

Laboratory work report №10 administration of local systems

Настройка списков управления доступом (ACL)

Выполнил: Леснухин Даниил Дмитриевич,
НПИБд-02-22, 1132221553

Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

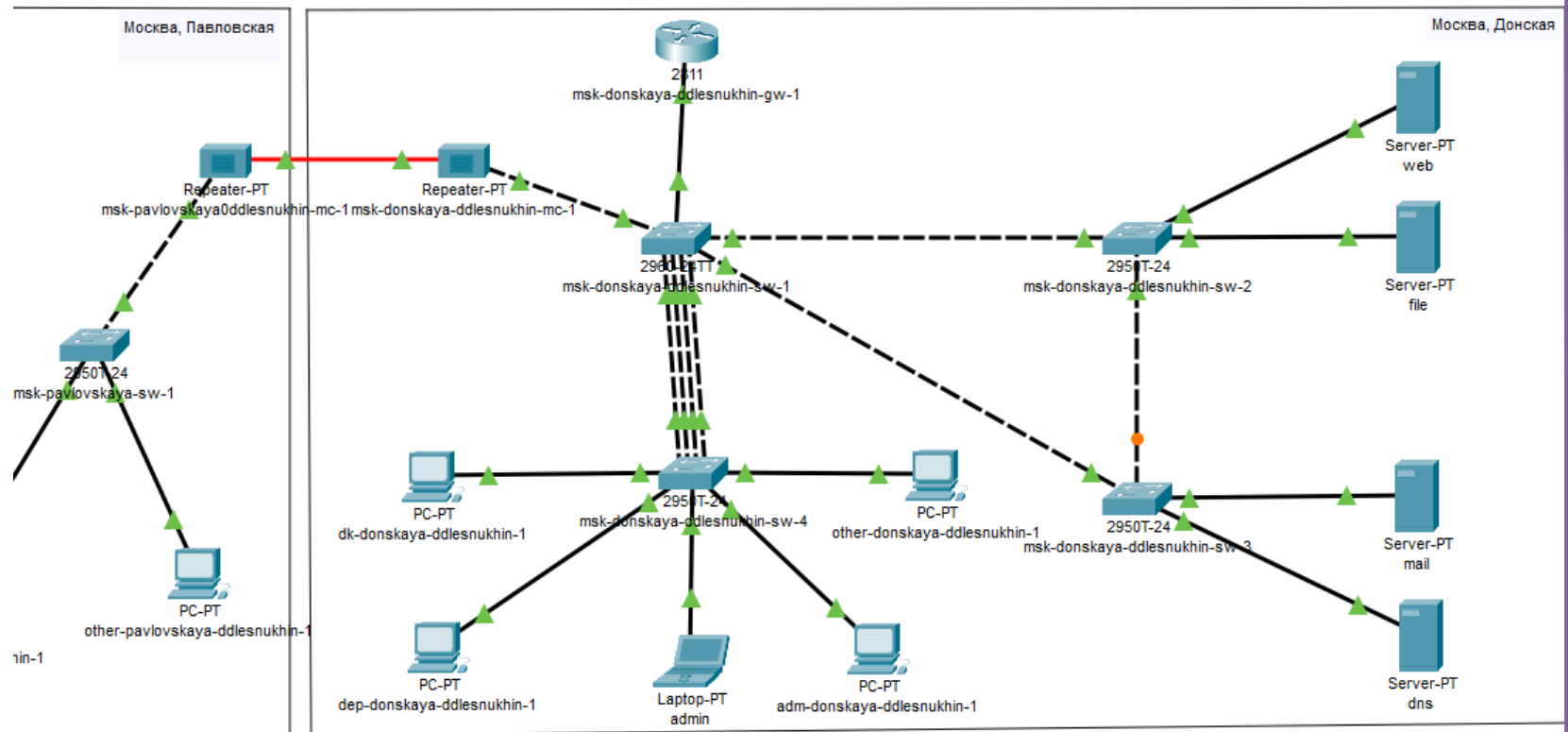
Выполнение работы

1. Откроем проект с названием `lab_PT-09.pkt` и сохраним под названием `lab_PT-10.pkt`. После чего откроем его для дальнейшего редактирования.
Рис. 1.1. Открытие проекта `lab_PT-10.pkt` # Изменение топологии
2. В рабочей области проекта подключите ноутбук администратора с именем `admin` к сети `other-donskaya-1` с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоедините ноутбук к порту 24 коммутатора `msk-donskaya-sw-4` и присвойте 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. 1.2. Формирование резервного соединения между коммутаторами. # Статический адрес
3. Указываем статический адрес `10.128.6.200` и gateway адрес `10.128.6.1` Рис. 1.3. Настройка ноутбука `admin`.
4. После чего мы пропируем. 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. Различают стандартные (standard) и расширенные (extended) списки контроля доступа (Access Control List, ACL). Стандартные ACL проверяют только адрес источника трафика, расширенные — адрес как источника, так и получателя, тип протокола и TCP/UDP порты.

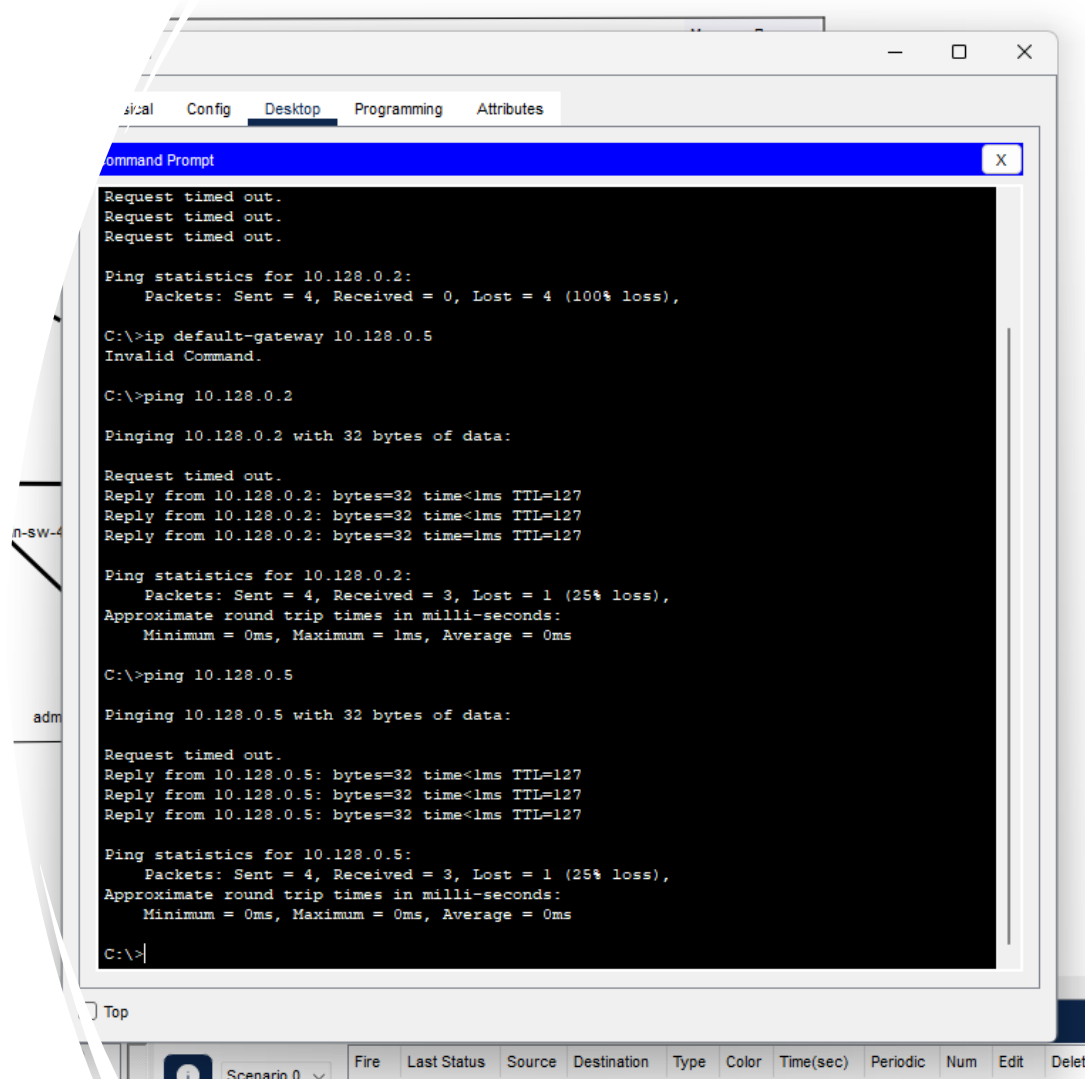
Рис. 1.4. Проверяем настройку адресов ноутбука `admin`

Рис. 1.4. Проверяем настройку адресов ноутбука `admin`

В рабочей области проекта подключите 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 подсоедините ноутбук к порту 24 коммутатора `msk-donskaya-sw-4` и присвойте ему статический адрес `10.128.6.200`, указав в качестве gateway-адреса `10.128.6.1` и адреса DNS-сервера `10.128.0.5`



- После чего мы пропингуем. Права доступа пользователей сети будем настраивать на маршрутизаторе msk-donskaya-gw-1, поскольку именно через него проходит весь трафик сети.



The screenshot shows a Windows Command Prompt window with the following text:

```
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:\>ip default-gateway 10.128.0.5
Invalid Command.

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<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:\>
```

The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active. The window title is 'Command Prompt'. The taskbar at the bottom shows 'Scenario 0' and various system icons.

Настройка web-сервера

Далее настроим доступ к web-серверу по порту tcp 80 Здесь :

1. Создадим список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик)
2. Укажем (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером;
3. Дадим 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

Рис. 1.5. Настройка доступа к web-серверу по порту tcp 80.

Рис. 1.5. Настройка доступа к web-серверу по порту tcp 80.

К интерфейсу f0/0.3 подключаем список прав доступа serversout и применяем к исходящему трафику (out). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера)

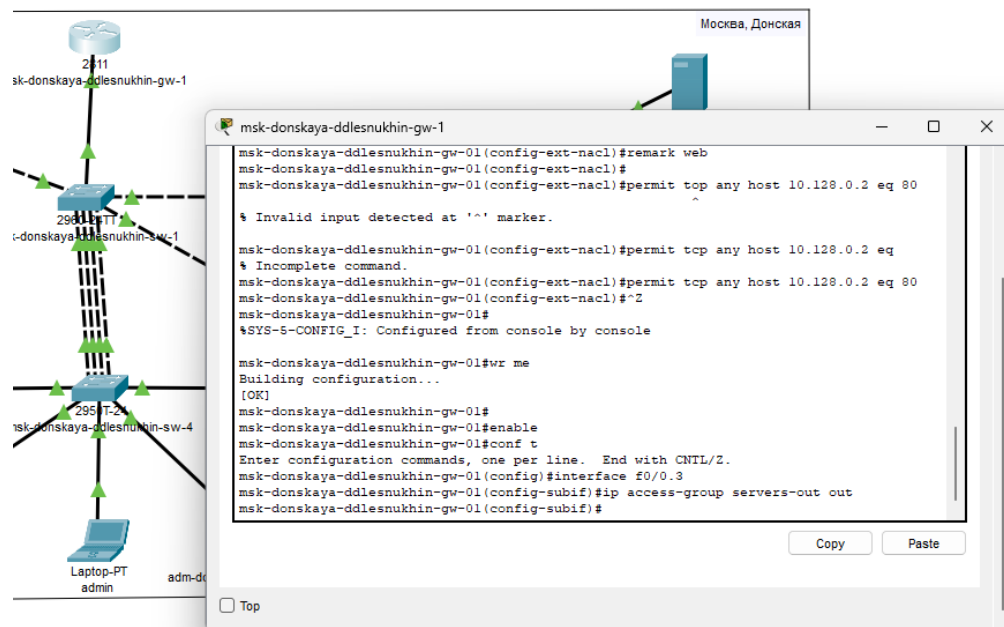


Рис. 1.6. Подключение списка прав доступа serversout`.

5. Проверка демонстрации недоступности web-сервера при использовании команды ping по ip-адресу web-сервера.

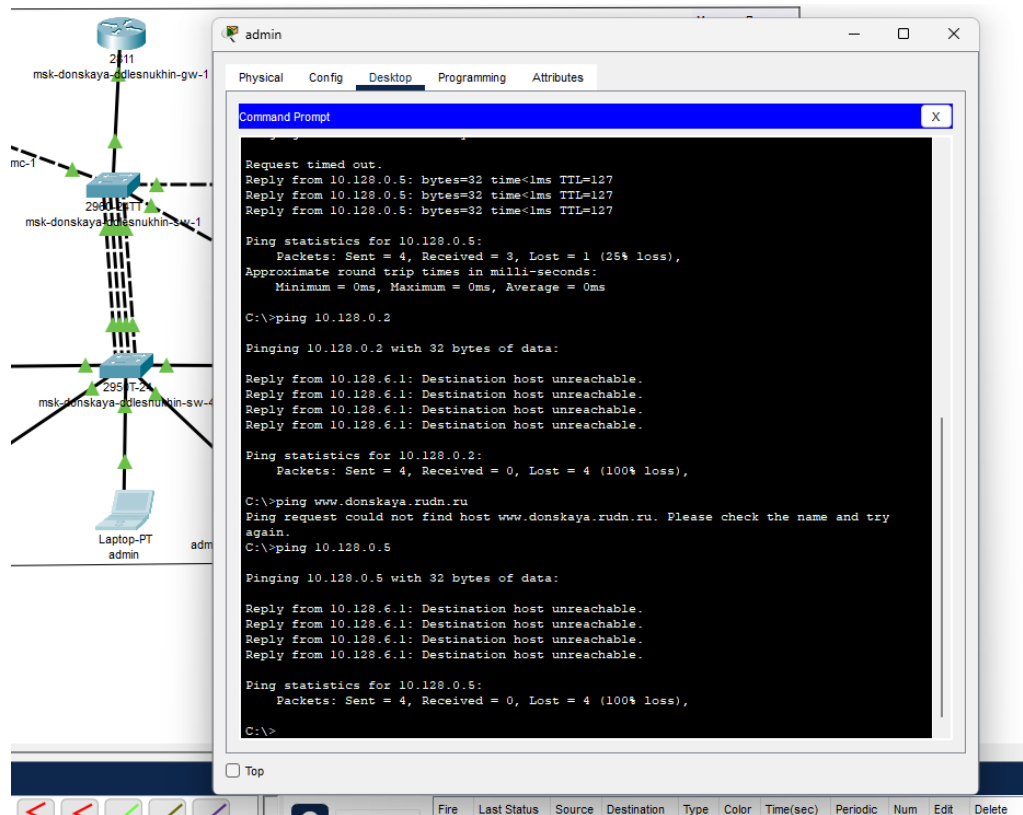


Рис. 1.7. Проверка командой ping.

Добавляем дополнительный доступ для администратора по протоколам Telnet и FTP:

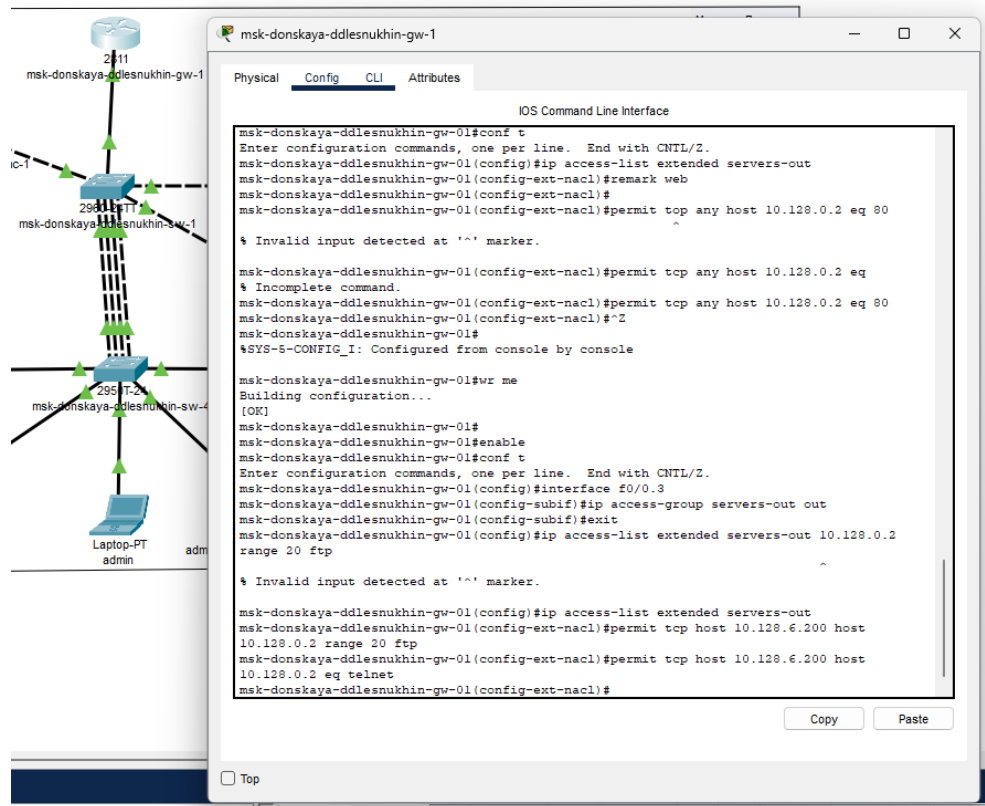


Рис. 1.9. Добавляем дополнительный доступ для администратора по протоколам Telnet и FTP.

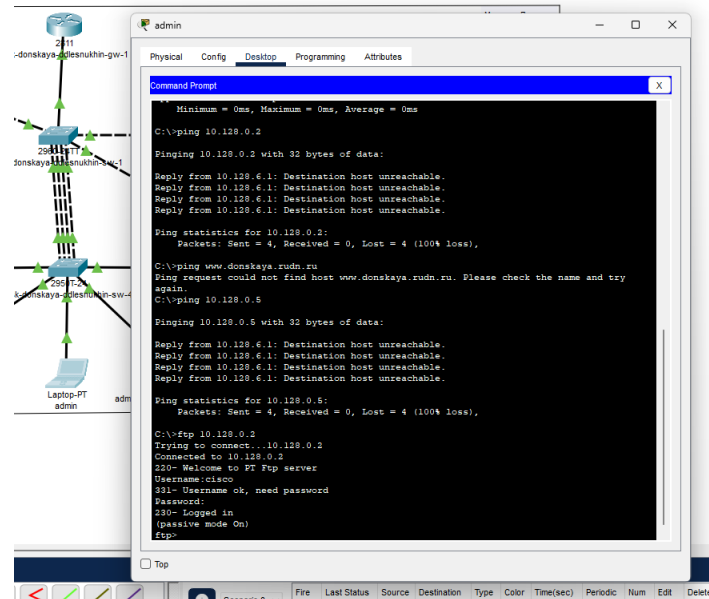


Рис.1.9

#

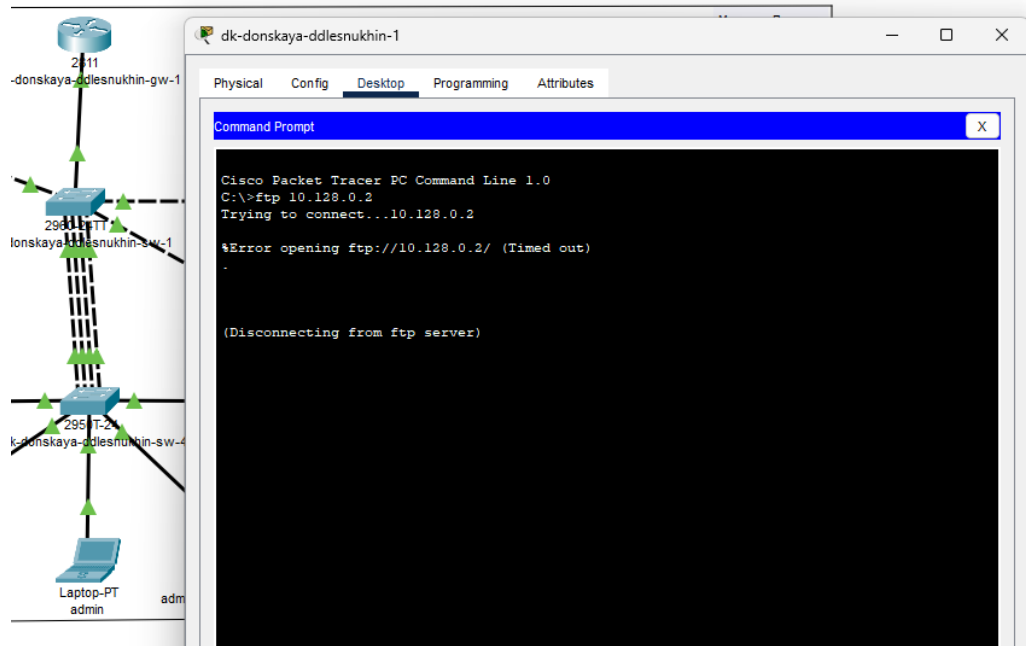


Рис. 2

Настройка доступа к серверам

Настроим доступ к файловому, почтовому и web серверу. Здесь:

1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark file), что следующие ограничения
предназначены для работы с file-сервером;
2. Всем узлам внутренней сети (10.128.0.0) разрешим доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования;
3. Любым узлам разрешим доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

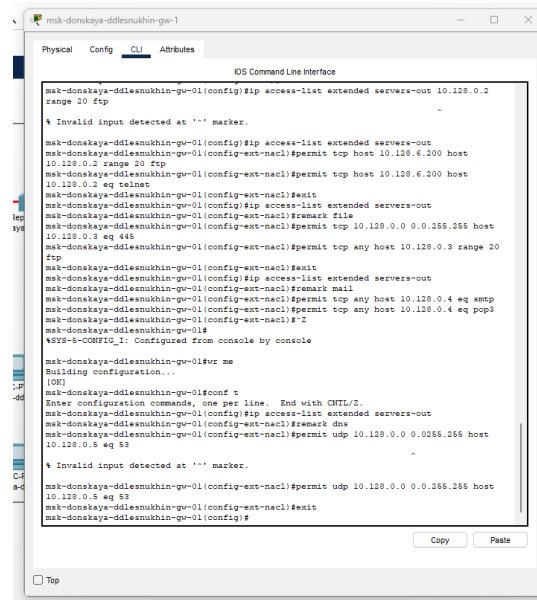


Рис. 1.10. Доступ к серверам .

Разрешим icmp-запросы. Здесь:

Демонстрируем 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 `show access -lists` (Рис. 1.17):

```
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#exit
msk-donskaya-ddlesnukhin-gw-01(config)#ip access-list extended servers-out
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#1 permit icmp any any
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#^Z
msk-donskaya-ddlesnukhin-gw-01#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-ddlesnukhin-gw-01#wr me
Building configuration...
[OK]
msk-donskaya-ddlesnukhin-gw-01#
```

Copy

Paste

 Top

Рис. 1.12.

```
msk-donskaya-ddlesnukhin-gw-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ddlesnukhin-gw-01(config)#ip access-list extended other-in
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#remark admin
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#exit
msk-donskaya-ddlesnukhin-gw-01(config)#interface f0/0.104
msk-donskaya-ddlesnukhin-gw-01(config-subif)#ip access-group other-in in
msk-donskaya-ddlesnukhin-gw-01(config-subif)#^Z
msk-donskaya-ddlesnukhin-gw-01#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-ddlesnukhin-gw-01#wr me
Building configuration...
[OK]
msk-donskaya-ddlesnukhin-gw-01#
```

Copy

Paste

☐ Top

Рис. 1.13. Настройка доступа для сети Other .

8. Настроим доступ администратора к сети сетевого оборудования.

```
msk-donskaya-ddlesnukhin-gw-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ddlesnukhin-gw-01(config)#ip access-list extended management-out
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#remark admin
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0
0.0.0.255
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#exit
msk-donskaya-ddlesnukhin-gw-01(config)#interface f0/0.2
msk-donskaya-ddlesnukhin-gw-01(config-subif)#ip access-group management-out out
msk-donskaya-ddlesnukhin-gw-01(config-subif)#^Z
msk-donskaya-ddlesnukhin-gw-01#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-ddlesnukhin-gw-01#wr me
Building configuration...
[OK]
msk-donskaya-ddlesnukhin-gw-01#
```

Copy

Paste

☐ Top

Рис. 1.16. Настройка доступа

10. Проверим корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования

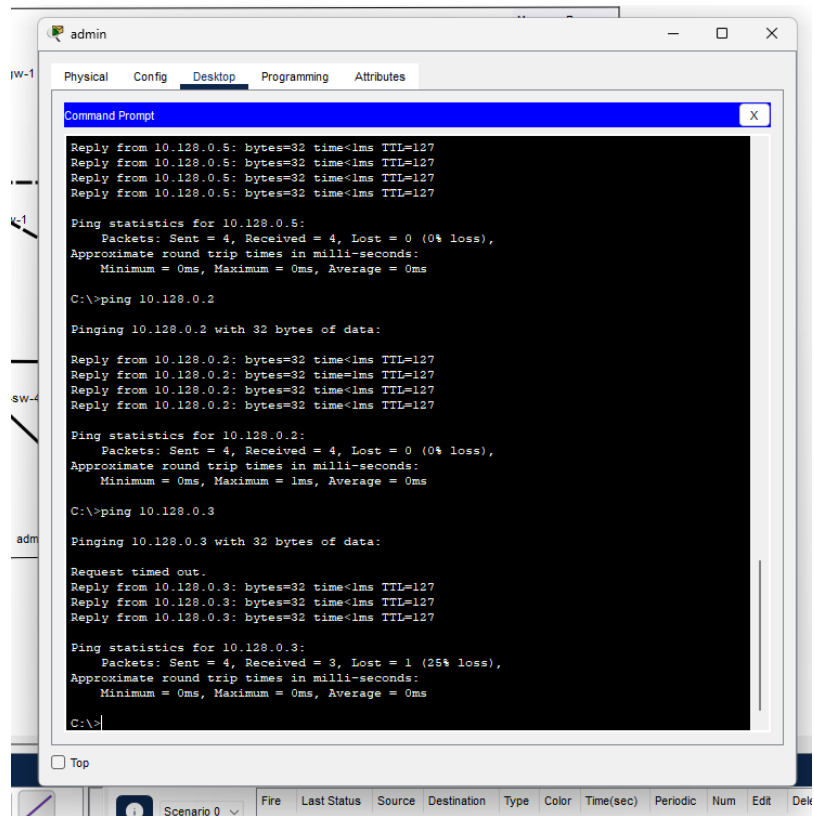


Рис. 1.18. Проверка.

Вывод

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

Ответы на контрольные вопросы

1 Как задать действие правила для конкретного протокола? – permit...

2 Как задать действие правила сразу для нескольких портов? - ... range...

3 Как узнать номер правила в списке прав доступа? – show access-lists

4 Каким образом можно изменить порядок применения правил в списке

контроля доступа? – ip access-list resequence...