

Лабораторная работа №10

Настройка списков управления доступом (ACL)

Джахангиров Илгар Залид оглы

Российский университет дружбы народов, Москва, Россия

Информация

- Джахангиров Илгар Залид оглы
- студент
- Российский университет дружбы народов
- [1032225689@pfur.ru]

Освоить настройку прав доступа пользователей к ресурсам сети.

1. Требуется настроить следующие правила доступа:
 - web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
 - файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
 - 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;
 - DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
 - разрешить icmp-сообщения, направленные в сеть серверов;
 - запретить для сети Other любые запросы за пределы сети, за исключением администратора;
 - 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 Парковой

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

Выполнение лабораторной работы

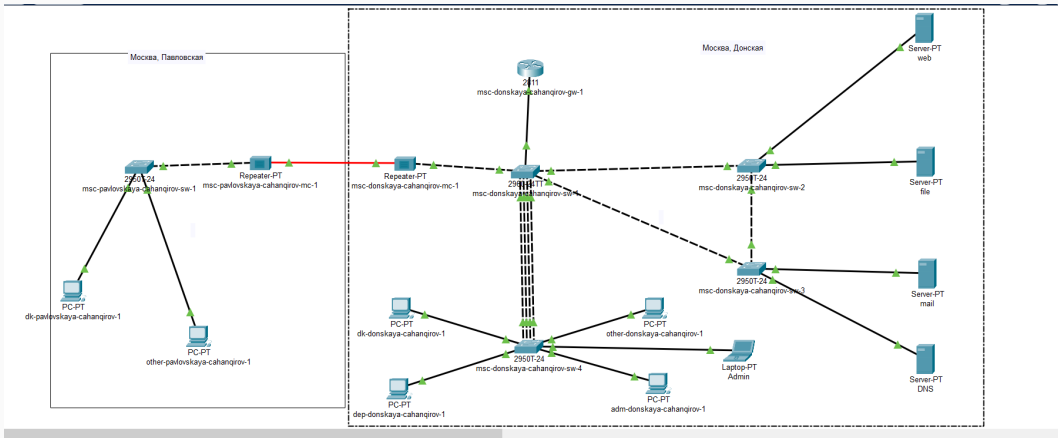


Figure 1: Размещение ноутбука администратора в сети other-donskaya-1

Выполнение лабораторной работы

Admin

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.C980.A641

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 10.128.6.200

Subnet Mask 255.255.255.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::201:C9FF:FE80:A641

Выполнение лабораторной работы

The screenshot shows a web-based configuration interface for a device named 'Admin'. The interface has a top navigation bar with tabs: Physical, Config (selected), Desktop, Programming, and Attributes. On the left is a sidebar menu with categories: GLOBAL (containing Settings and Algorithm Settings), INTERFACE (containing FastEthernet0 and Bluetooth), and a search bar. The main content area is titled 'Global Settings' and is divided into two sections for IP configuration. The 'FastEthernet0' interface is selected in a dropdown menu. The 'Gateway/DNS IPv4' section has 'Static' selected, with a 'Default Gateway' of 10.128.6.1 and a 'DNS Server' of 10.128.0.5. The 'Gateway/DNS IPv6' section also has 'Static' selected, but the 'Default Gateway' and 'DNS Server' fields are empty. A 'Top' link is at the bottom left.

Admin

Physical Config Desktop Programming Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

Global Settings

Display Name Admin

Interfaces FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 10.128.6.1

DNS Server 10.128.0.5

Gateway/DNS IPv6

☐ Automatic

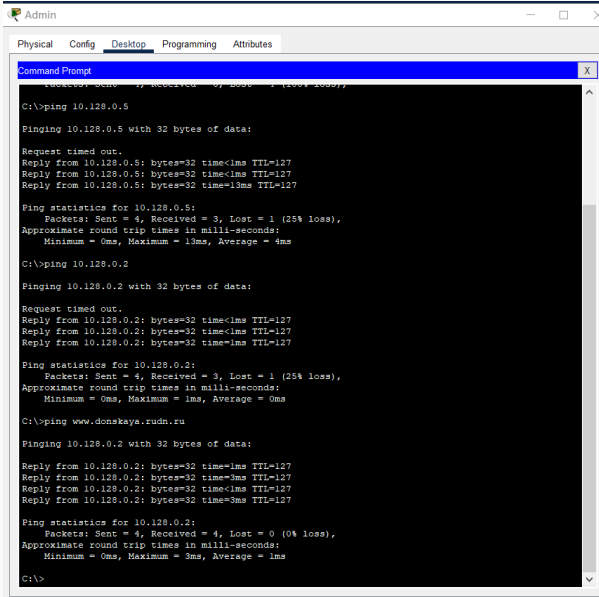
☒ Static

Default Gateway

DNS Server

☐ Top

Выполнение лабораторной работы



```
Admin
Physical Config Desktop Programming Attributes
Command Prompt X

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Request timed out.
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=13ms TTL=127

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 4ms

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 = 1ms, Average = 0ms

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

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=3ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time=3ms 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 = 3ms, Average = 1ms

C:\>
```

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended servers-out
^
% Invalid input detected at '^' marker.

msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended servers-out
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark web
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

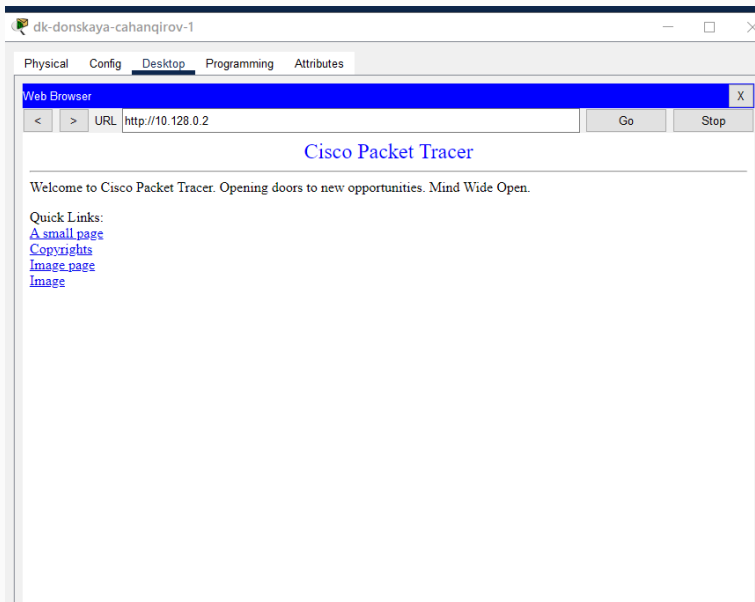
Figure 5: Настройка доступа к web-серверу по порту tcp 80

```
msc-donskaya-cahanqirov-gw-1#  
msc-donskaya-cahanqirov-gw-1#conf t  
Enter configuration commands, one per line.  End with CNTL/Z.  
msc-donskaya-cahanqirov-gw-1(config)#interface f0/0.3  
msc-donskaya-cahanqirov-gw-1(config-subif)#ip access-group servers-out out  
msc-donskaya-cahanqirov-gw-1(config-subif)#^Z  
msc-donskaya-cahanqirov-gw-1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
msc-donskaya-cahanqirov-gw-1#wr m  
Building configuration...  
[OK]  
msc-donskaya-cahanqirov-gw-1#
```

Figure 6: Добавление списка управления доступом к интерфейсу

Проверим, что доступ к web-серверу есть через протокол HTTP, введя в строке браузера хоста IP-адрес web-сервера (рис.??). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по IP-адресу web-сервера (рис.??).

Выполнение лабораторной работы



```
C:\>ping 10.128.0.5
```

```
Pinging 10.128.0.5 with 32 bytes of data:
```

```
Request timed out.
```

```
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=13ms TTL=127
```

```
Ping statistics for 10.128.0.5:
```

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

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

```
    Minimum = 0ms, Maximum = 13ms, Average = 4ms
```

```
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 = 1ms, Average = 0ms
```

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Figure 9: Настройка дополнительного доступа для администратора по протоколам Telnet и FTP

Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP (рис.??). Для этого в командной строке устройства администратора введем ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco, увидим, что доступ действительно есть.

```
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>
```

Figure 10: Проверка работы ftp у администратора

Попробуем провести аналогичную процедуру с другого устройства сети (рис.??). Увидим, что доступ запрещён.


```
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)
```

Figure 11: Проверка недоступности подключения по ftp у просто пользователя

Настроим доступ к файловому серверу (рис.??). 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

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Figure 12: Настройка доступа к файловому серверу

Настроим доступ к почтовому серверу (рис.??). 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

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
```

Figure 13: Настройка доступа к почтовому серверу

Настроим доступ к DNS-серверу (рис.??). 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

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Figure 14: Настройка доступа к DNS-серверу

Разрешим істр-запросы (рис.??).

```
m-sc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
m-sc-donskaya-cahanqirov-gw-1(config)#ip access-list extended servers-out
m-sc-donskaya-cahanqirov-gw-1(config-ext-nacl)#1 permit icmp any an
m-sc-donskaya-cahanqirov-gw-1(config-ext-nacl)#^Z
m-sc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

m-sc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
m-sc-donskaya-cahanqirov-gw-1#
```

Figure 15: Разрешение icmp-запросов

Посмотрим номера строк правил в списке контроля доступа (рис.??).

```
msc-donskaya-cahanqirov-gw-1#show access-lists
Extended IP access list servers-out
 10 permit icmp any any (16 match(es))
 20 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
 30 permit tcp any host 10.128.0.3 range 20 ftp
 40 permit tcp any host 10.128.0.4 eq smtp
 50 permit tcp any host 10.128.0.4 eq pop3
 60 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (2 match(es))
 70 permit tcp any host 10.128.0.2 eq www (10 match(es))
 80 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
 90 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
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 (33 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
Extended IP access list servers-in
 10 permit ip host 10.128.6.200 any
msc-donskaya-cahanqirov-gw-1#
```

Figure 16: Просмотр строк в списке контроля доступа

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended other-in
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark admin
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#exit
msc-donskaya-cahanqirov-gw-1(config)#interface f0/0.104
msc-donskaya-cahanqirov-gw-1(config-subif)#ip access group other in in
                                                                    ^
% Invalid input detected at '^' marker.

msc-donskaya-cahanqirov-gw-1(config-subif)#ip access group other in in
                                                                    ^
% Invalid input detected at '^' marker.

msc-donskaya-cahanqirov-gw-1(config-subif)#ip access-group other-in in
msc-donskaya-cahanqirov-gw-1(config-subif)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
```

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended management-out
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark admin
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#exit
msc-donskaya-cahanqirov-gw-1(config)#interface f0/0.2
msc-donskaya-cahanqirov-gw-1(config-subif)#ip access-group management-out out
msc-donskaya-cahanqirov-gw-1(config-subif)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Figure 18: Настройка доступа администратора к сети сетевого оборудования

Проверим получившийся список контроля доступа (рис.??).


```
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 servers-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
!
```

В процессе выполнения данной лабораторной работы я освоил настройку прав доступа пользователей к ресурсам сети.