

# **Лабораторная работа № 10**

**Настройка списков управления доступом (ACL)**

Коннова Татьяна Алексеевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Самостоятельная работа</b>	<b>12</b>
<b>5</b>	<b>Выводы</b>	<b>13</b>
<b>6</b>	<b>Контрольные вопросы</b>	<b>14</b>

## Список иллюстраций

3.1	Размещение ноутбука администратора в сети other-donskaya-1 . .	6
3.2	Задание статического ip-адреса ноутбуку admin . . . . .	7
3.3	Задание gateway-адреса и адреса DNS-сервера ноутбуку admin . .	7
3.4	Настройка доступа к web-серверу по порту tcp 80 . . . . .	8
3.5	Добавление списка управления доступом к интерфейсу . . . . .	8
3.6	Настройка дополнительного доступа для администратора по протоколам Telnet и FTP . . . . .	8
3.7	Настройка доступа к файловому серверу . . . . .	9
3.8	Настройка доступа к почтовому серверу . . . . .	9
3.9	Настройка доступа к DNS-серверу . . . . .	9
3.10	Разрешение icmp-запросов . . . . .	10
3.11	Просмотр строк в списке контроля доступа . . . . .	10
3.12	Настройка доступа для сети Other . . . . .	10
3.13	Настройка доступа администратора к сети сетевого оборудования	11

# **1 Цель работы**

Освоить настройку прав доступа пользователей к ресурсам сети.

## 2 Задание

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 Павловской.

4. При выполнении работы необходимо учитывать соглашение об именовании.

### 3 Выполнение лабораторной работы

В рабочей области проекта подключим ноутбук администратора с именем admin к сети other-donskaya-1 (рис. 3.1) 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. 3.2), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 3.3).

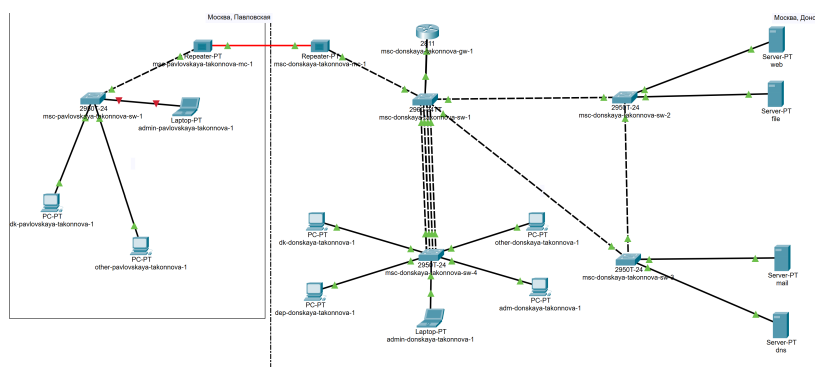


Рис. 3.1: Размещение ноутбука администратора в сети other-donskaya-1

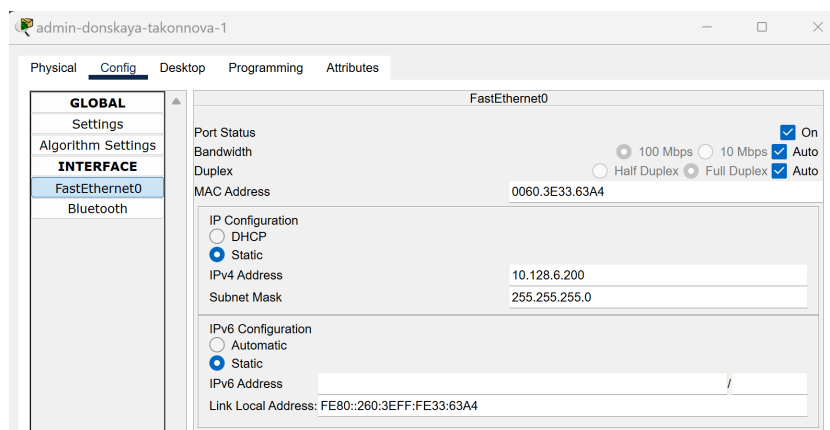


Рис. 3.2: Задание статического ip-адреса ноутбуку admin

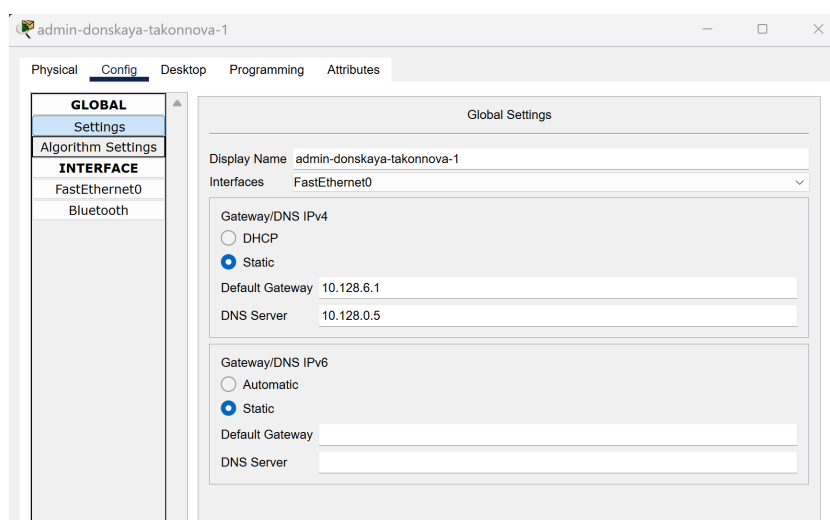


Рис. 3.3: Задание gateway-адреса и адреса DNS-сервера ноутбуку admin

Проверим что у ноутбука корректно работает соединение через пингование разных устройств сети, например серверов.

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 сначала мы надо давать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny).

Настроим доступ к web-серверу по порту tcp 80 (рис.3.4). Мы создаем 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, а также даем 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.

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

Рис. 3.4: Настройка доступа к web-серверу по порту tcp 80

Добавим список управления доступом к интерфейсу (рис.3.5). К интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out).

```
msc-donskaya-takonnova-gw-1(config-ext-nacl)#interface f0/0.3
msc-donskaya-takonnova-gw-1(config-subif)#ip access group servers out out
% Invalid input detected at '^' marker.
msc-donskaya-takonnova-gw-1(config-subif)#ip access group servers-out out
% Invalid input detected at '^' marker.
msc-donskaya-takonnova-gw-1(config-subif)#ip access-group servers-out out
msc-donskaya-takonnova-gw-1(config-subif)#
```

Рис. 3.5: 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. При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по IP-адресу web-сервера.

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP (рис.3.6). 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.

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

Рис. 3.6: 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. 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.

Настроим доступ к файловому серверу (рис.3.7). 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).

```
msc-donskaya-takonnova-gw-1(config-ext-nacl)#ip access-list extended servers-out
msc-donskaya-takonnova-gw-1(config-ext-nacl)#remark file
msc-donskaya-takonnova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
msc-donskaya-takonnova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msc-donskaya-takonnova-gw-1(config-ext-nacl)#
```

Рис. 3.7: Настройка доступа к файловому серверу

Настроим доступ к почтовому серверу (рис.3.8). 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.

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

Рис. 3.8: Настройка доступа к почтовому серверу

Настроим доступ к DNS-серверу (рис.3.9). 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-takonnova-gw-1(config-ext-nacl)#ip access-list extended servers-out
msc-donskaya-takonnova-gw-1(config-ext-nacl)#remark dns
msc-donskaya-takonnova-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
msc-donskaya-takonnova-gw-1(config-ext-nacl)#
```

Рис. 3.9: Настройка доступа к DNS-серверу

Разрешим icmp-запросы (рис.3.10).

```
msc-donskaya-takonnova-gw-1(config-ext-nacl)#ip access-list extended servers-out
msc-donskaya-takonnova-gw-1(config-ext-nacl)#1 permit icmp any any
msc-donskaya-takonnova-gw-1(config-ext-nacl)#
```

---

Рис. 3.10: Разрешение icmp-запросов

Посмотрим номера строк правил в списке контроля доступа (рис.3.11).

```
msc-donskaya-takonnova-gw-1#show access lists
```

Рис. 3.11: Просмотр строк в списке контроля доступа

Настроим доступ для сети Other (рис.3.12). Наложим ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком. В списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом 10.128.6.200 на любые действия (any); к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in).

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

msc-donskaya-takonnova-gw-1(config)#ip access-list extended other-in
msc-donskaya-takonnova-gw-1(config-ext-nacl)##remark admin
% Invalid input detected at '^' marker.

msc-donskaya-takonnova-gw-1(config-ext-nacl)#remark admin
msc-donskaya-takonnova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msc-donskaya-takonnova-gw-1(config-ext-nacl)#exit
msc-donskaya-takonnova-gw-1(config)#interface f0/0.104
msc-donskaya-takonnova-gw-1(config-subif)#ip access group other in in
% Invalid input detected at '^' marker.

msc-donskaya-takonnova-gw-1(config-subif)#ip access-group other-in in
msc-donskaya-takonnova-gw-1(config-subif)#
```

---

Рис. 3.12: Настройка доступа для сети Other

Настроим доступ администратора к сети сетевого оборудования (рис.3.13). 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 интер-

фейсу f0/0.2 подключается список прав доступа management-out и применяется к исходящему трафику (out).

```
msc-donskaya-takonnova-gw-1(config-subif)#ip access-group other-in in
msc-donskaya-takonnova-gw-1(config-subif)#ip access list extended management out
^
% Invalid input detected at '^' marker.

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

msc-donskaya-takonnova-gw-1(config-subif)#ip access-group management-out out
msc-donskaya-takonnova-gw-1(config-subif)#
```

Рис. 3.13: Настройка доступа администратора к сети сетевого оборудования

## 4 Самостоятельная работа

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

Разместим в рабочей области ноутбук admin-pavlovskaya на Павловской.

После очередных попыток настройки, индикация у меня, к сожалению, так и не стала “зелёной”.

## **5 Выводы**

В процессе выполнения данной лабораторной работы я получила практические навыки настройки прав доступа пользователей к ресурсам сети.

## 6 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Например, `permit tcp any host 10.128.0.4 eq pop3`.

2. Как задать действие правила сразу для нескольких портов?

Для этого нужна команда `interface range`.

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?

Команда `access-list <номер в списке> permit`.