

Laboratory work report №10 administration of local systems

(ACL)

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

Цель работы	3
Выполнение работы	3
Настройка web-сервера	6
	14
Ответы на контрольные вопросы	19

1	Рис. 1.3. Настройка ноутбука admin.	5
2	Рис. 1.4. Проверяем настройку адресов ноутбука admin	6
3	Рис. 1.5. Настройка доступа к web-серверу по порту tcp 80.	7
4	Рис. 1.6. Подключение списка прав доступа serversout'.	8
5	Рис. 1.7. Проверка командой ping.	9
6	Рис. 1.8. Отслеживание пакетов ICMP для web.	10
7	Рис. 1.9. Добавляем дополнительный доступ для администратора по протоколам Telnet и FTP.	11
8	Рис.1.9	12
9	Рис. 2	13
1	Рис. 1.10. Доступ к серверам	15
2	Рис. 1.12.	16
3	Рис. 1.13. Настройка доступа для сети Other	16
4	Рис. 1.16. Настройка доступа	17
5	Рис. 1.18. Проверка.	18

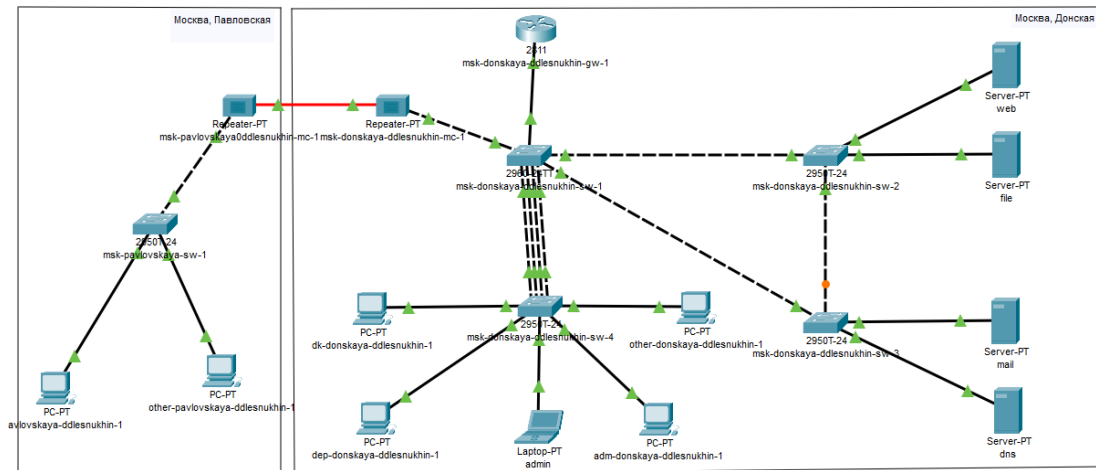
Освоить настройку прав доступа пользователей к ресурсам сети.

1. Откроем проект с названием lab_PT-09.pkt и сохраним под названием lab_PT-10.pkt. После чего откроем его для дальнейшего редактирования.



Изменение топологии

2. 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



Статический адрес

3. Указываем статический адрес 10.128.6.200 и gateway адрес 10.128.6.1

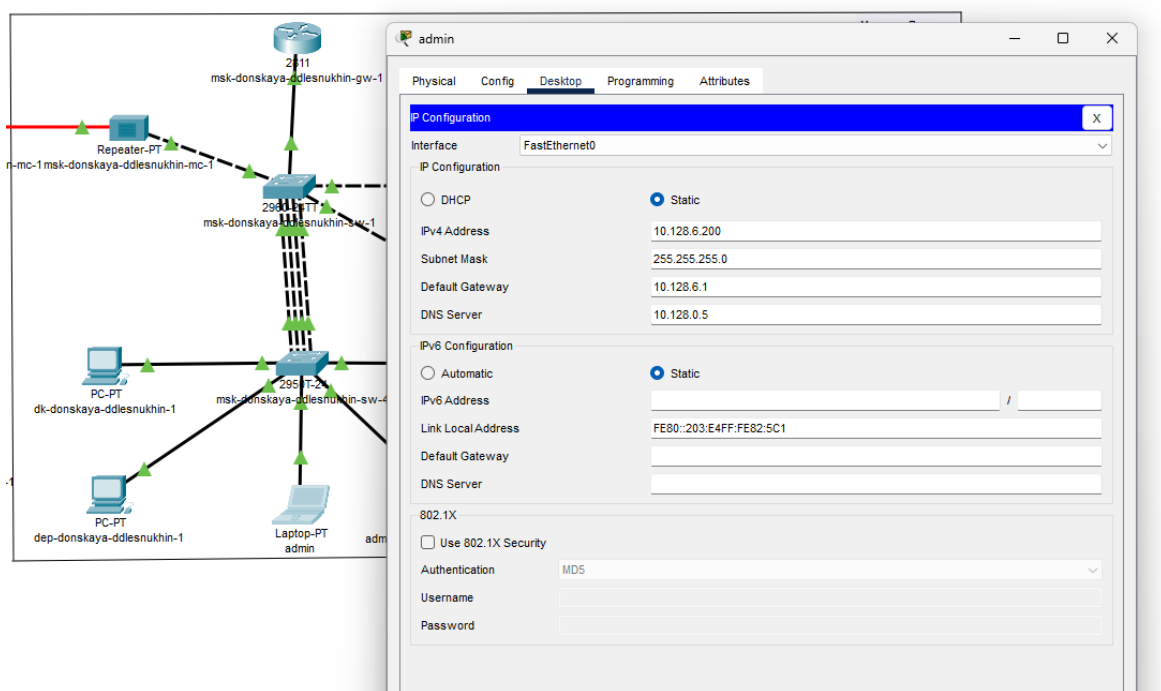


Рис. 1: Рис. 1.3. Настройка ноутбука admin.

4. После чего мы пропишем. Права доступа пользователей сети будем настраивать на маршрутизаторе msk- donsкаaya-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.

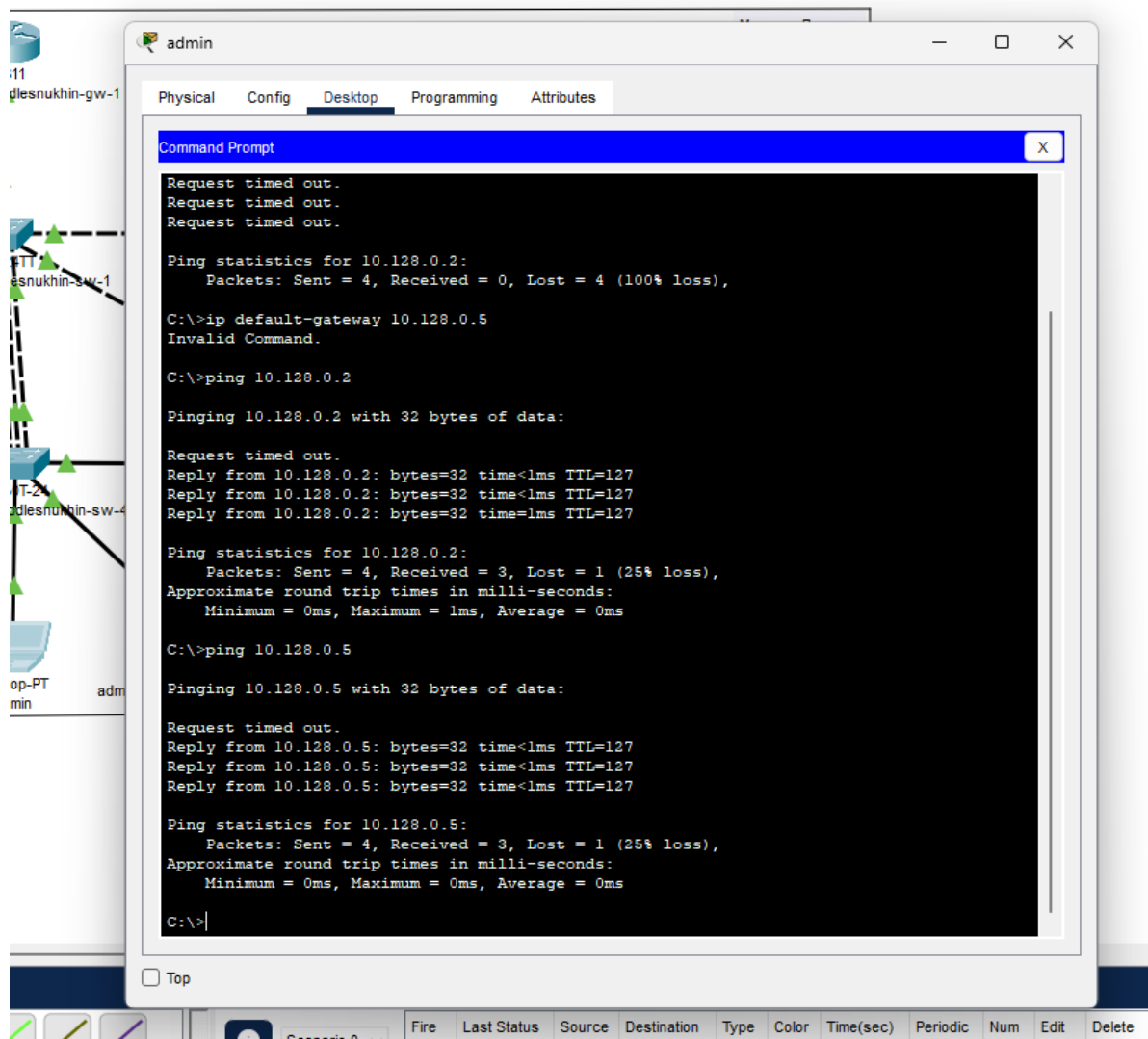


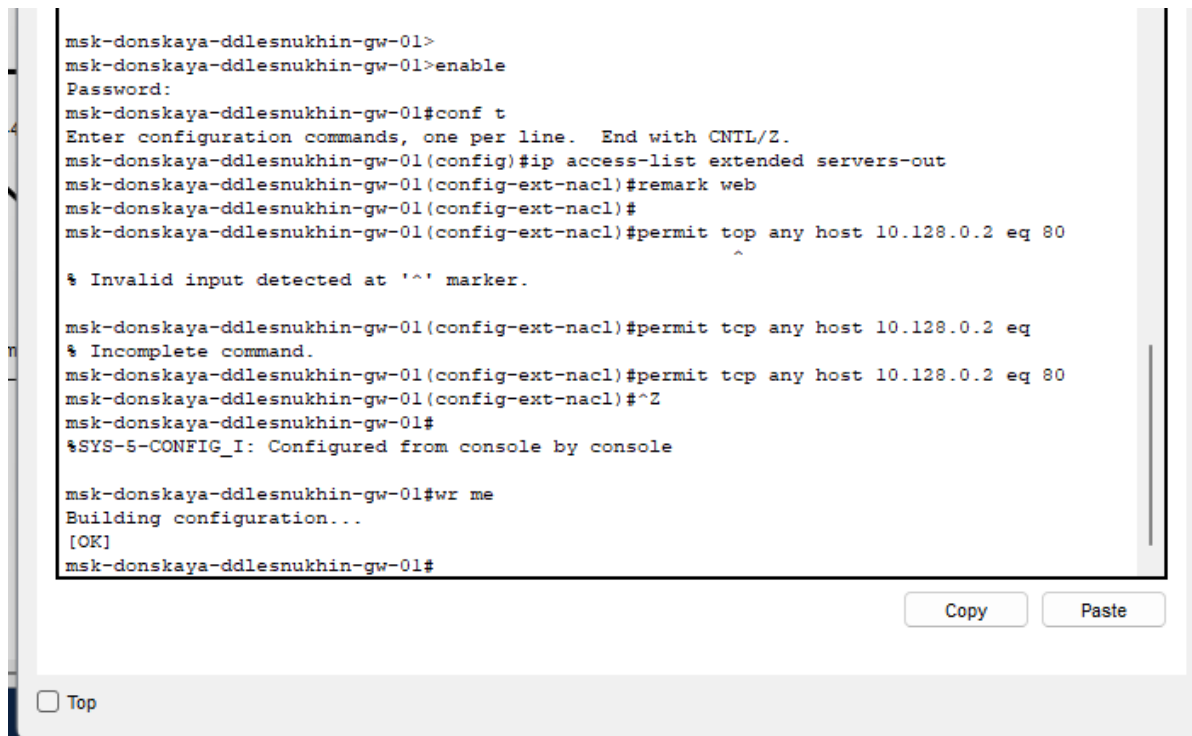
Рис. 2: Рис. 1.4. Проверяем настройку адресов ноутбука admin

web-

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



```
msk-donskaya-ddlesnukhin-gw-01>
msk-donskaya-ddlesnukhin-gw-01>enable
Password:
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 servers-out
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#remark web
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
                                     ^
% Invalid input detected at '^' marker.

msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#permit tcp any host 10.128.0.2 eq
% Incomplete command.
msk-donskaya-ddlesnukhin-gw-01(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
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. 3: 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)

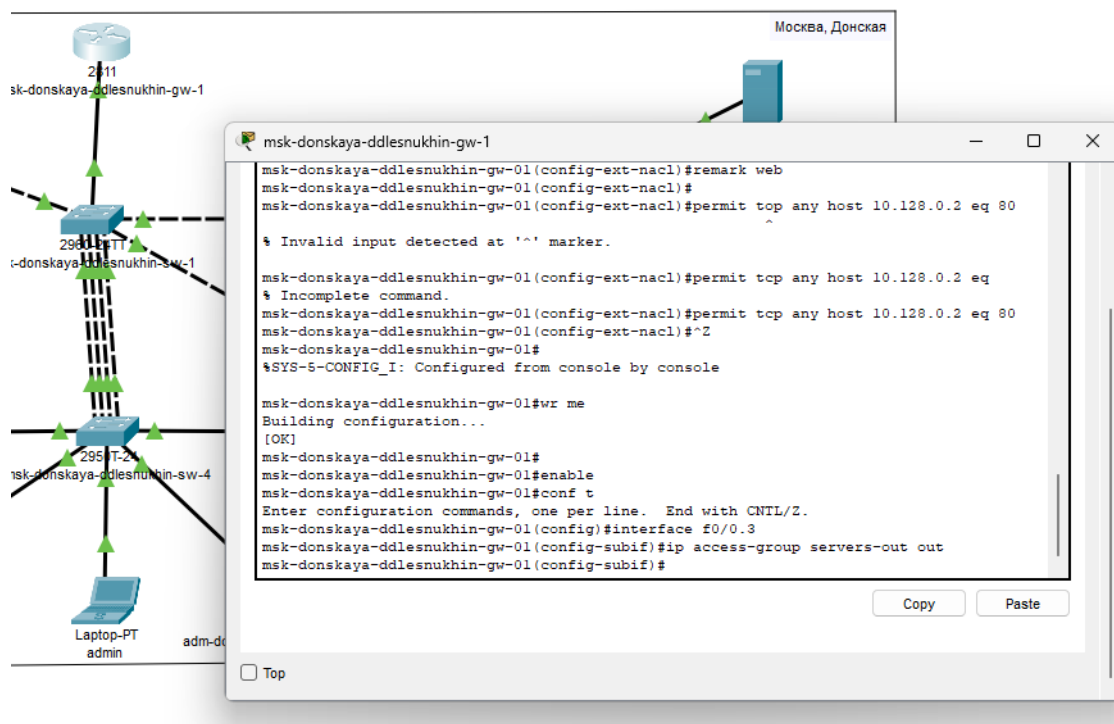


Рис. 4: Рис. 1.6. Подключение списка прав доступа serversout'.

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

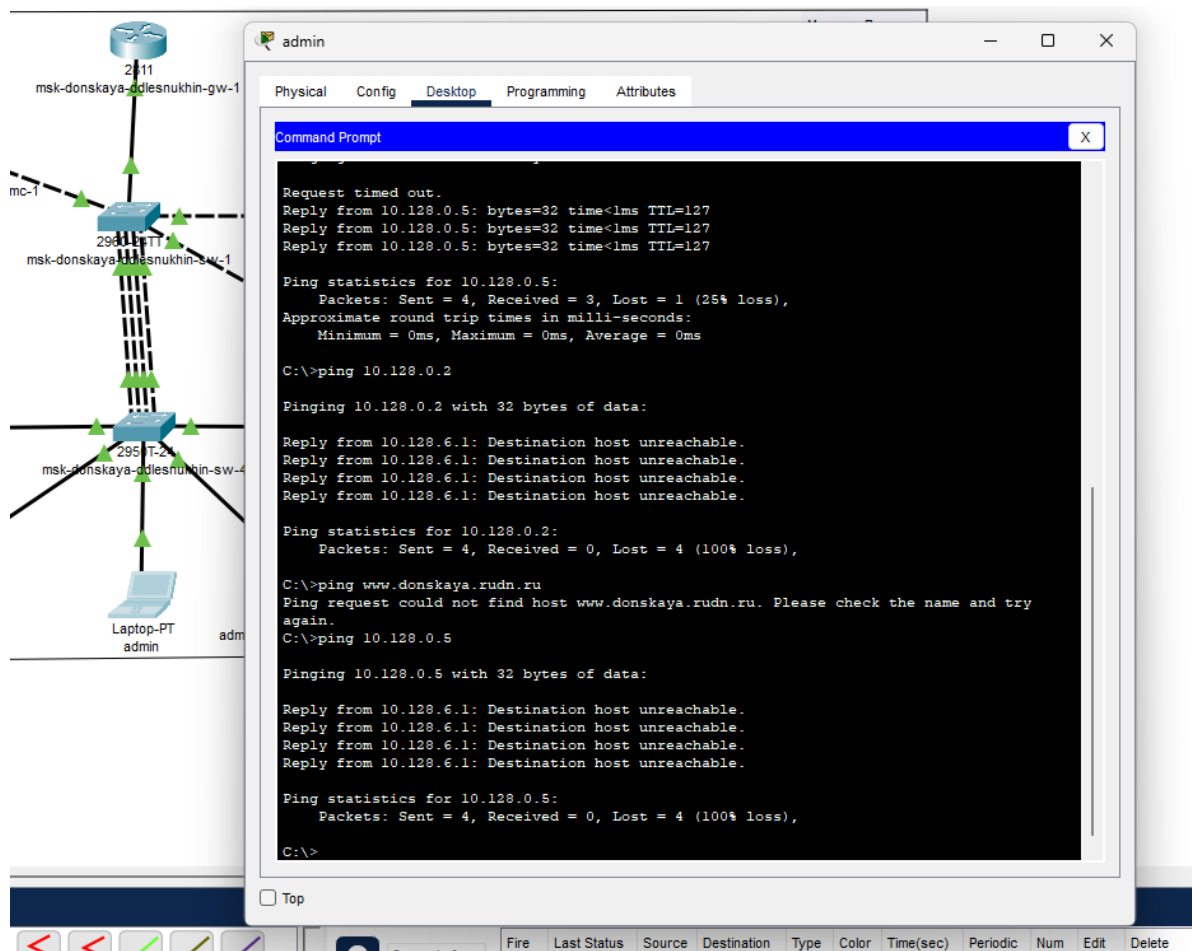


Рис. 6: Рис. 1.8. Отслеживание пакетов ICMP для web.

Добавляем дополнительный доступ для администратора по протоколам Telnet и FTP:

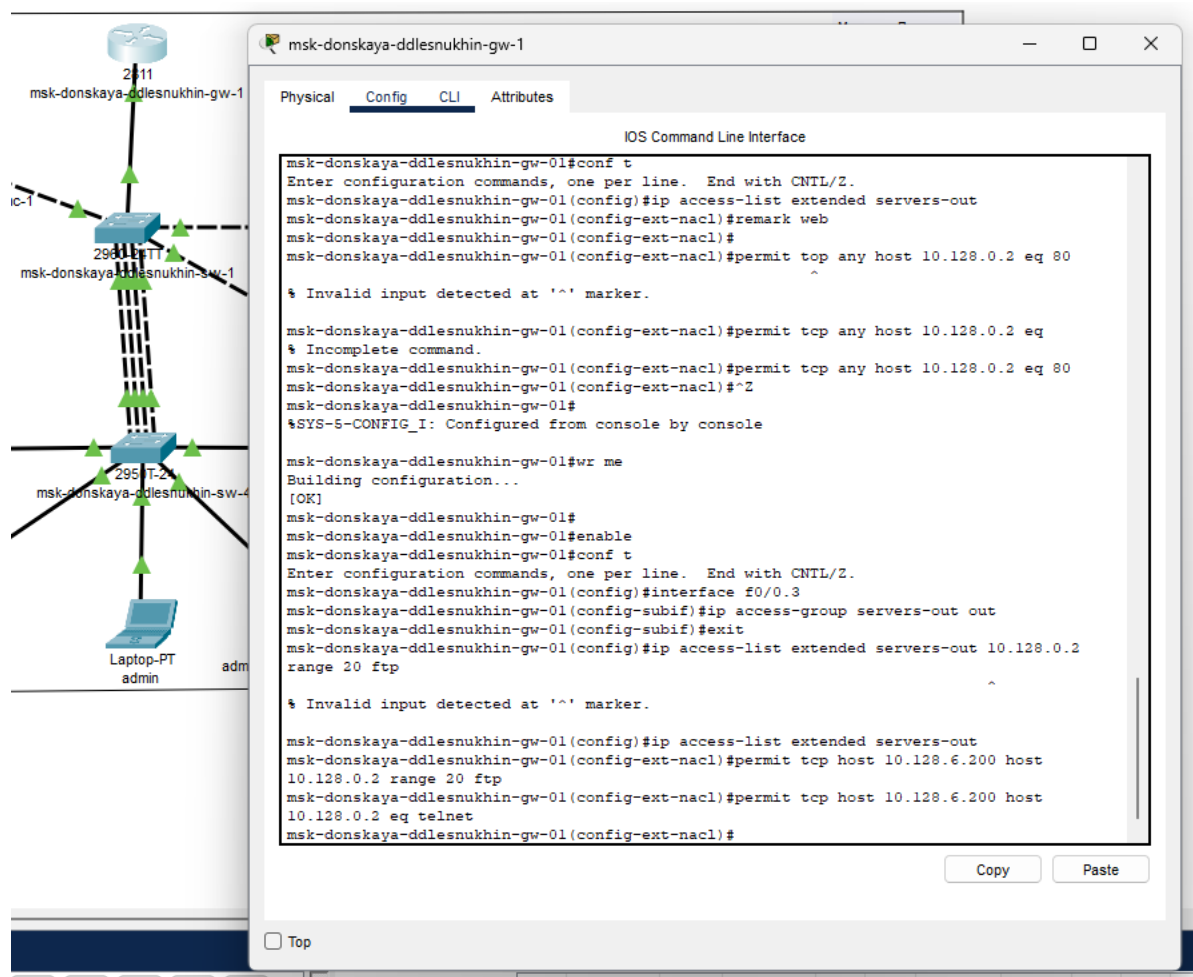


Рис. 7: Рис. 1.9. Добавляем дополнительный доступ для администратора по протоколам Telnet и FTP.

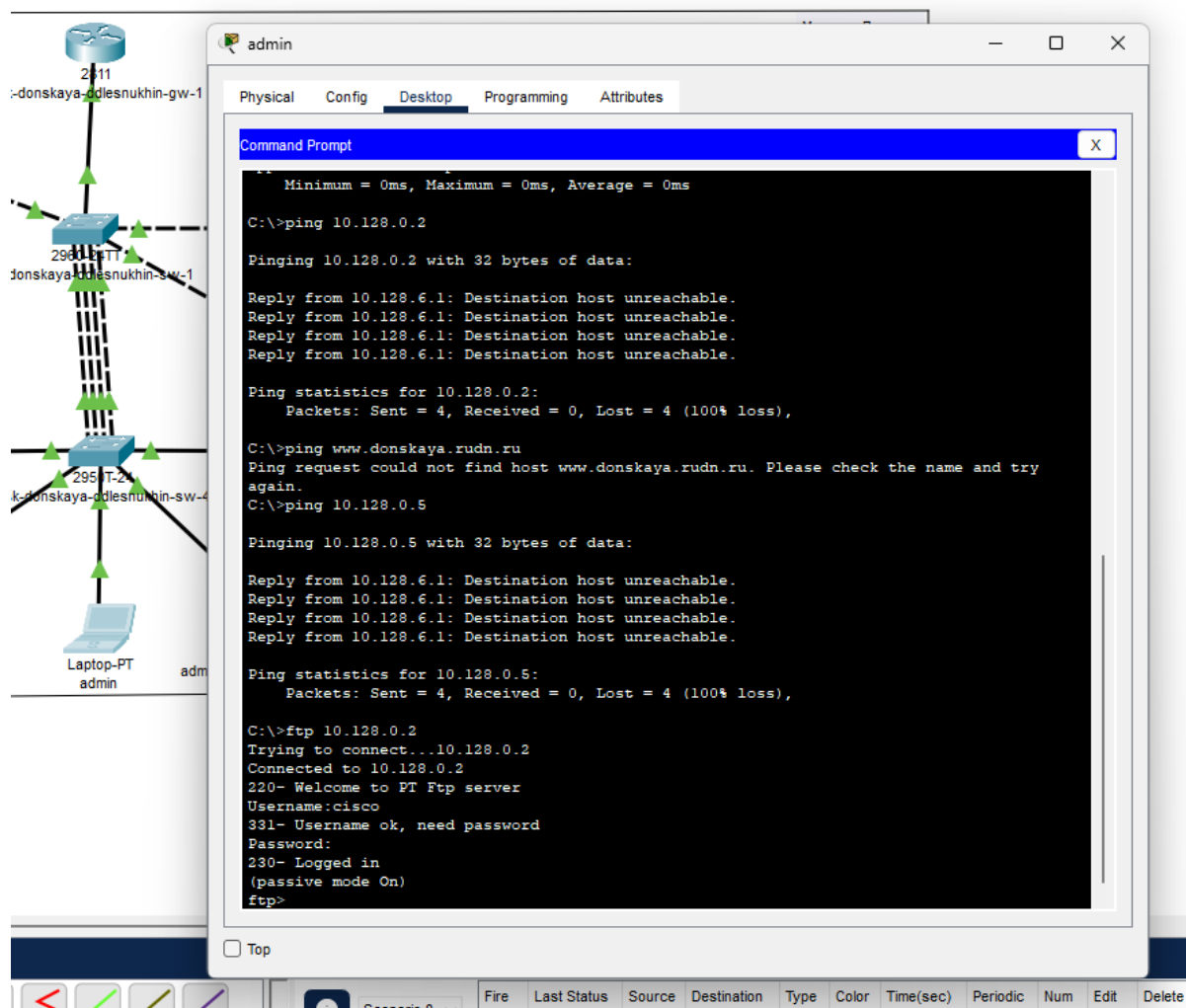


Рис. 8: Рис.1.9

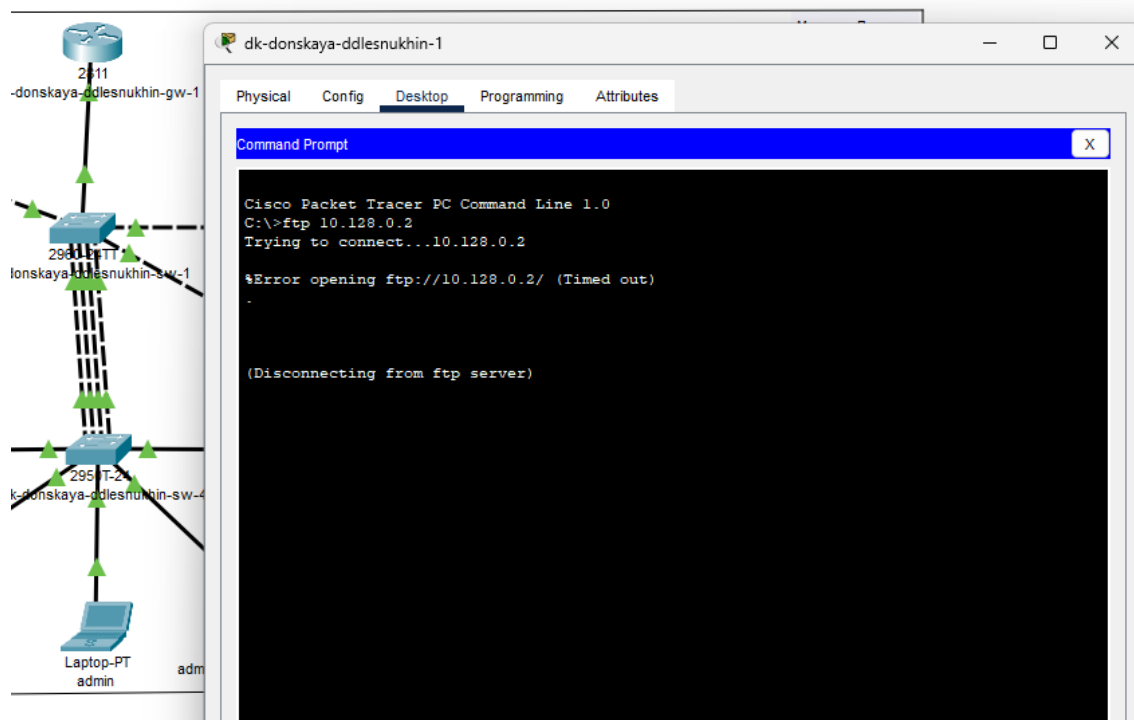


Рис. 9: Рис. 2

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).

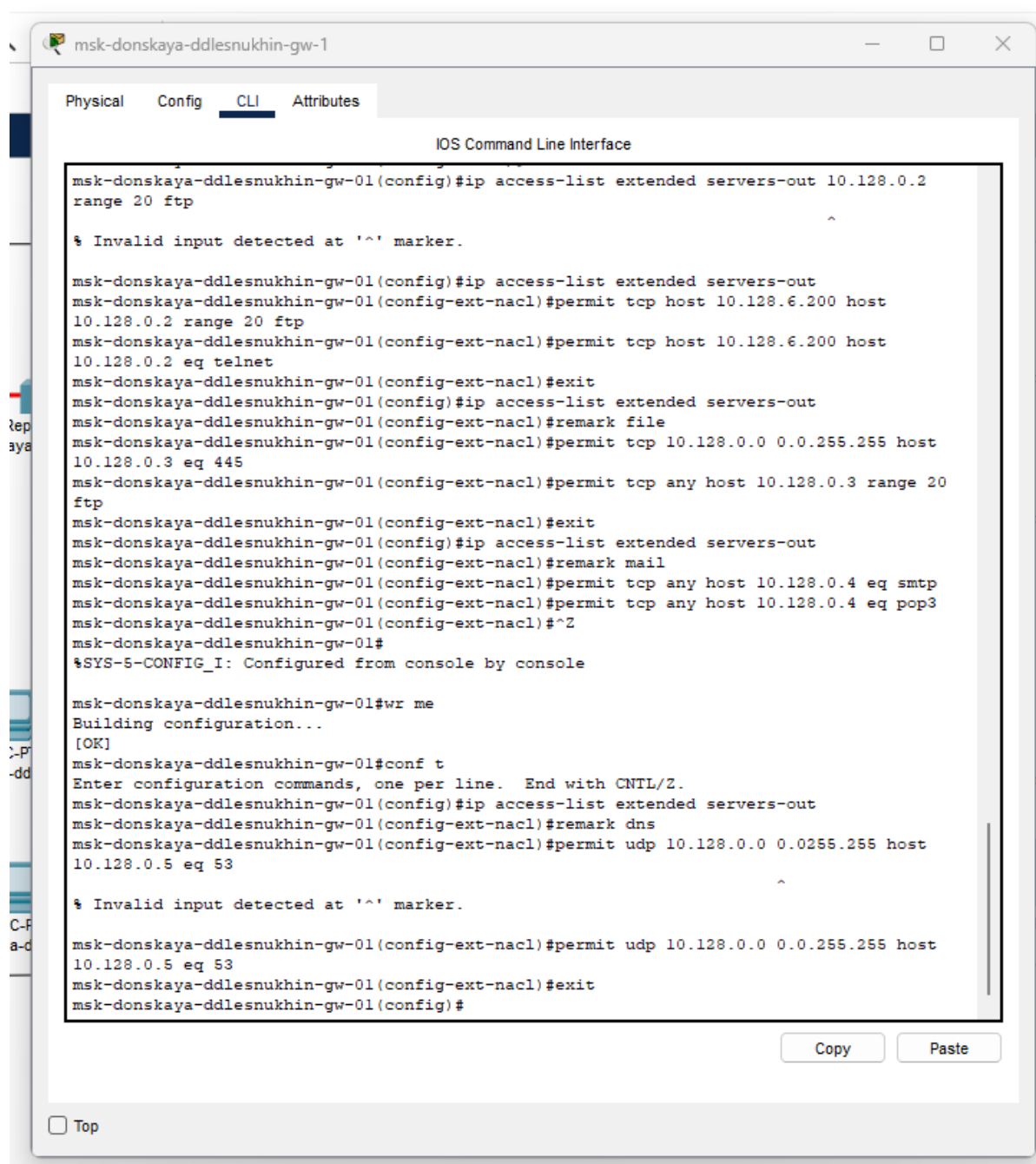


Рис. 1: Рис. 1.10. Доступ к серверам .

Разрешим істр-запросы. Здесь:

Демонстрируем явное управление порядком размещения правил — правило разреше-
ния для істр-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. 2: 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. 3: 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. 4: 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

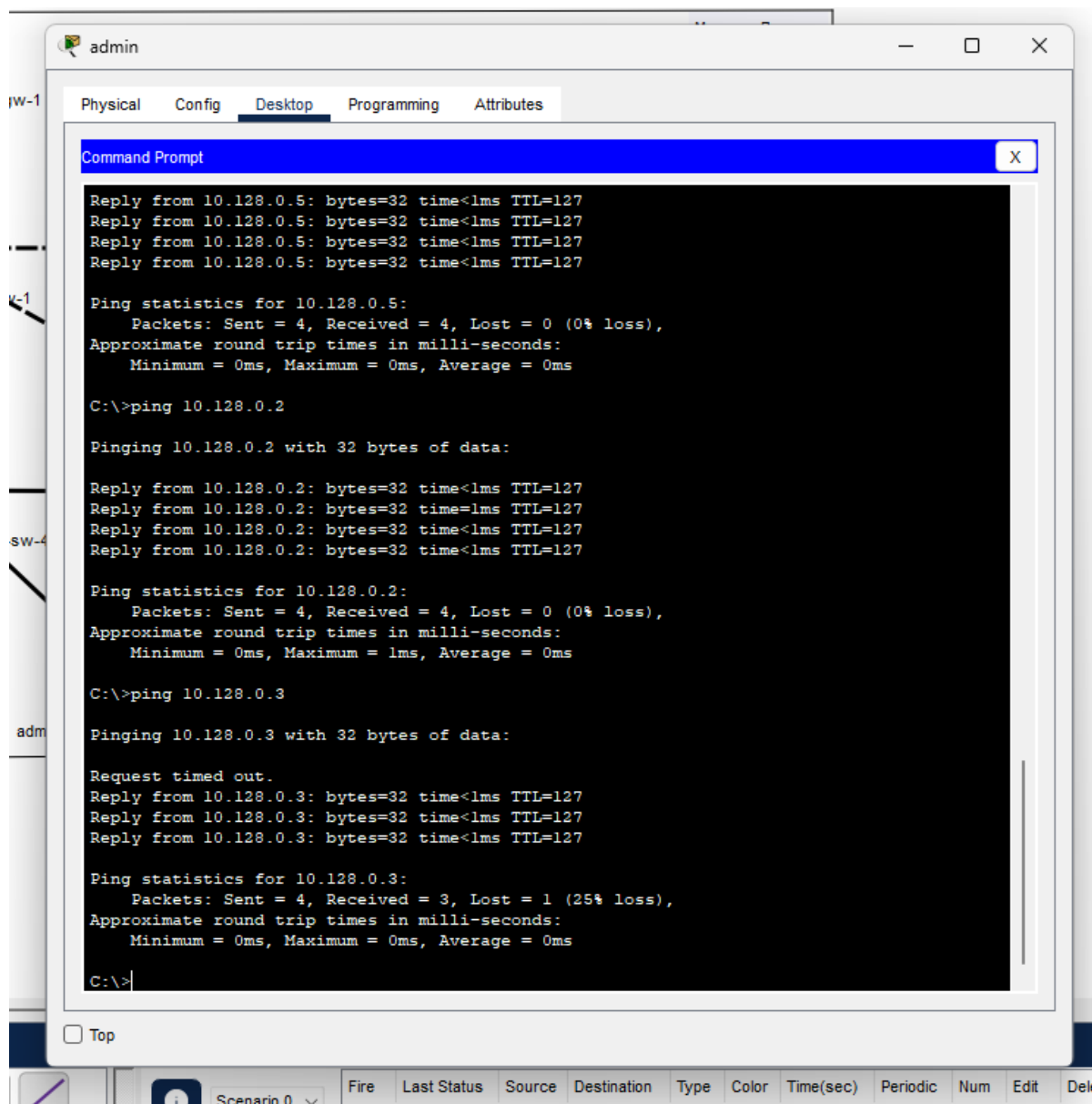


Рис. 5: Рис. 1.18. Проверка.

Вывод

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

- 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...`