

Лабораторная работа 10

Настройка списков управления доступом (ACL)

Ланцова Я. И.

Российский университет дружбы народов, Москва, Россия

Информация

- Ланцова Яна Игоревна
- студентка
- Российский университет дружбы народов

Освоить настройку прав доступа пользователей к ресурсам сети.

1. Требуется настроить правила доступа.
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.

Выполнение лабораторной работы

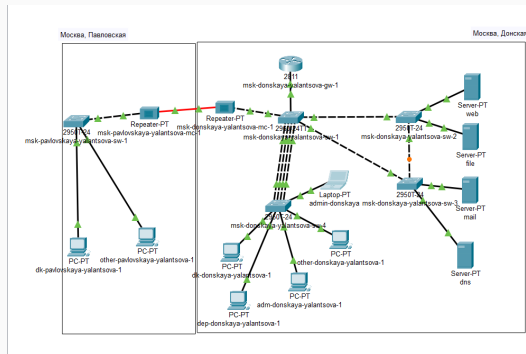


Рис. 1: Размещение ноутбука администратора в сети other-donskaya-1

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

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


```
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.3
msk-donskaya-yalantsova-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-yalantsova-gw-1(config-subif)#
```

Рис. 3: Добавление список управления доступом к интерфейсу

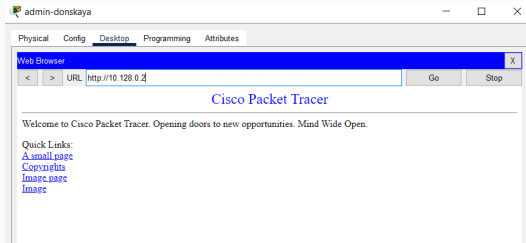
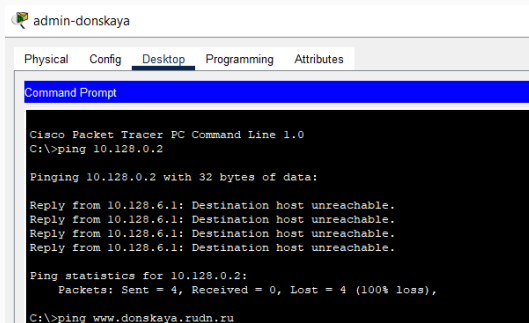


Рис. 4: Проверка доступа к web-серверу через браузер



```
admin-donskaya
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
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),

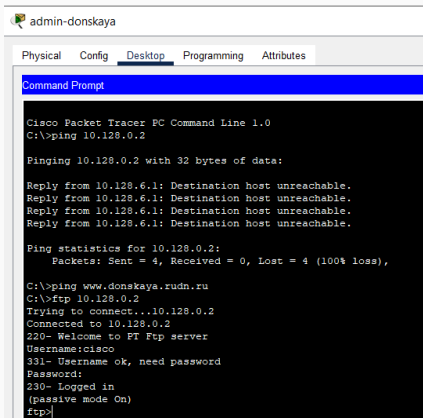
C:\>ping www.donskaya.rudn.ru
```

Рис. 5: Проверка доступа к web-серверу с помощью ping

```
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#
```

Рис. 6: Настройка доступа по Telnet и FTP

Выполнение лабораторной работы



The screenshot shows the Cisco Packet Tracer PC Command Line interface for a device named 'admin-donskaya'. The interface has tabs for Physical, Config, Desktop, Programming, and Attributes, with 'Desktop' currently selected. The Command Prompt window displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
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 www.donskaya.rudn.ru
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>
```

Рис. 7: Проверка доступа к web-серверу по протоколу FTP с устройства администратора

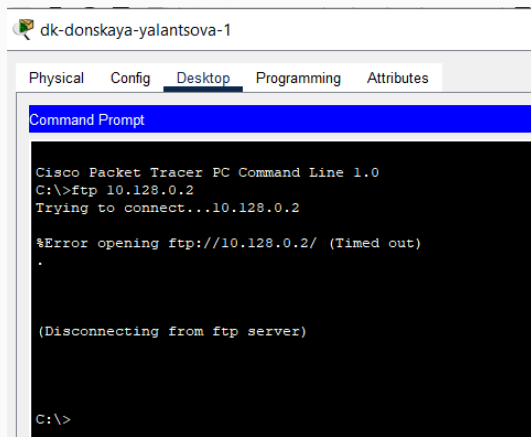


Рис. 8: Проверка доступа к web-серверу по протоколу FTP с устройства dk-donskaya-1

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

Рис. 9: Настройка доступа к файловому серверу

```
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark mail
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
```

Рис. 10: Настройка доступа к почтовому серверу


```
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark dns
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#
```

Рис. 11: Настройка доступа к DNS-серверу

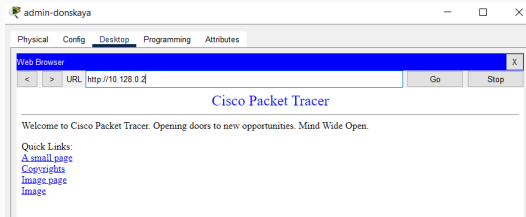


Рис. 12: Проверка доступа к web-серверу по ip-адресу

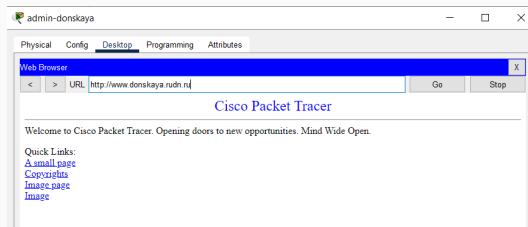


Рис. 13: Проверка доступа к web-серверу по имени

```
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#exit
msk-donskaya-yalantsova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-yalantsova-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 (15 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))

msk-donskaya-yalantsova-gw-1#
```

Рис. 14: Разрешение icmp-запросов

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

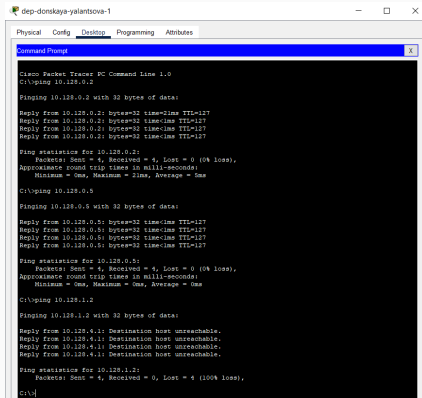
Рис. 15: Настройка доступа для сети Other

```
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended management-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.2
msk-donskaya-yalantsova-gw-1(config-subif)#ip access group management out out
^
% Invalid input detected at '^' marker.

msk-donskaya-yalantsova-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-yalantsova-gw-1(config-subif)#
```

Рис. 16: Настройка доступа администратора к сети сетевого оборудования

Выполнение лабораторной работы



```
dep-donskaya-yalantsova-1
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
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=21ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms 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 = 0ms, Maximum = 21ms, Average = 5ms

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Reply from 10.128.0.5: bytes=32 time<1ms TTL=127
Reply from 10.128.0.5: bytes=32 time<1ms TTL=127
Reply from 10.128.0.5: bytes=32 time<1ms TTL=127
Reply from 10.128.0.5: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.

Ping statistics for 10.128.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 17: Проверка правил доступа для оконечного устройства на примере dep-donskaya-1 с помощью команды ping

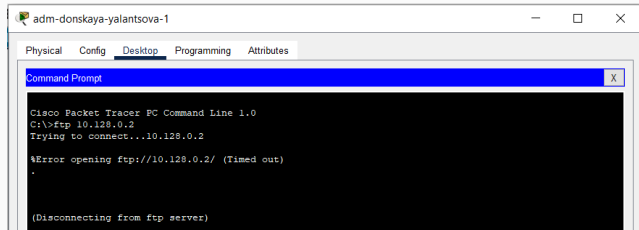
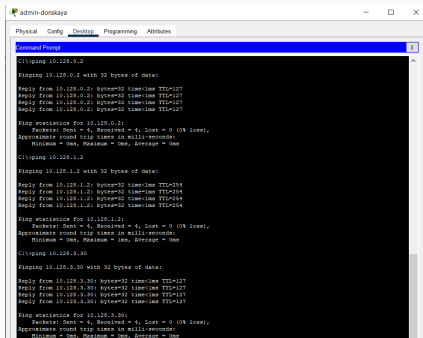


Рис. 18: Проверка правил доступа для оконечного устройства на примере dep-donskaya-1 с помощью протокола ftp

Выполнение лабораторной работы



```
admin-donskaya
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.129.0.2

Pinging 10.129.0.2 with 32 bytes of data:

Reply from 10.129.0.2: bytes=32 time=1ms TTL=127
Reply from 10.129.0.2: bytes=32 time=1ms TTL=127
Reply from 10.129.0.2: bytes=32 time=1ms TTL=127
Reply from 10.129.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.129.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 10.129.1.2

Pinging 10.129.1.2 with 32 bytes of data:

Reply from 10.129.1.2: bytes=32 time=1ms TTL=254
Reply from 10.129.1.2: bytes=32 time=1ms TTL=254
Reply from 10.129.1.2: bytes=32 time=1ms TTL=254
Reply from 10.129.1.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.129.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 10.129.3.30

Pinging 10.129.3.30 with 32 bytes of data:

Reply from 10.129.3.30: bytes=32 time=1ms TTL=127
Reply from 10.129.3.30: bytes=32 time=1ms TTL=127
Reply from 10.129.3.30: bytes=32 time=1ms TTL=127
Reply from 10.129.3.30: bytes=32 time=1ms TTL=127

Ping statistics for 10.129.3.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Рис. 19: Проверка правил доступа для администратора с помощью команды ping

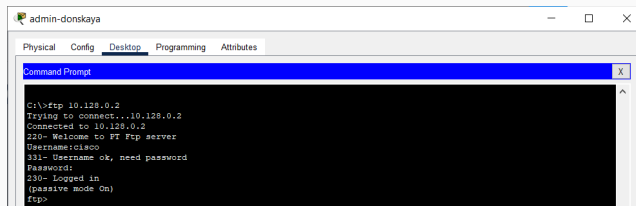
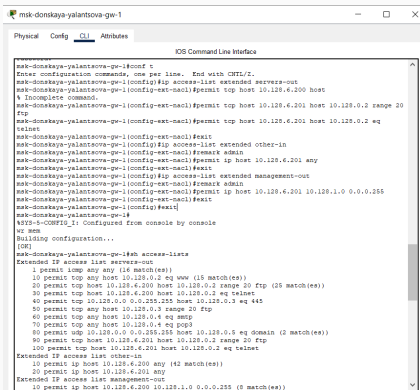


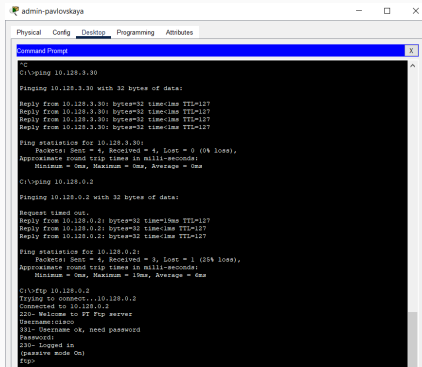
Рис. 20: Проверка правил доступа для администратора с помощью протокола ftp



```
msk-donskaya-yalantsova-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
#
msk-donskaya-yalantsova-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
% Incomplete command.
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range 20
ftp
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended other-in
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended management-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#exit
msk-donskaya-yalantsova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
vr mem
Building configuration...
[OK]
msk-donskaya-yalantsova-gw-1#sh access-lists
Extended IP access list servers-out
  1 permit icmp any any (16 match(es))
  10 permit tcp any host 10.128.0.2 eq www (15 match(es))
  20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (25 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 443
  50 permit tcp any host 10.128.0.3 range 20 smtp
  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))
  90 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
  100 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 (42 match(es))
  20 permit ip host 10.128.6.201 any
Extended IP access list management-out
  10 permit sp host 10.128.6.200 10.128.1.0 0.0.0.255 (8 match(es))
```

Рис. 21: Настройка прав администратора на Павловской

Выполнение лабораторной работы



```
admin-pavlovskaya
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>
C:\>ping 10.128.3.30

Pinging 10.128.3.30 with 32 bytes of data:

Reply from 10.128.3.30: bytes=32 time<1ms TTL=127
Reply from 10.128.3.30: bytes=32 time<1ms TTL=127
Reply from 10.128.3.30: bytes=32 time<1ms TTL=127
Reply from 10.128.3.30: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.3.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 6ms

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

Рис. 22: Проверка правил доступа для администратора на Павловской

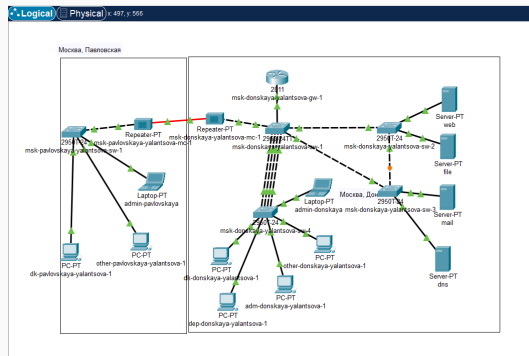


Рис. 23: Схема сети в логической рабочей области Packet Tracer

В результате выполнения лабораторной работы освоили настройку прав доступа пользователей к ресурсам сети.