

Лабораторная работа 10

Настройка списков управления доступом (ACL)

Ланцова Яна Игоревна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	21
5	Контрольные вопросы	22

Список иллюстраций

3.1	Размещение ноутбука администратора в сети other-donskaya-1 . . .	7
3.2	Настройка доступа к web-серверу по порту tcp 80	8
3.3	Добавление список управления доступом к интерфейсу	8
3.4	Проверка доступа к web-серверу через барузер	9
3.5	Проверка доступа к web-серверу с помощью ping	9
3.6	Настройка доступа по Telnet и FTP	9
3.7	Проверка доступа к web-серверу по протоколу FTP с устройства ад- министратора	10
3.8	Проверка доступа к web-серверу по протоколу FTP с устройства dk- donskaya-1	11
3.9	Настройка доступа к файловому серверу	11
3.10	Настройка доступа к почтовому серверу	12
3.11	Настройка доступа к DNS-серверу	12
3.12	Проверка доступа к web-серверу по ip-адресу	12
3.13	Проверка доступа к web-серверу по имени	13
3.14	Разрешение icmp-запросов	13
3.15	Настройка доступа для сети Other	14
3.16	Настройка доступа администратора к сети сетевого оборудования	14
3.17	Проверка правил доступа для оконечного устройства на примере dep-donskaya-1 с помощью команды ping	15
3.18	Проверка правил доступа для оконечного устройства на примере dep-donskaya-1 с помощью протокола ftp	16
3.19	Проверка правил доступа для администратора с помощью команды ping	16
3.20	Проверка правил доступа для администратора с помощью протоко- ла ftp	17
3.21	Настройка прав администратора на Павловской	18
3.22	Проверка правил доступа для администратора на Павловской	19
3.23	Схема сети в логической рабочей области Packet Tracer	20

Список таблиц

1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

2 Задание

1. Требуется настроить следующие правила доступа:
 - 1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
 - 2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних – доступ по протоколу FTP;
 - 3) 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;
 - 4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
 - 5) разрешить icmp-сообщения, направленные в сеть серверов;
 - 6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;
 - 7) 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 Павловской.
4. При выполнении работы необходимо учитывать соглашение об именовании.

3 Выполнение лабораторной работы

Откроем проект прошлой лабораторной работы. В рабочей области проекта подключим ноутбук администратора с именем `admin` к сети к `other-donskaya-1` с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоединим ноутбук к порту 24 коммутатора `msk-donskaya-eademidova-sw-4` и присвоим 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. 3.1).

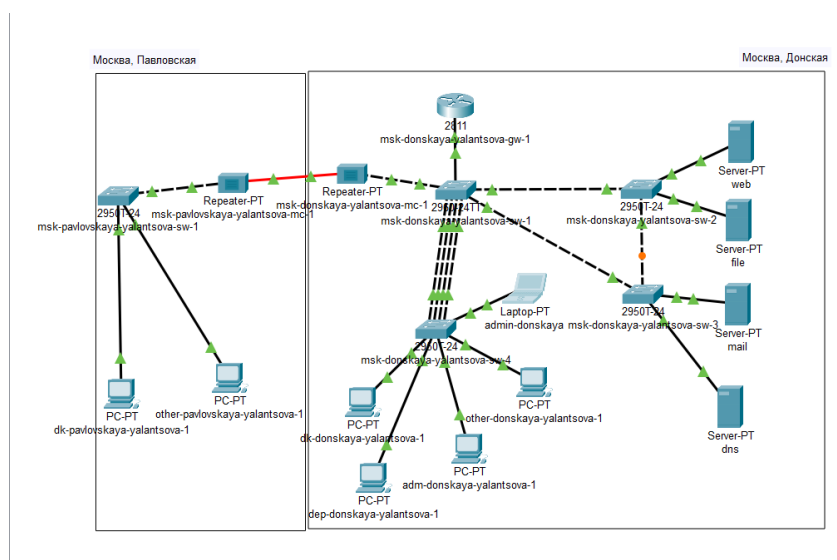


Рис. 3.1: Размещение ноутбука администратора в сети `other-donskaya-1`

Права доступа пользователей сети будем настраивать на маршрутизаторе `msk-donskaya-gw-1`, поскольку именно через него проходит весь трафик сети. Ограничения можно накладывать как на входящий (in), так и на исходящий (out) трафик. По отношению к маршрутизатору накладываемые ограничения будут касаться в основном исходящего трафика.

Следует помнить, что на оборудовании Cisco правила в списке доступа проверяются по порядку сверху вниз до первого совпадения – как только одно из правил сработало, проверка списка правил прекращается и обработка трафика происходит на основе сработавшего правила. Поэтому рекомендуется сначала дать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Кроме того, после всех правил в конце дописывается неявное запрещение на всё, что не разрешено: deny ip any any (implicit deny).

1. Настроим доступа к web-серверу по порту tcp 80 (рис. 3.2):

```
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. 3.2: Настройка доступа к web-серверу по порту tcp 80

Создан список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указано (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером; дано разрешение доступа (permit) по протоколу TCP всем (any) пользователям сети (host) на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80.

2. Добавим список управления доступом к интерфейсу (рис. 3.3):

```
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. 3.3: Добавление список управления доступом к интерфейсу

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) (рис. 3.4):

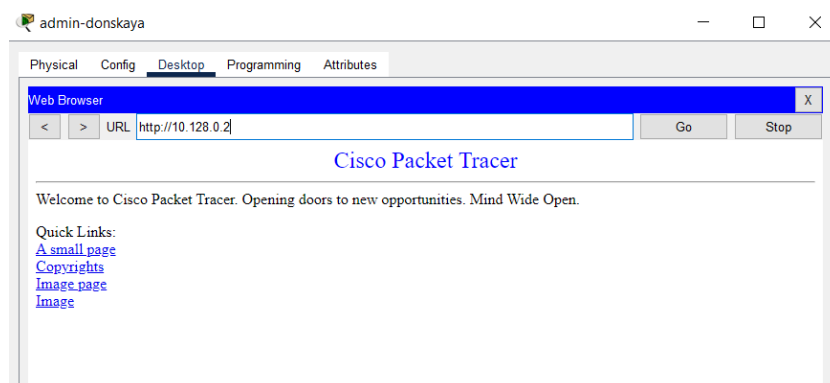


Рис. 3.4: Проверка доступа к web-серверу через браузер

При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера(рис. 3.5).

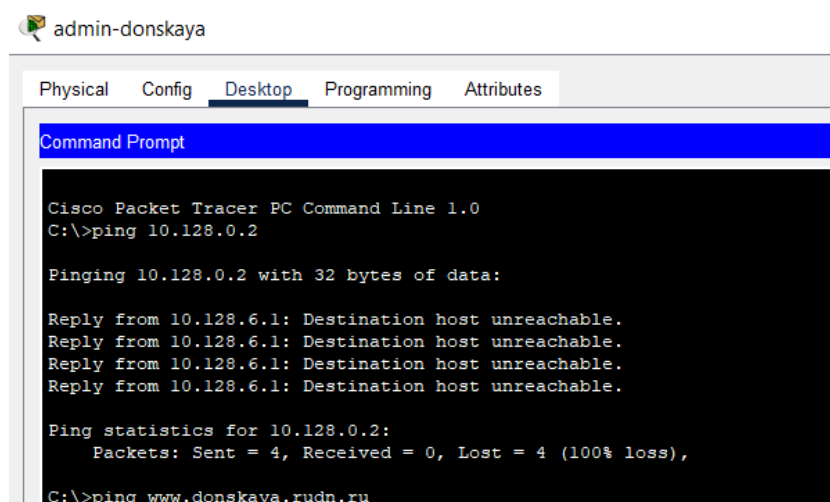


Рис. 3.5: Проверка доступа к web-серверу с помощью ping

3. Дополнительный доступ для администратора по протоколам Telnet и FTP(рис. 3.6).

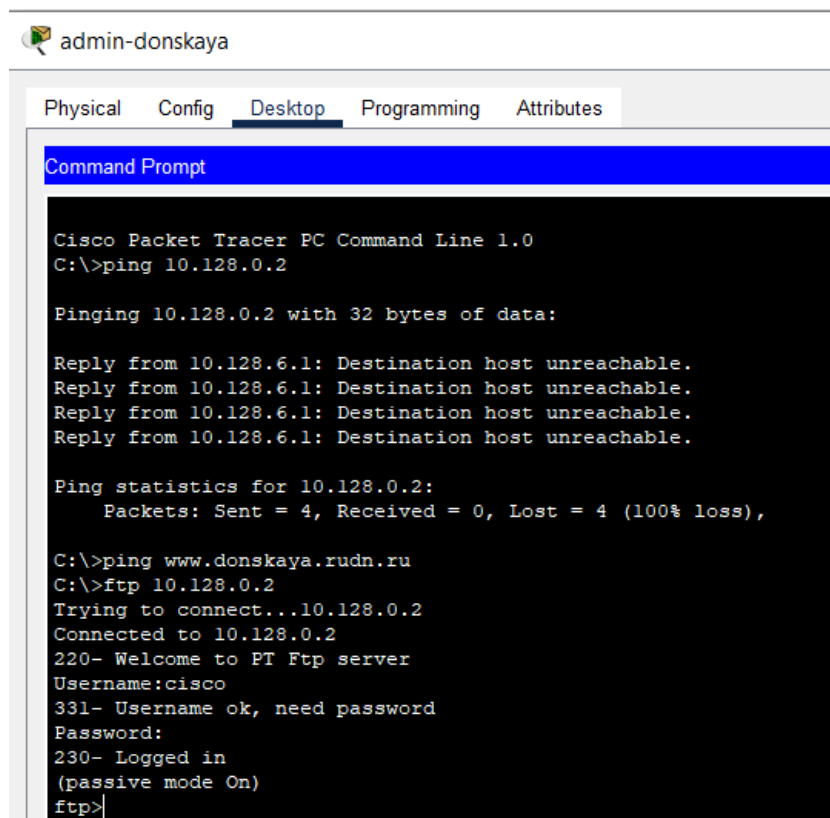
```
msk-donskaya-valantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-valantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-valantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
msk-donskaya-valantsova-gw-1(config-ext-nacl)#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

Рис. 3.6: Настройка доступа по Telnet и FTP

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.

Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введем ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco(рис. 3.7).



```
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
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>
```

Рис. 3.7: Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Попробуем провести аналогичную процедуру с другого устройства сети. Убедимся, что доступ будет запрещён(рис. 3.8).

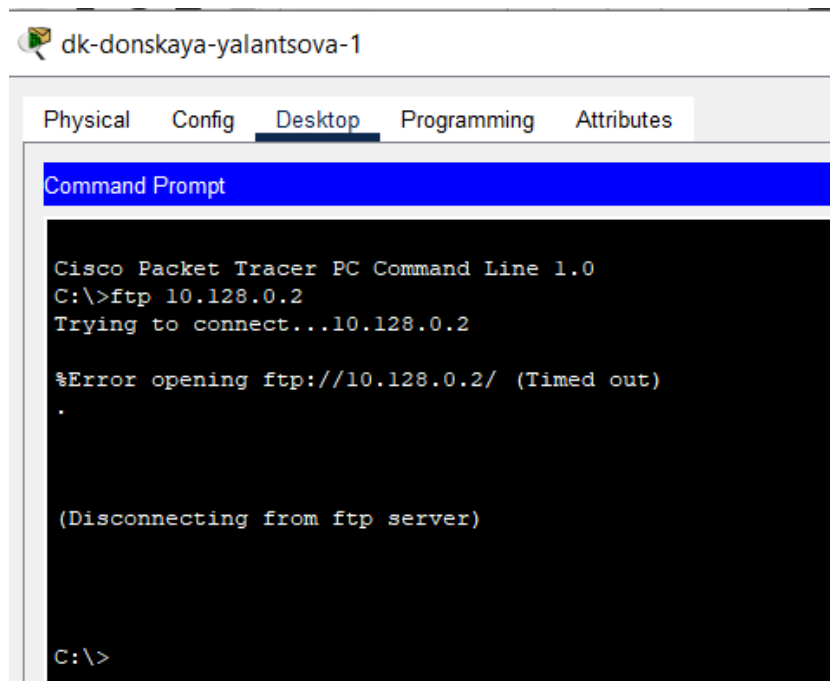


Рис. 3.8: Проверка доступа к web-серверу по протоколу FTP с устройства dk-donskaya-1

4. Настройка доступа к файловому серверу(рис. 3.9).

```
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. 3.9: Настройка доступа к файловому серверу

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 доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

5. Настройка доступа к почтовому серверу(рис. 3.10).

```
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. 3.10: Настройка доступа к почтовому серверу

Здесь: 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 серверу по протоколам POP3 и SMTP.

6. Настройка доступа к DNS-серверу(рис. 3.11).

```
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. 3.11: Настройка доступа к DNS-серверу

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.

Проверм доступность web-сервера (через браузер) не только по ip-адресу, но и по имени (рис. 3.12, 3.13).

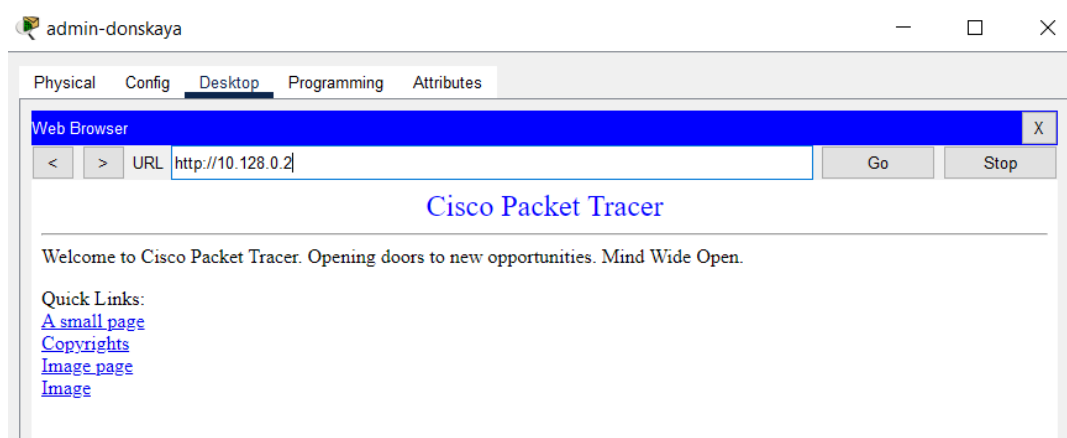


Рис. 3.12: Проверка доступа к web-серверу по ip-адресу

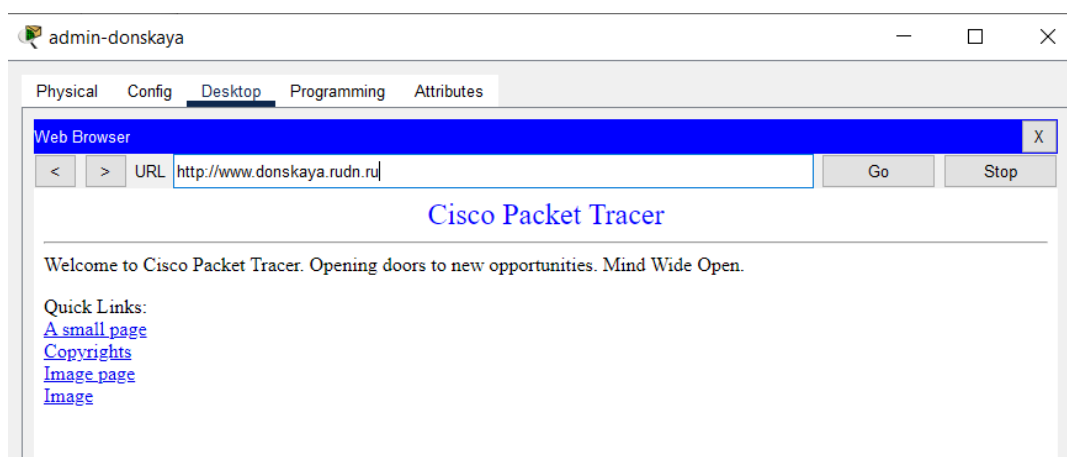


Рис. 3.13: Проверка доступа к web-серверу по имени

7. Разрешение icmp-запросов (рис. 3.14).

```
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. 3.14: Разрешение icmp-запросов

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 `sh access-lists`.

8. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору

msk-donskaya-yalantsova-gw-1 является входящим трафиком)(рис. 3.15).

```
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 other-in
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.104
msk-donskaya-yalantsova-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-yalantsova-gw-1(config-subif)#
```

Рис. 3.15: Настройка доступа для сети Other

Здесь: в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом 0.128.6.200 на любые действия (any); к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in).

9. Настройка доступа администратора к сети сетевого оборудования(рис. 3.16).

```
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. 3.16: Настройка доступа администратора к сети сетевого оборудования

Здесь: в списке контроля доступа management-out указано (в качестве комментария-напоминания remark admin), что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключается список прав доступа management-out и применяется к исходящему трафику (out).

Перейдем к выполнению самостоятельной работы

Проверим доступность устройств с помощью команды ping. С устройства der-donskaya-1 пингуются серверы и другие оконечные устройства, однако доступ к сетевому оборудованию запрещен, а также нет доступа по ftp(рис. 3.17, 3.18).

```
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. 3.17: Проверка правил доступа для оконечного устройства на примере der-donskaya-1 с помощью команды ping

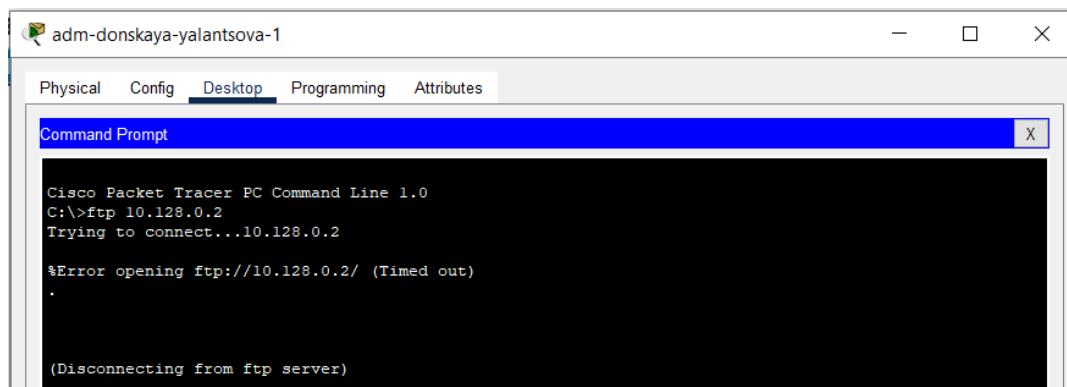


Рис. 3.18: Проверка правил доступа для оконечного устройства на примере der-donskaya-1 с помощью протокола ftp

С устройства администратора есть доступ ко всем устройствам сети по іспр-запросам, а также есть доступ к web-серверу по ftp(рис. 3.19, 3.20).

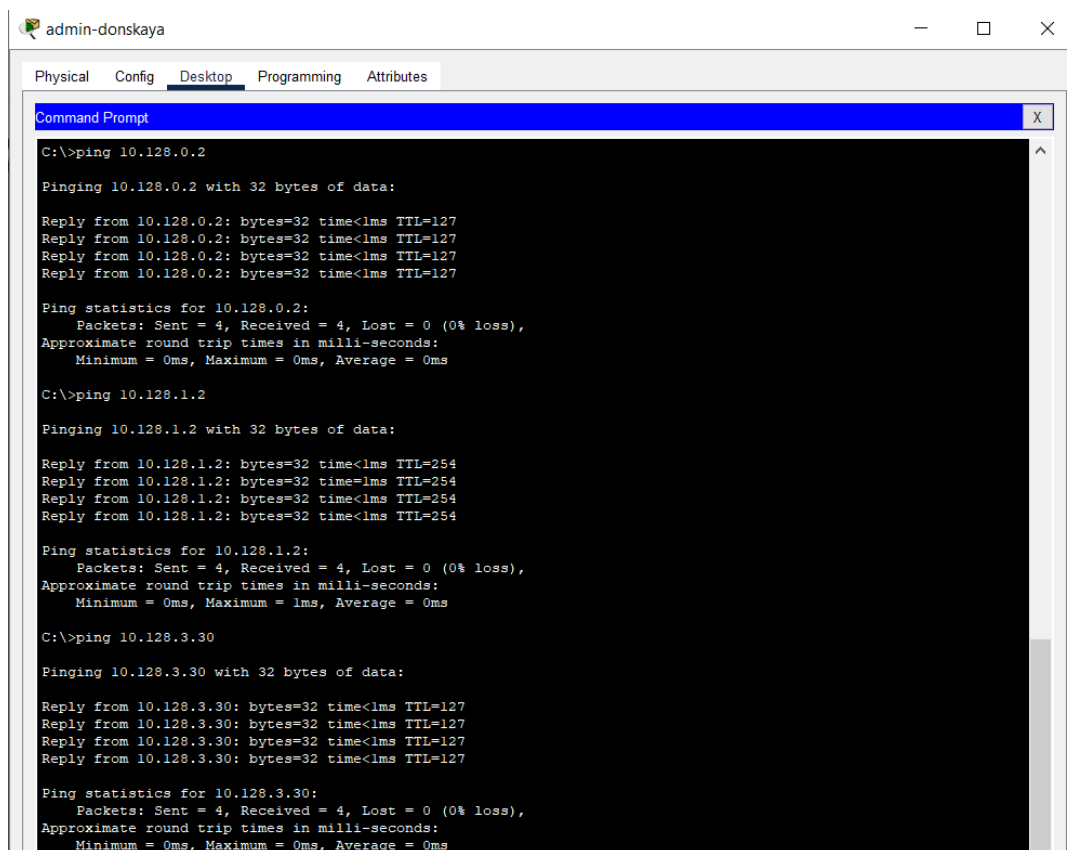


Рис. 3.19: Проверка правил доступа для администратора с помощью команды ping

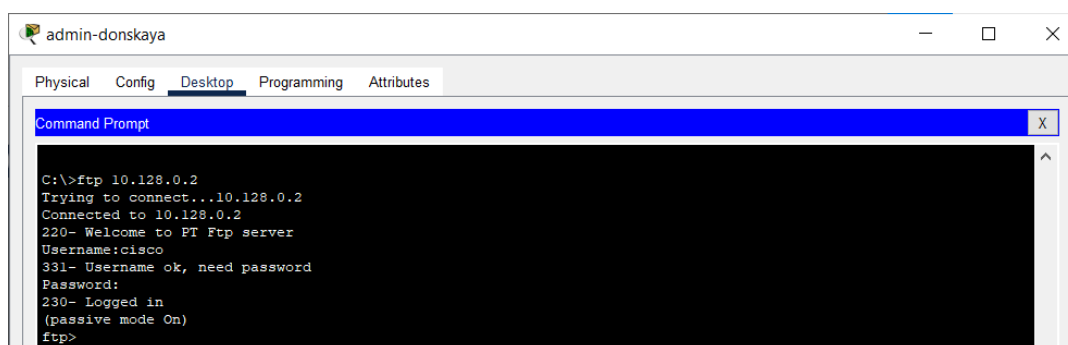


Рис. 3.20: Проверка правил доступа для администратора с помощью протокола ftp

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской. А именно дадим дополнительный доступ для администратора по протоколам Telnet и FTP, настроим доступ для сети Other и настроим доступ к сети сетевого оборудования(рис. 3.21).

The screenshot shows a network device's CLI interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the IOS Command Line Interface. The user has entered the following commands:

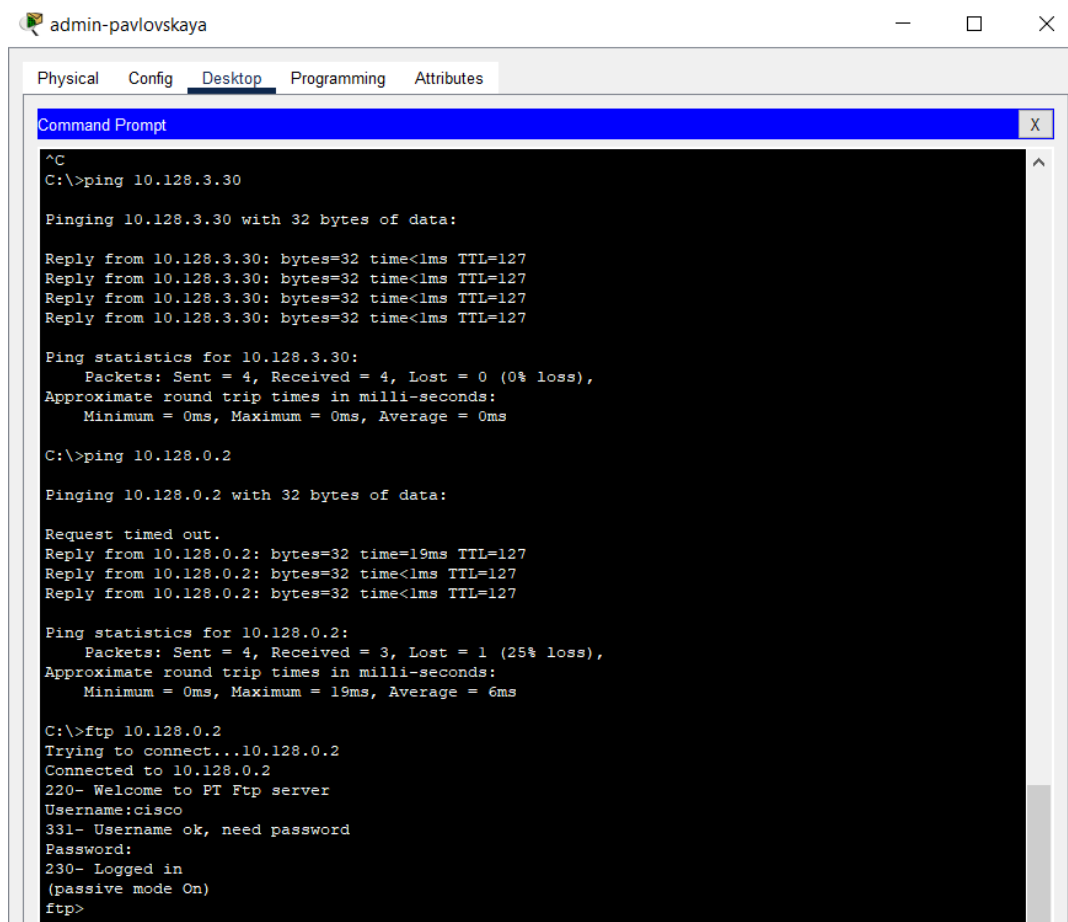
```
msk-donskaya-yalantsova-gw-1#conf t
msk-donskaya-yalantsova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
% Incomplete command.
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 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
wr mem
Building configuration...
[OK]
msk-donskaya-yalantsova-gw-1#sh access-lists
```

The output shows the configuration of three extended IP 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 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))
 - 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 ip host 10.128.6.200 10.128.1.0 0.0.0.255 (8 match(es))

Рис. 3.21: Настройка прав администратора на Павловской

Проверим корректность внесенных прав доступа(рис. 3.22).



```
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=19ms 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 = 19ms, 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 Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Рис. 3.22: Проверка правил доступа для администратора на Павловской

Итоговый проект выглядит следующим образом (рис. 3.23).

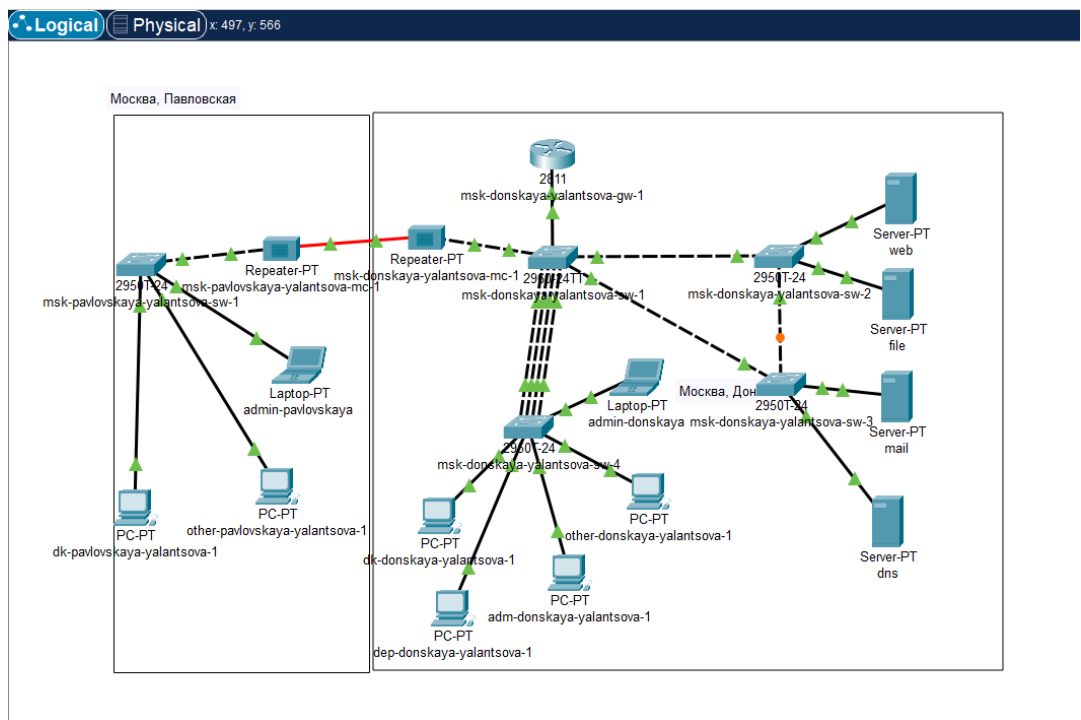


Рис. 3.23: Схема сети в логической рабочей области Packet Tracer

4 Выводы

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

5 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Указать протокол в конце записи команды `permit`. Примеры:

```
permit tcp any host 10.128.0.3 range 20 ftp
```

```
permit tcp any host 10.128.0.4 eq smtp
```

2. Как задать действие правила сразу для нескольких портов?

Нужно использовать команду `interface range` и порты через дефис.

3. Как узнать номер правила в списке прав доступа?

С помощью команды `show access-lists`.

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

Необходимо указать права доступа с номерами в нужном порядке, используя команду `access-list <Номер в списке> permit`.