

Лабораторная Работа №10. Настройка списков управления доступом (ACL).

Администрирование локальных сетей

Исаев Б.А.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

- Исаев Булат Абубакарович
- НПИБд-01-22
- Российский университет дружбы народов
- [1132227131@pfur.ru]

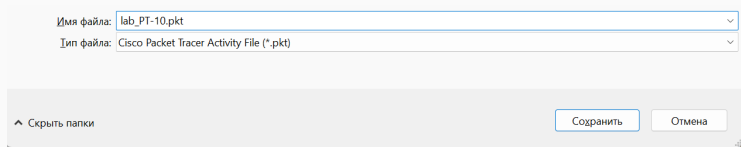


Figure 1: Открытие проекта lab_PT-10.pkt.

Подсоединение ноутбука

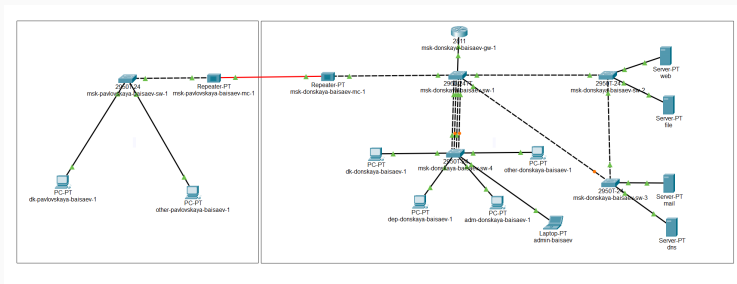
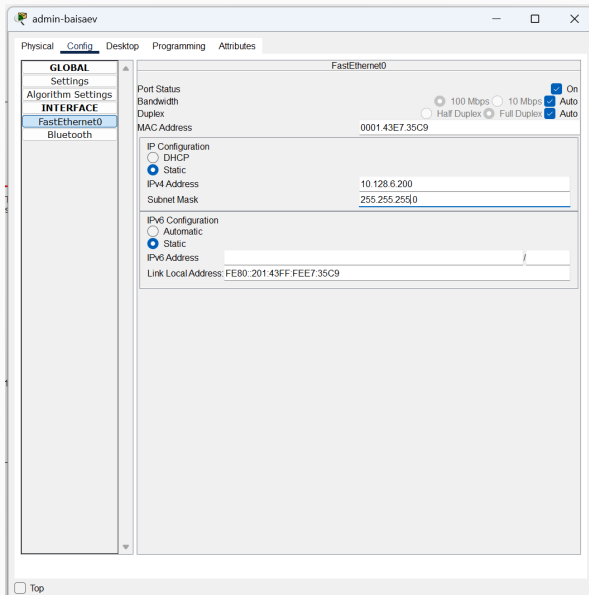


Figure 2: Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-baisaev-sw-4 и изменение названия.

Присвоение адресов



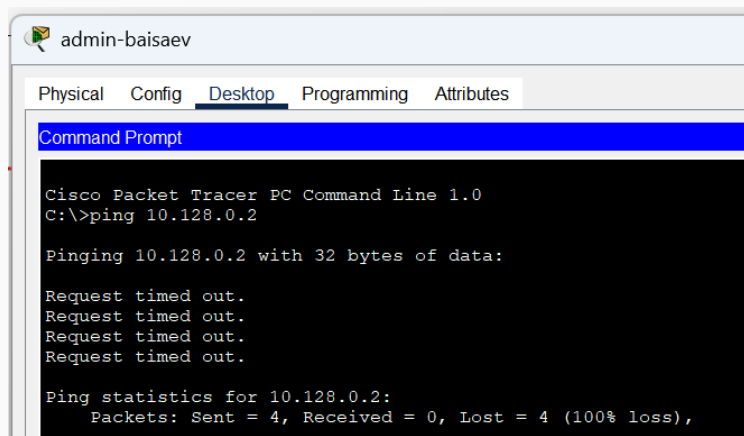


Figure 4: Проверка (пингуем с admin-baisaev 10.128.0.2 и 10.128.0.5).

Настройка доступа к web-серверу

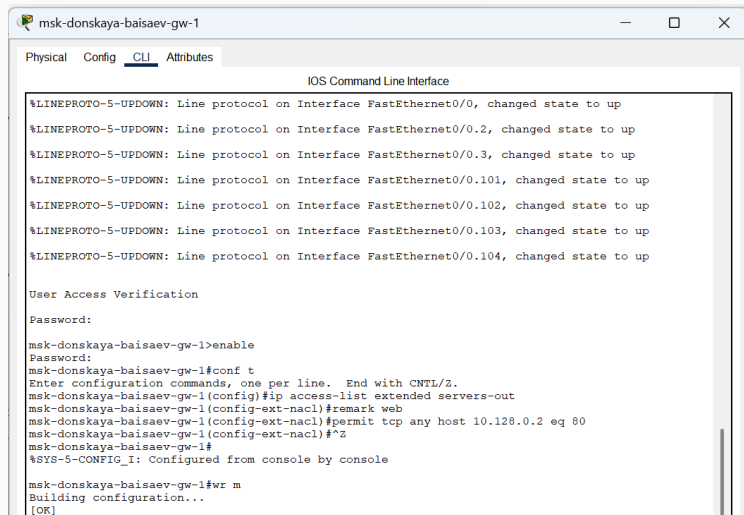


Figure 5: Настройка доступа к web-серверу по порту tcp 80 (создан список контроля доступа с названием servers-out; указано, что ограничения предназначены для работы 7/26

Добавление списка управления

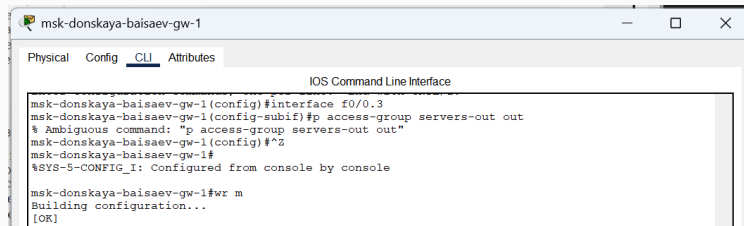
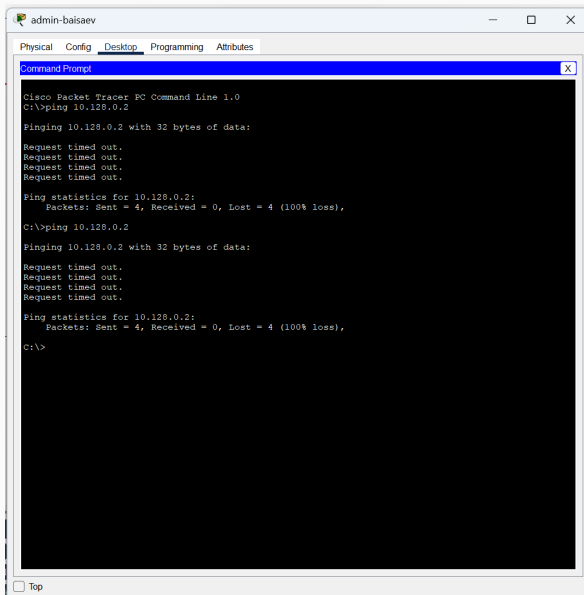


Figure 6: Добавление списка управления доступом к интерфейсу (к интерфейсу f0/0.3 подключается список прав доступа serversout и применяется к исходящему трафику).

Проверка



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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.128.0.2:
    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:

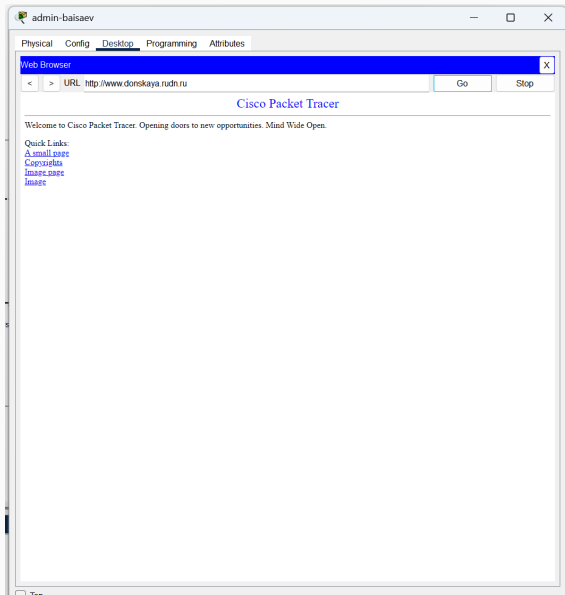
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

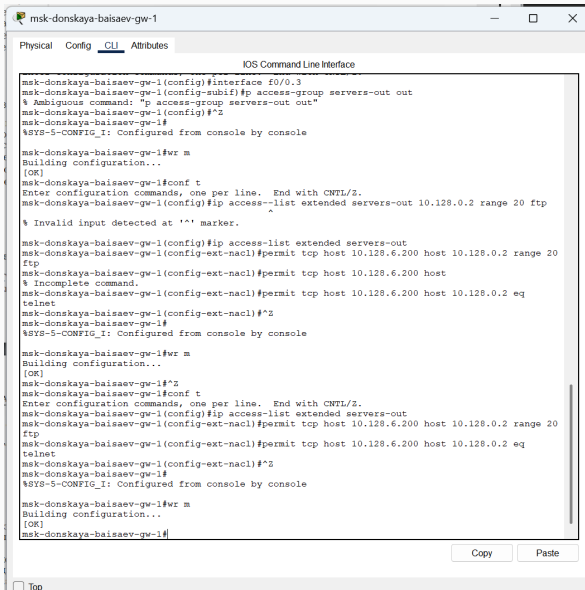
C:\>
```

At the bottom left of the window, there is a 'Top' button.

Проверка



Настройка дополнительного доступа



The screenshot shows a network configuration window titled "msk-donskaya-baisaev-gw-1" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the IOS Command Line Interface. The configuration process is shown in two stages, each starting with "msk-donskaya-baisaev-gw-1#wr m" and "Building configuration...".

```
msk-donskaya-baisaev-gw-1(config)#interface f0/0.3
msk-donskaya-baisaev-gw-1(config-subif)#p access-group servers-out out
% Ambiguous command: "p access-group servers-out out"
msk-donskaya-baisaev-gw-1(config)#^Z
msk-donskaya-baisaev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out 10.128.0.2 range 20 ftp
% Invalid input detected at '^' marker.

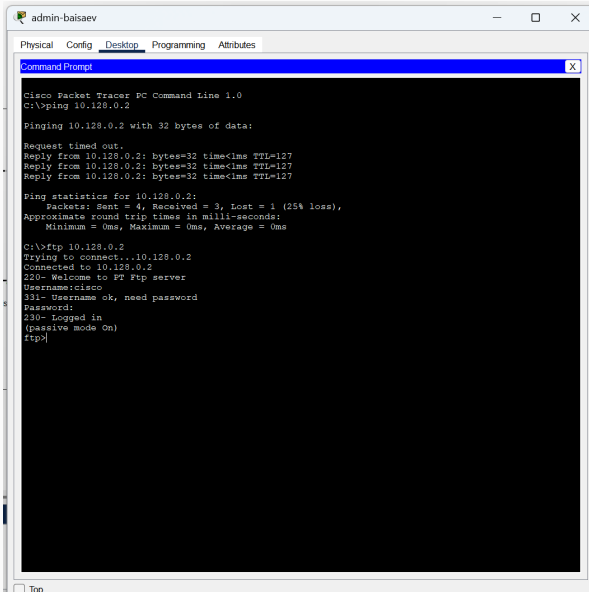
msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20
ftp
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
% Incomplete command.
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
msk-donskaya-baisaev-gw-1(config-ext-nacl)#^Z
msk-donskaya-baisaev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" button in the bottom left corner.

Проверка



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'admin-balsaev'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt shows the following sequence of commands and outputs:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.128.0.2

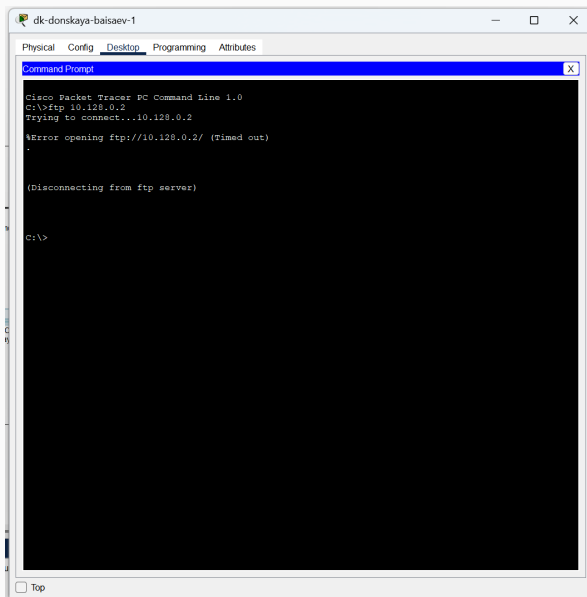
Pinging 10.128.0.2 with 32 bytes of data:

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 = 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 FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Проверка



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'dk-donskaya-balsaev-1'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. Inside the window, a 'Command Prompt' window is open, displaying the following text:

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

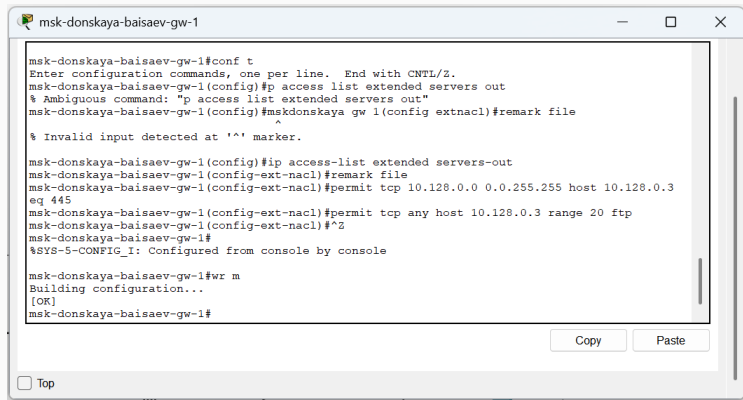
%Error opening ftp://10.128.0.2/ (Timed out)
.

(Disconnecting from ftp server)

C:\>
```

At the bottom left of the main window, there is a 'Top' button.

Настройка доступа к файловому серверу



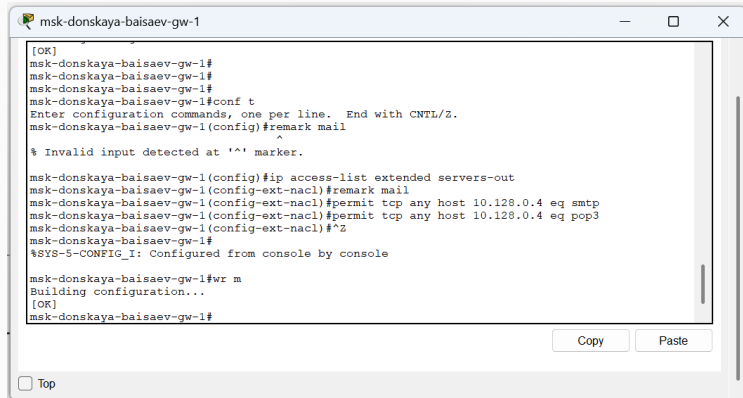
```
mik-donskaya-baisaev-gw-1
mik-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
mik-donskaya-baisaev-gw-1(config)#p access list extended servers out
% Ambiguous command: "p access list extended servers out"
mik-donskaya-baisaev-gw-1(config)#mskdonskaya gw 1(config extnacl)#remark file
^
% Invalid input detected at '^' marker.

mik-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
mik-donskaya-baisaev-gw-1(config-ext-nacl)#remark file
mik-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
mik-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
mik-donskaya-baisaev-gw-1(config-ext-nacl)#^Z
mik-donskaya-baisaev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

mik-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
mik-donskaya-baisaev-gw-1#
```

Figure 12: Настройка доступа к файловому серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP (запись 0.0.255.255 — обратная маска)).

Настройка доступа к почтовому серверу



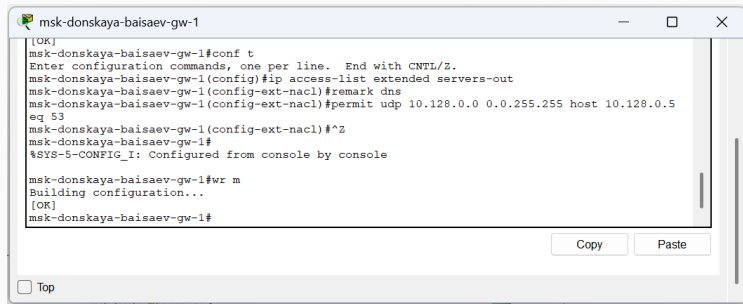
```
[OK]
msk-donskaya-baisaev-gw-1#
msk-donskaya-baisaev-gw-1#
msk-donskaya-baisaev-gw-1#
msk-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#remark mail
      ^
% Invalid input detected at '^' marker.

msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
msk-donskaya-baisaev-gw-1(config-ext-nacl)#remark mail
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-baisaev-gw-1(config-ext-nacl)#^Z
msk-donskaya-baisaev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Figure 13: Настройка доступа к почтовому серверу (в списке контроля доступа `servers-out` указано, что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP).

Настройка доступа к DNS-серверу

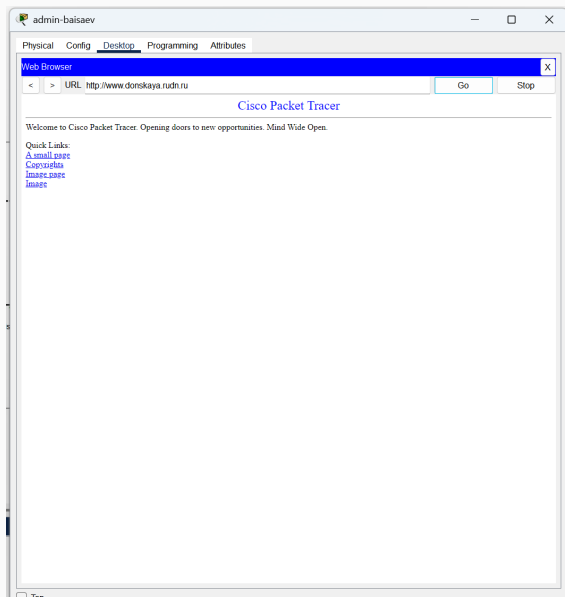


```
msk-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
msk-donskaya-baisaev-gw-1(config-ext-nacl)#remark dns
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host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

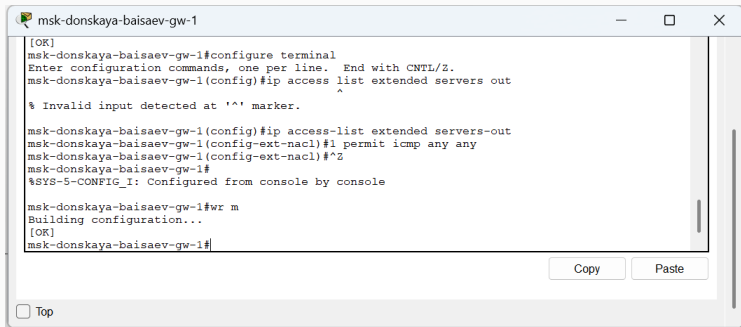
msk-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-baisaev-gw-1#
```

Figure 14: Настройка доступа к DNS-серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53)

Проверка



Разрешение icmp-запросов



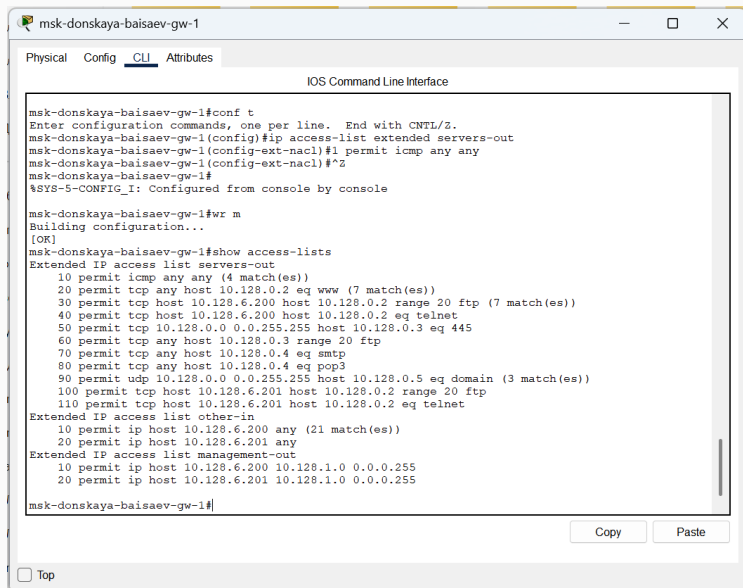
```
[OK]
msk-donskaya-baisaev-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
                                     ^
% Invalid input detected at '^' marker.

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

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

Figure 16: Разрешение icmp-запросов (демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступ).

Просмотр номеров строк

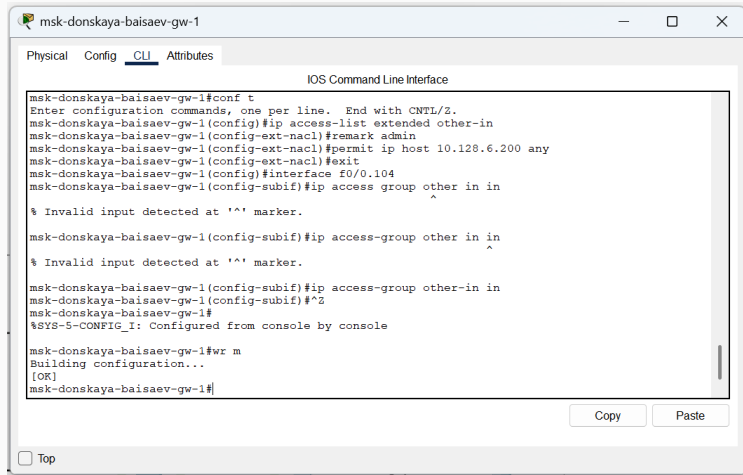


```
msk-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#ip access-list extended servers-out
msk-donskaya-baisaev-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-baisaev-gw-1(config-ext-nacl)#^Z
msk-donskaya-baisaev-gw-1#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

msk-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-baisaev-gw-1#show access-lists
Extended IP access list servers-out
 10 permit icmp any any (4 match(es))
 20 permit tcp any host 10.128.0.2 eq www (7 match(es))
 30 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
 40 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
 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
 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 (3 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 (21 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-donskaya-baisaev-gw-1#
```

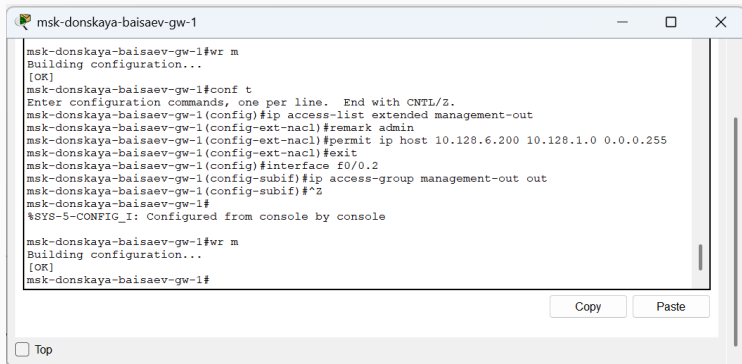
Настройка доступа для сети Other



```
msk-donskaya-baisaev-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
msk-donskaya-baisaev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-baisaev-gw-1(config)#ip access-list extended other-in
msk-donskaya-baisaev-gw-1(config-ext-nacl)#remark admin
msk-donskaya-baisaev-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-baisaev-gw-1(config-ext-nacl)#exit
msk-donskaya-baisaev-gw-1(config)#interface f0/0.104
msk-donskaya-baisaev-gw-1(config-subif)#ip access group other in in
^
% Invalid input detected at '^' marker.
msk-donskaya-baisaev-gw-1(config-subif)#ip access-group other in in
^
% Invalid input detected at '^' marker.
msk-donskaya-baisaev-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-baisaev-gw-1(config-subif)#^Z
msk-donskaya-baisaev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
msk-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-baisaev-gw-1#
```

Figure 18: Настройка доступа для сети Other (в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; разрешение устройству с адресом 10.128.6.200 на публичные действия: подключение к интерфейсу

Настройка доступа администратора



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

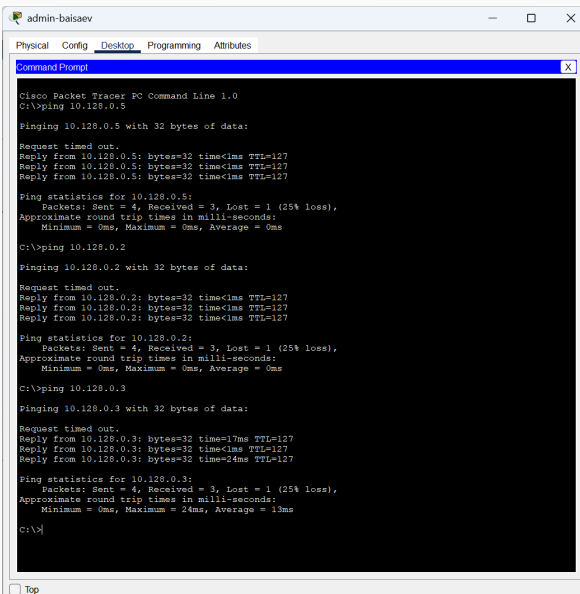
msk-donskaya-baisaev-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-baisaev-gw-1#
```

Copy Paste

☐ Top

Figure 19: Настройка доступа администратора к сети сетевого оборудования (в списке контроля доступа management-out указано, что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключён список прав доступа management-out и применено к исходящему трафику).

Проверка корректности правил



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

```
Cisco Packet Tracer PC Command Line 1.0
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<1ms 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 = 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 = 0ms, Average = 0ms

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=17ms TTL=127
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
Reply from 10.128.0.3: bytes=32 time=24ms 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 = 24ms, Average = 13ms

C:\>
```

At the bottom left of the window, there is a checkbox labeled 'Top' which is currently unchecked.

Проверка корректности правил

```
other-donskaya-baisaev-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:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

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:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

C:\>ping 10.128.0.3

Pinging 10.128.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.128.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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)
```

Разрешение администратору (Павловская)

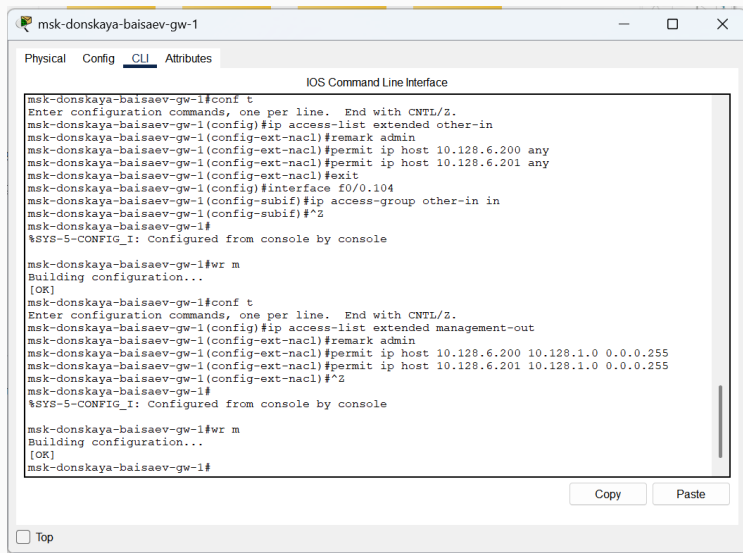
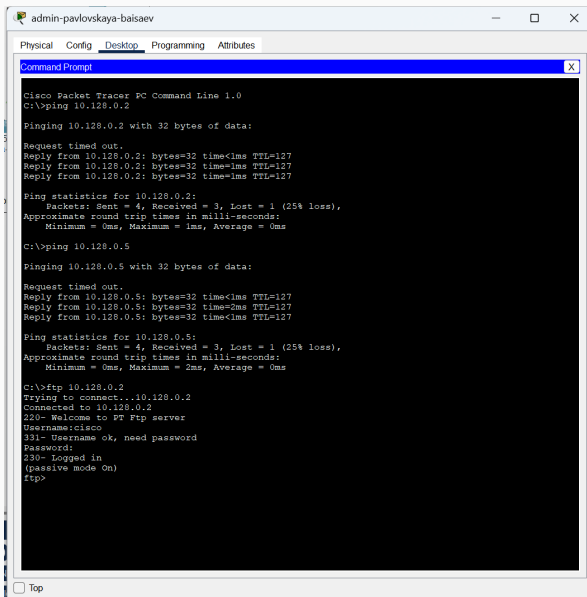


Figure 22: Разрешение администратору из сети Other на Павловской действия

Проверка разрешений



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'admin-pavlovskaya-baisaev'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The Command Prompt shows the following commands and output:

```
Cisco Packet Tracer PC Command Line 1.0
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 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=2ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, 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>
```

At the bottom left of the window, there is a checkbox labeled 'Top' which is currently unchecked.

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