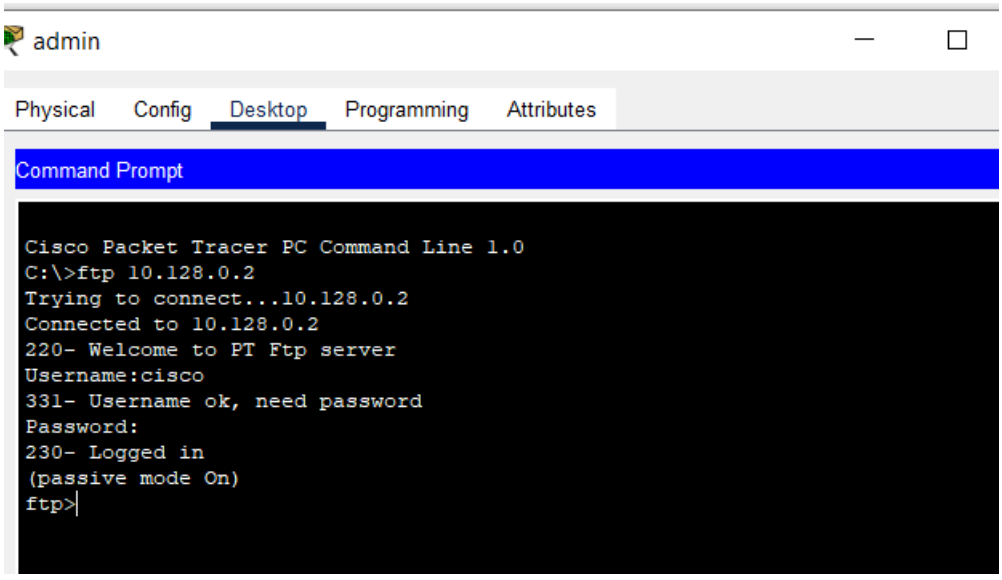

Рис. 7

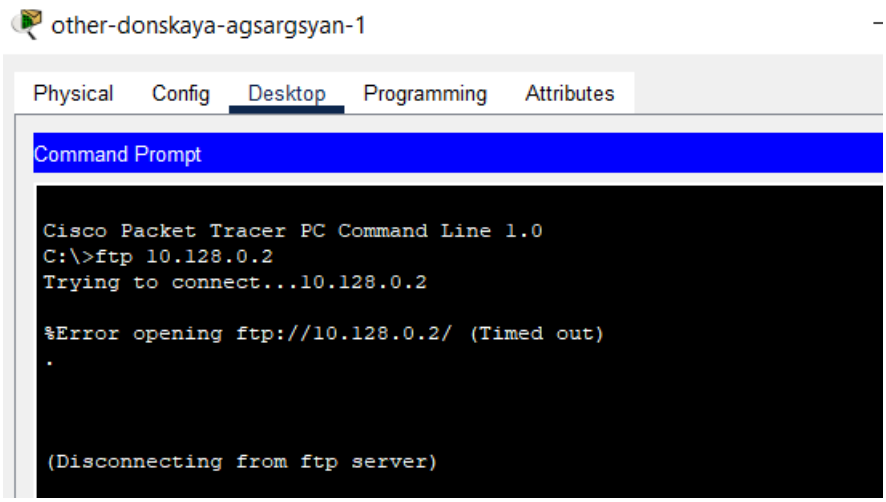

Рис. 8

6. Настроил доступ к файловому серверу (Рис. 9).

```
[OK]
msk-donskaya-agsargsyan-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended servers-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#remark file
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#exit
msk-donskaya-agsargsyan-gw-1(config)#exit
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 9

7. Настроил доступа к почтовому серверу (Рис. 10).

```
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended servers-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#remark mail
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 10

8. Настроил доступ к DNS-серверу (Рис. 11).

```
msk-donskaya-agsargsyan-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended servers-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#remark dns
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#exit
msk-donskaya-agsargsyan-gw-1(config)#exit
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 11

9. Разрешаил icmp-запросы (Рис. 12).

```
msk-donskaya-agsargsyan-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended servers-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#show access-lists
                                              ^
% Invalid input detected at '^' marker.

msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#exit
msk-donskaya-agsargsyan-gw-1(config)#exit
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#show access-lists
Extended IP access list servers-out
    1 permit icmp any any
    10 permit tcp any host 10.128.0.2 eq www
    20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (8 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

msk-donskaya-agsargsyan-gw-1#
```

Рис. 12

10. Настроил доступ для сети Other (Рис. 13).

```
%SYS-5-CONFIG_I: Configured from console by console

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

Рис. 13

11. Настроил доступ администратора к сети сетевого оборудования (Рис. 14).

```
msk-donskaya-agsargsyan-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-agsargsyan-gw-1(config)#ip access-list extended management-out
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#remark admin
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#eexit
                                              ^
% Invalid input detected at '^' marker.

msk-donskaya-agsargsyan-gw-1(config-ext-nacl)#exit
msk-donskaya-agsargsyan-gw-1(config)#f0/0.2
                                    ^
% Invalid input detected at '^' marker.

msk-donskaya-agsargsyan-gw-1(config)#int f0/0.2
msk-donskaya-agsargsyan-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-agsargsyan-gw-1(config-subif)#
msk-donskaya-agsargsyan-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-agsargsyan-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 14

12. Проверил корректность установленных правил (Рис. 15-16).

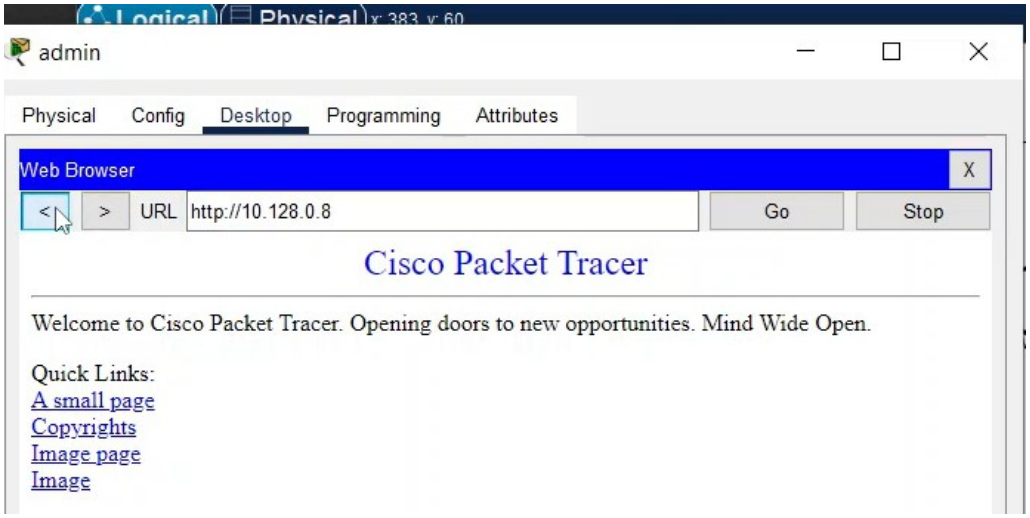

Рис. 15

Рис. 16

13. Настроил права доступа для администратора сети Павловской (Рис. 17)

```
Password:

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

msk-donskaya-agsargsyan-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-agsargsyan-gw-1#
```

Рис. 17

14. Обновил схемы L1, L2 и таблицу ip адресов (Рис. 18-22).

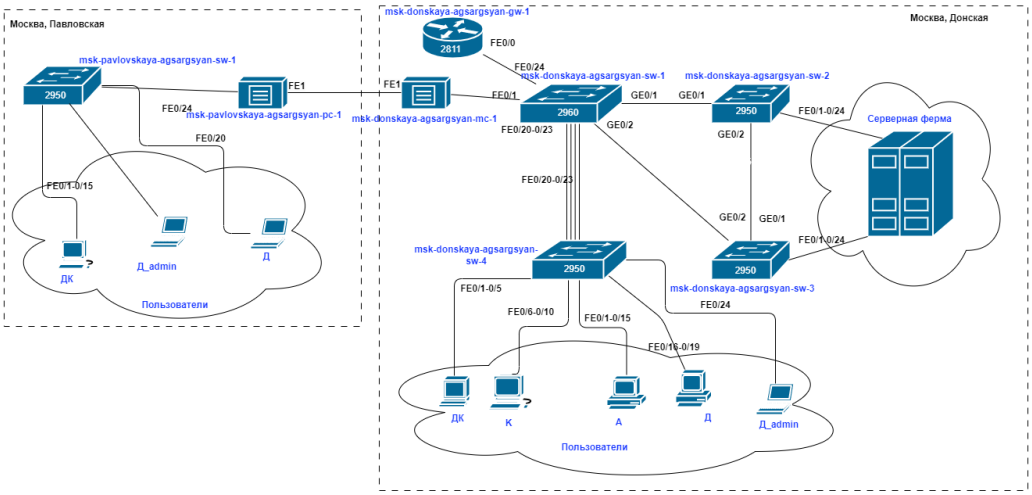

Рис. 18

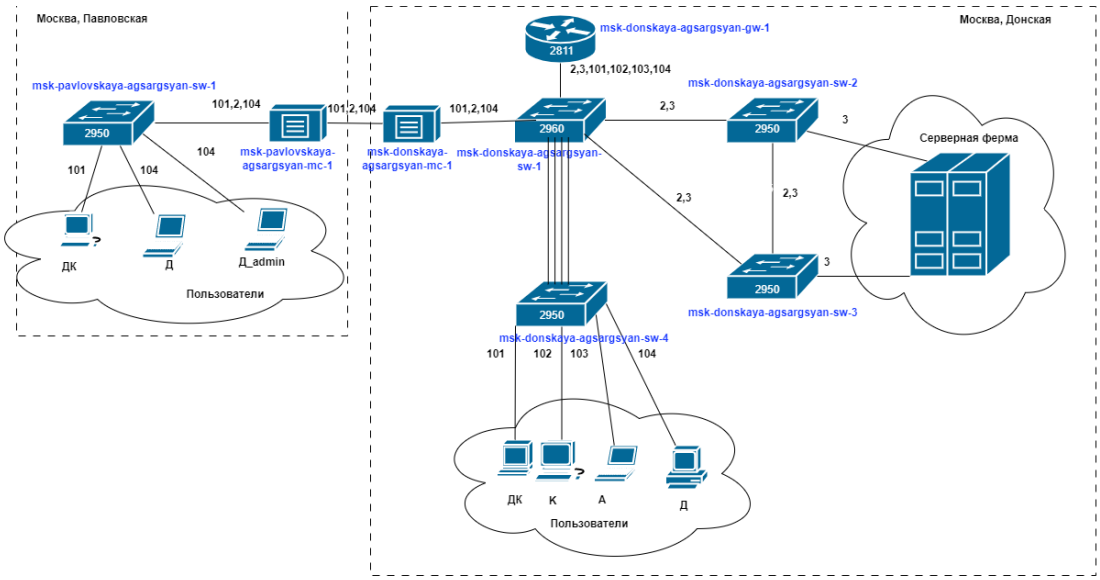

Рис. 19

A	B	C
№ VLAN	**Имя**	**Примечание**
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4-100	nat	для Интернета
5-100		Зарезервировано
101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей

Рис. 20

A	B	C
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-agsargsyan-sw-1	
10.128.1.3	msk-donskaya-agsargsyan-sw-2	
10.128.1.4	msk-donskaya-agsargsyan-sw-3	
10.128.1.5	msk-donskaya-agsargsyan-sw-4	
10.128.1.6	msk-pavlovskaya-agsargsyan-sw-1	
10.128.1.6-10.128.1.254	Зарезервировано	
10.128.2.0/24	Сеть Point-to-Point	
10.128.2.1	Шлюз	
10.128.2.30-10.128.2.199	Зарезервировано	
10.128.3.0/24	Дисплейные классы (ДК)	101
10.128.3.1	Шлюз	
10.128.3.30-10.128.3.199	Пул для пользователей	
10.128.4.0/24	Кафедры (К)	102
10.128.4.1	Шлюз	
10.128.4.30-10.128.4.199	Пул для пользователей	
10.128.5.0/24	Администрация (А)	103
10.128.5.1	Шлюз	
10.128.5.30-10.128.5.199	Пул для пользователей	
10.128.6.0/24	Другие пользователи (Д)	104
10.128.6.1	Шлюз	
10.128.6.30-10.128.6.199	Пул для пользователей	
10.128.6.200	admin-agsargsyan-donskaya	
10.128.6.201	Admin-agsargsyan-pavlovskaya	

Рис. 21

Устройство	Порт	Примечание	Access VLAN	Trunk VLAN
msk-donskaya-agsargsyan-gw-1	f0/1	UpLink		
	f0/0	msk-donskaya-agsargsyan-sw-1		2, 3, 101, 102, 103, 104
msk-donskaya-agsargsyan-sw-1	g1/1	msk-donskaya-agsargsyan-gw-1		
	g1/2	msk-donskaya-agsargsyan-sw-2		2,3
	f0/20-f0/23	msk-donskaya-agsargsyan-sw-4		2, 101, 102, 103, 104
	f0/2	msk-donskaya-agsargsyan-pc-1		2,101,104
msk-donskaya-agsargsyan-sw-2	g1/1	msk-donskaya-agsargsyan-sw-1		2,3
	g1/2	msk-donskaya-agsargsyan-sw-3		2,3
	f0/1	Web-server	3	
	f0/2	File-server	3	
	g1/1	msk-donskaya-agsargsyan-sw-2		2,3
msk-donskaya-agsargsyan-sw-3	f0/1	Mail-server	3	
	f0/2	Dns-server	3	
msk-donskaya-agsargsyan-sw-4	f0/20-f0/23	msk-donskaya-agsargsyan-sw-1		2, 101, 102, 103, 104
	f0/1–f0/5	dk	101	
	f0/6–f0/10	departments	102	
	f0/11–f0/15	adm	103	
	F0/24	other-adm	104	
	f0/16–f0/19	other	104	
msk-pavlovskaya-agsargsyan-sw-1	f0/24	msk-pavlovskaya-agsargsyan-pc-1		2, 101, 104
	f0/1–f0/15	dk	101	
	F0/23	other-adm	104	
	f0/20-f0/21	other	104	
msk-donskaya-agsargsyan-pc-1	f0/0	msk-donskaya-agsargsyan-sw-1		2, 101, 104
	f0/1	msk-pavlovskaya-agsargsyan-pc-1		2, 101, 104
msk-pavlovskaya-agsargsyan-pc-1	f0/0	msk-pavlovskaya-agsargsyan-sw-1		2, 101, 104
	f0/1	msk-donskaya-agsargsyan-pc-1		2, 101, 104

Рис. 22

ИТОГОВЫЕ КОНФИГУРАЦИИ

1. **msk-donskaya-agsargsyan-gw-1**

   !

   version 12.4

   no service timestamps log datetime msec

   no service timestamps debug datetime msec

   service password-encryption

   !

   hostname msk-donskaya-agsargsyan-gw-1

   !

   !

   !

   enable secret 5 1mERr$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
!
!
!
!
!
```

```
!
!
!
ip domain-name donskaya.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
 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
ip access-list extended other-in
 remark admin
 permit ip host 10.128.6.200 any
 permit ip host 10.128.6.201 any
ip access-list extended management-out
 remark admin
 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
 permit ip host 10.128.6.201 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-lists

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

ip access-list resequence

ВЫВОД

Я освоил настройку прав доступа пользователей к ресурсам сети.