Лабораторная работа №10

Настройка списков управления доступом ACL

Еюбоглу Тимур

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети

2 Задачи

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

3 Выполнение лабораторной работы

1. На главном (и единственном) роутере создаем списки доступа: Servers-out разрешает доступ на веб-сервер по протоколу http для всех, telnet и ftp только для администраторов. Разрешает доступ на файловый сервер по протоколу SMB для локальной сети и по FTP для всех Разрешает доступ на почтовый сервер по протоколам SMTP и POP3 Разрешает прохождение dns-запросов Разрешает пинг-запросы Other-in Разрешает доступ администраторам ко всем устройствам сети. Остальные действия запрещает Management-out Разрешает доступ к управлению устройствами cisco только для администраторов. (рис. 3.1) (рис. 3.2).

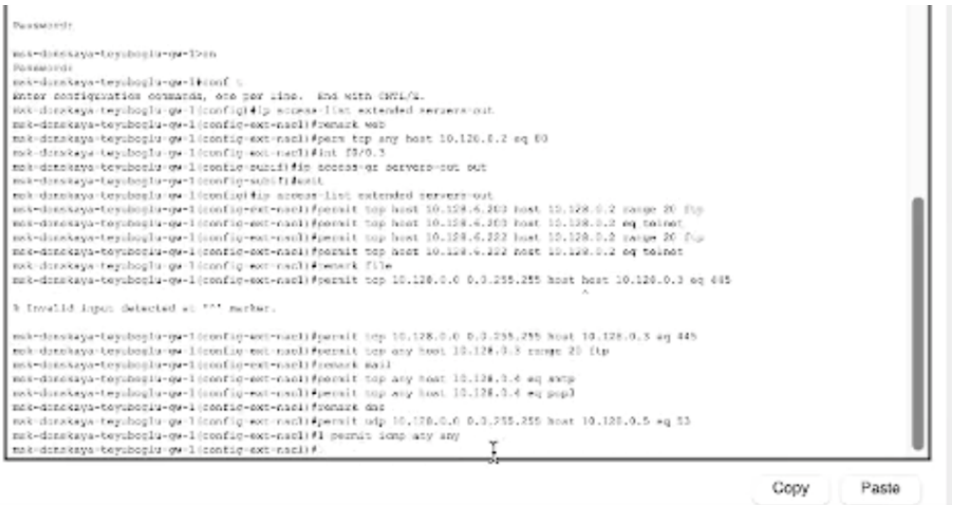

Рис. 3.1: Списки доступа

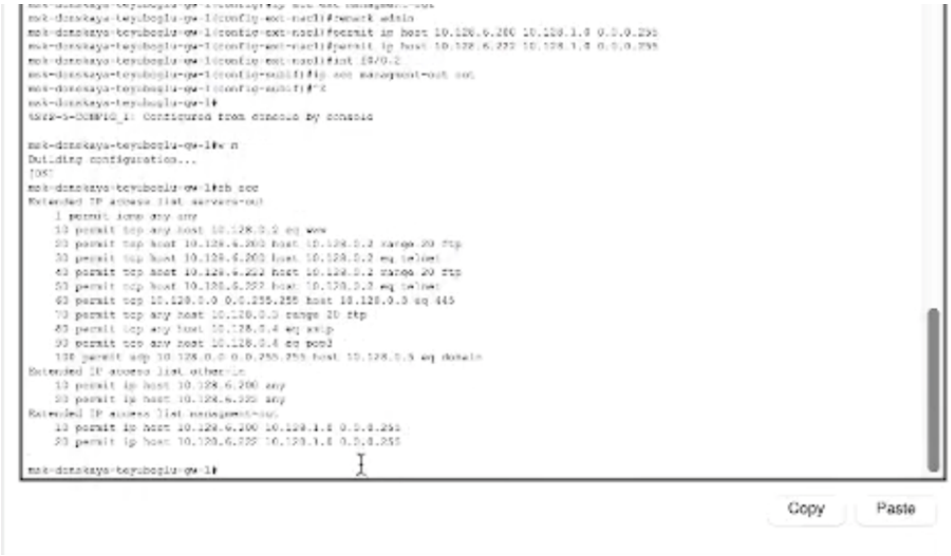

Рис. 3.2: Списки доступа

2. Проверяем работу списков доступа. Компьютеры могут получить доступ к сайту организации (рис. 3.3) (рис. 3.4).

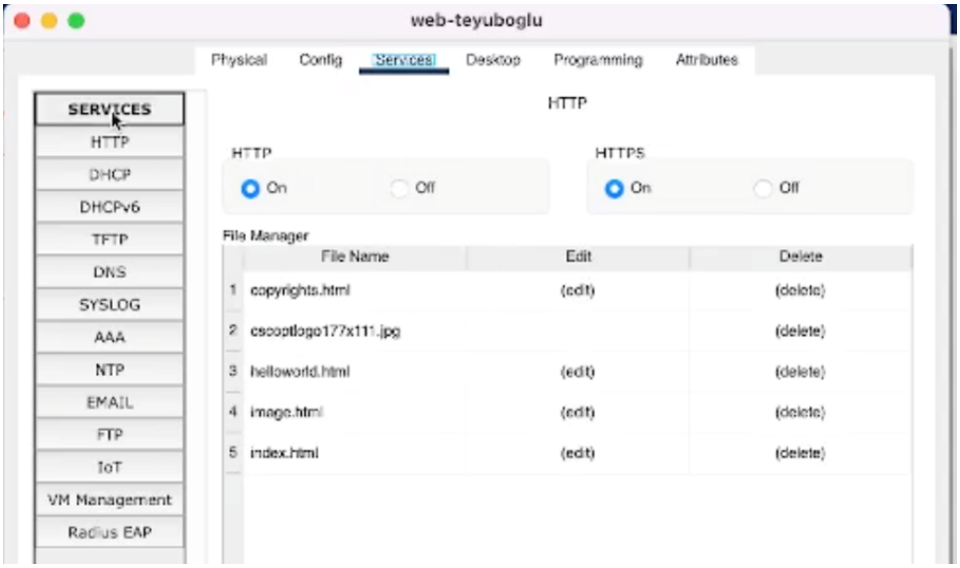

Рис. 3.3: Проверка работы

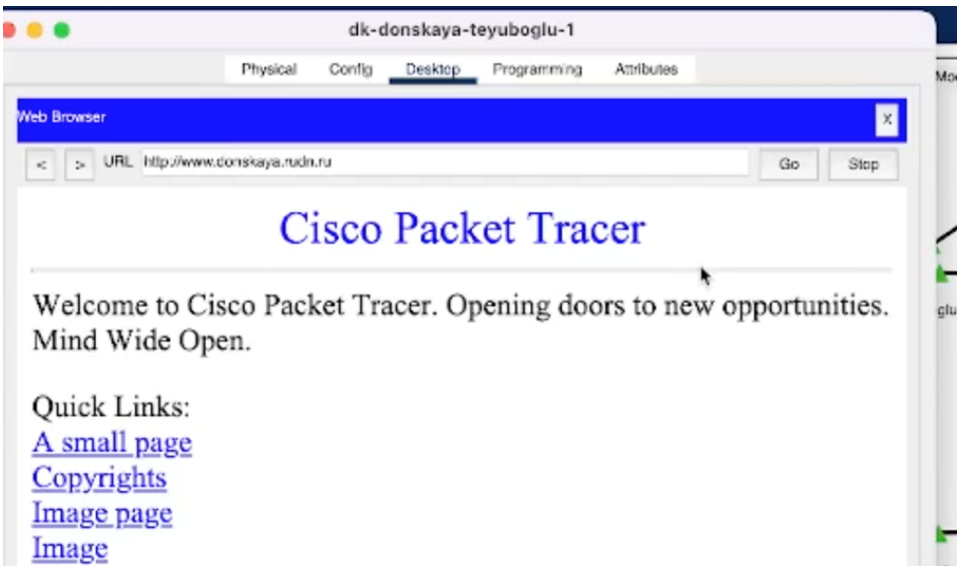

Рис. 3.4: Проверка работы

3. При этом по FTP подключиться к web-серверу не получилось (рис. 3.5).

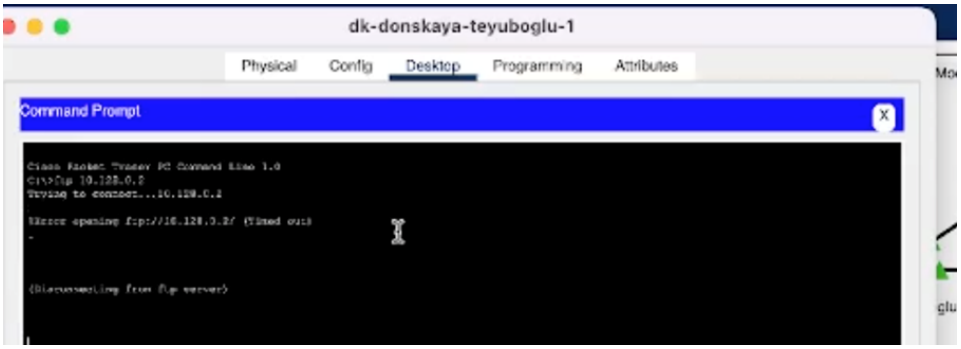

Рис. 3.5: Неудачное подключение

4. Устанавливаем компьютер администратора (рис. 3.6).

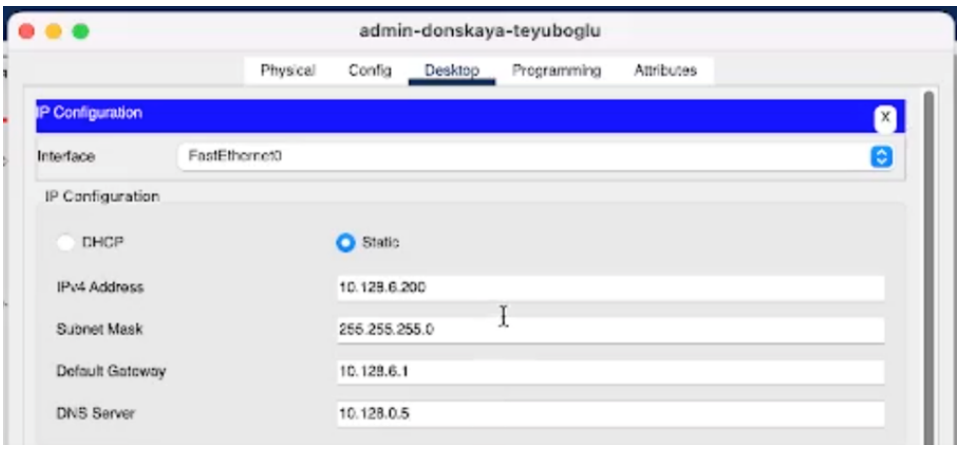

Рис. 3.6: Компьютер администратора

5. У администратора FTP работает (рис. 3.7).

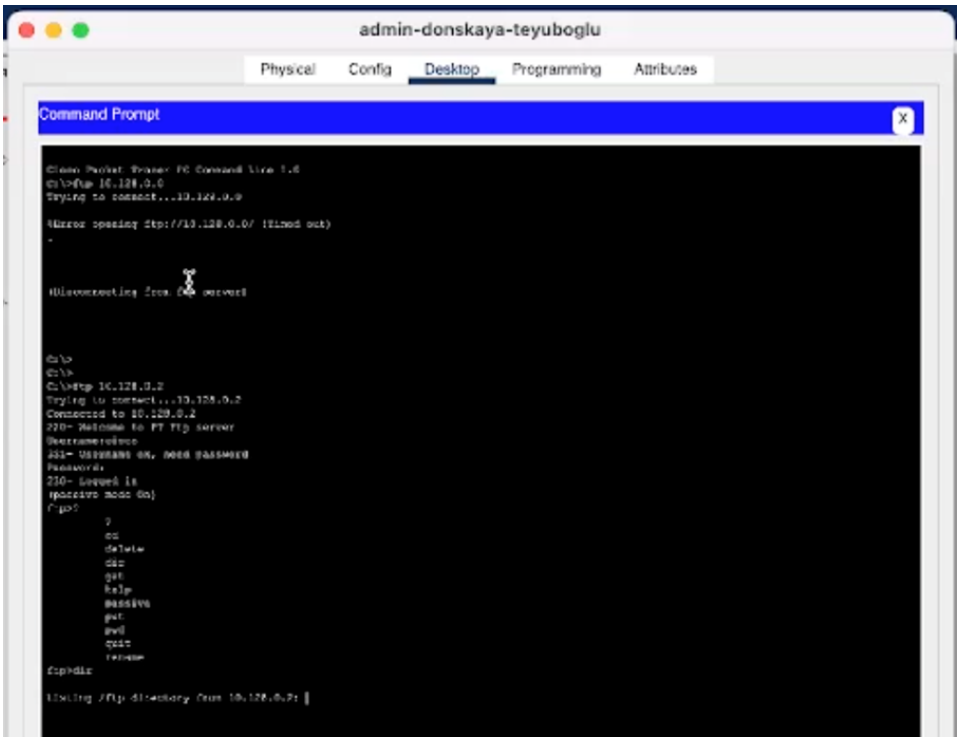

Рис. 3.7: FTP

6. На файловый сервер по FTP могут подключаться и остальные пользователи (рис. 3.8).

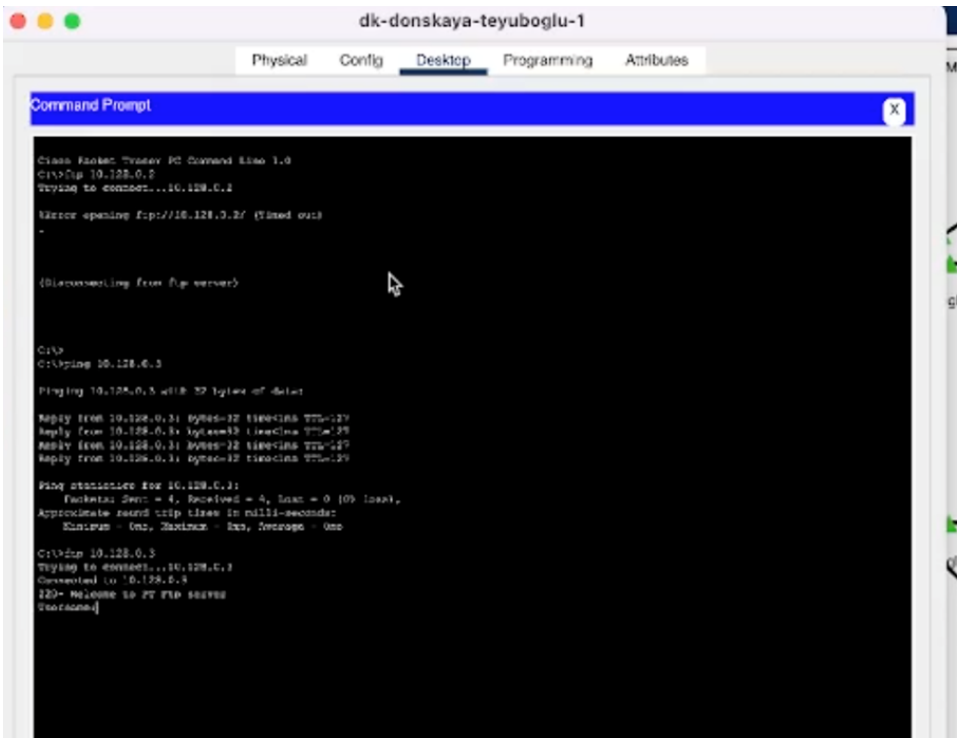

Рис. 3.8: FTP

7. Пользователям из группы other(vlan 104) запрещены любые действия(рис. 3.9).

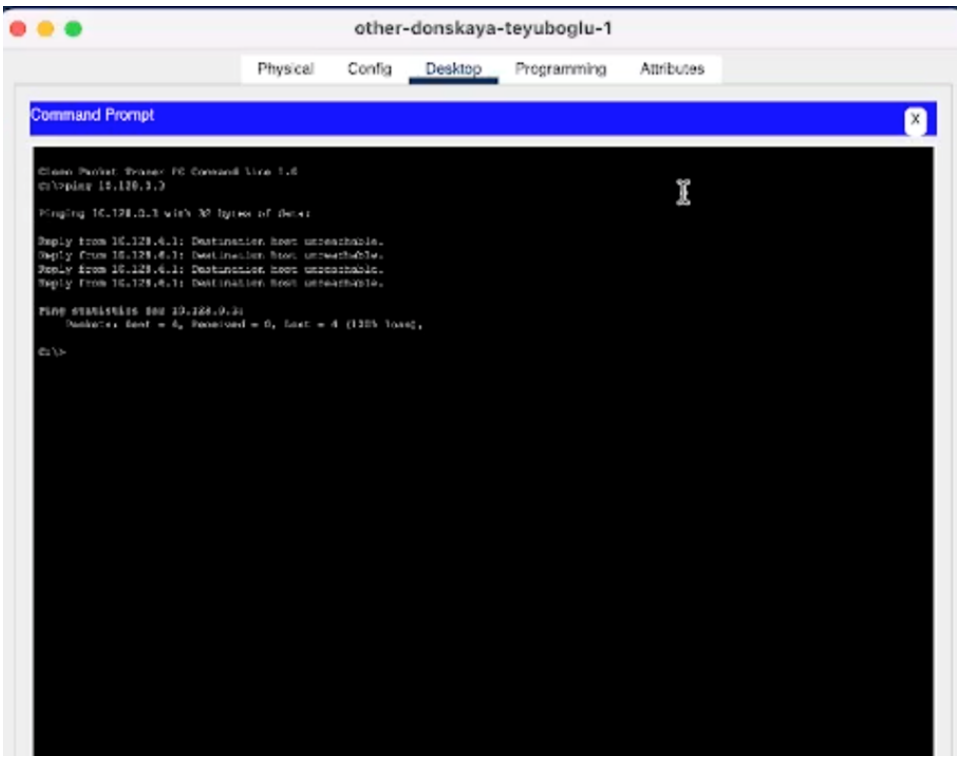

Рис. 3.9: Other

8. Настроим почтовый сервер (рис. 3.10).

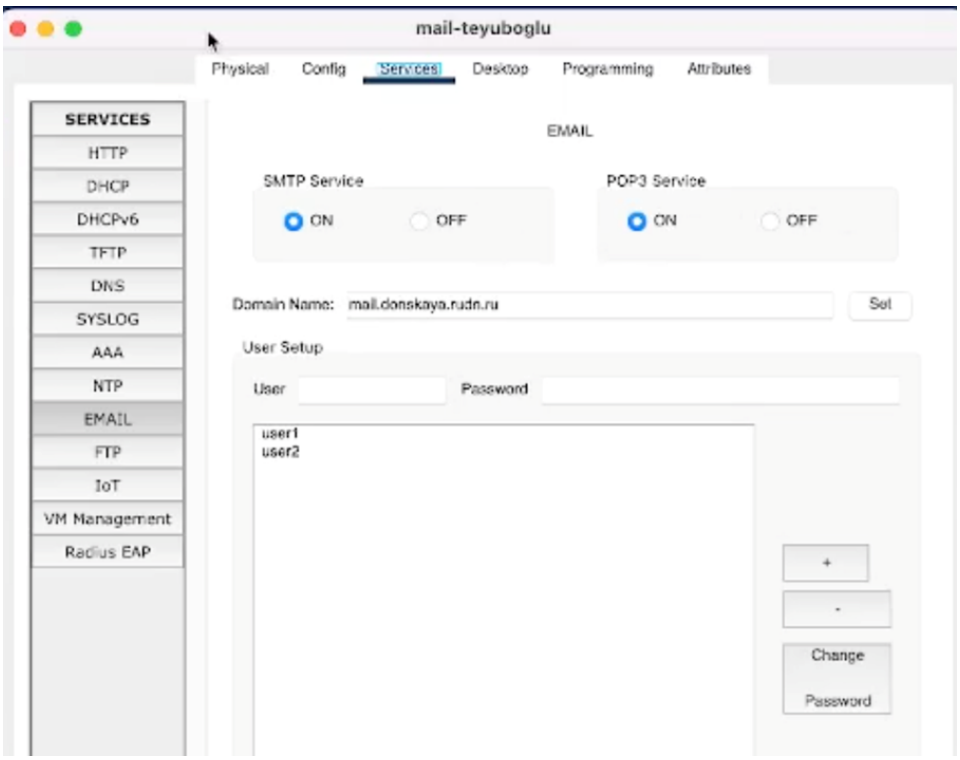

Рис. 3.10: Почтовый сервер

9. Обмен письмами (рис. 3.11).

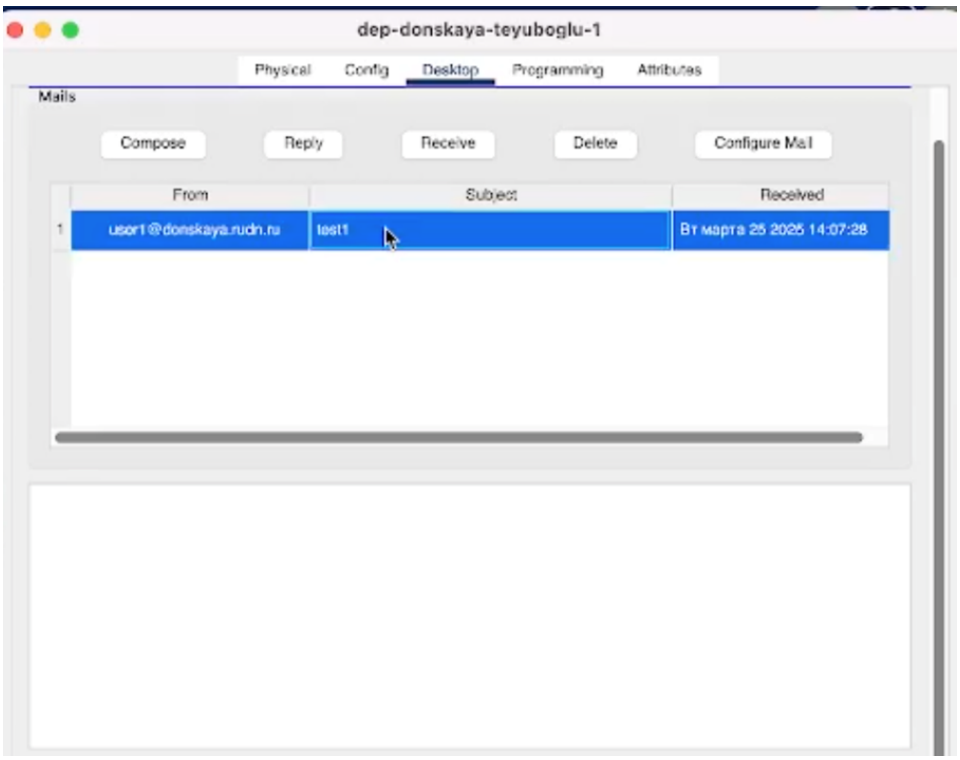

Рис. 3.11: Обмен письмами

10. Добавляем второго администратора (рис. 3.12).

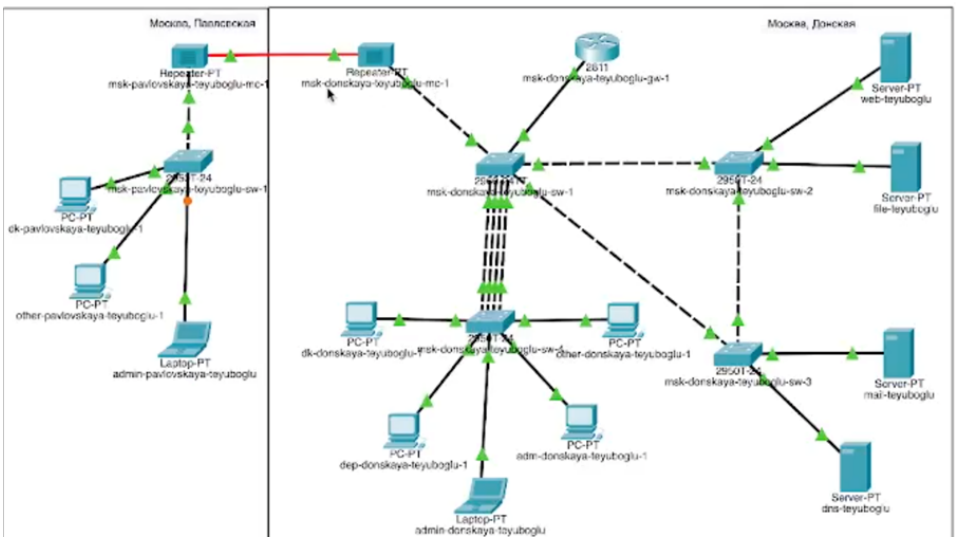

Рис. 3.12: Второй администратор

11. Он работает по FTP и SSH (рис. 3.13).

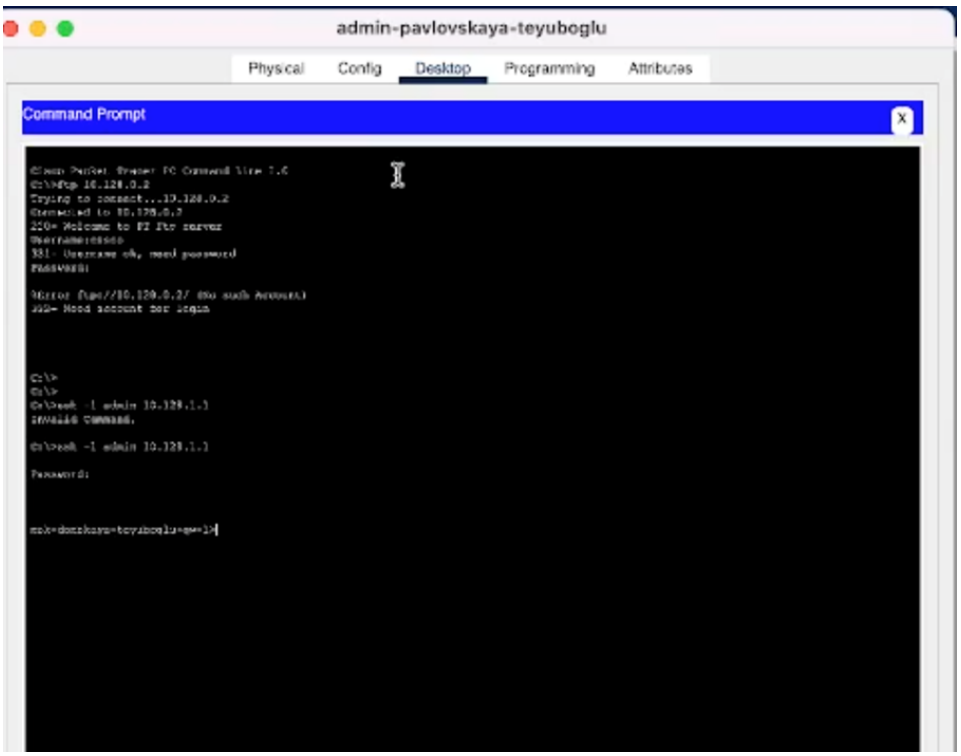

Рис. 3.13: Второй администратор

11. Пользователи могут работать по SSH только с роутером (рис. 3.14).

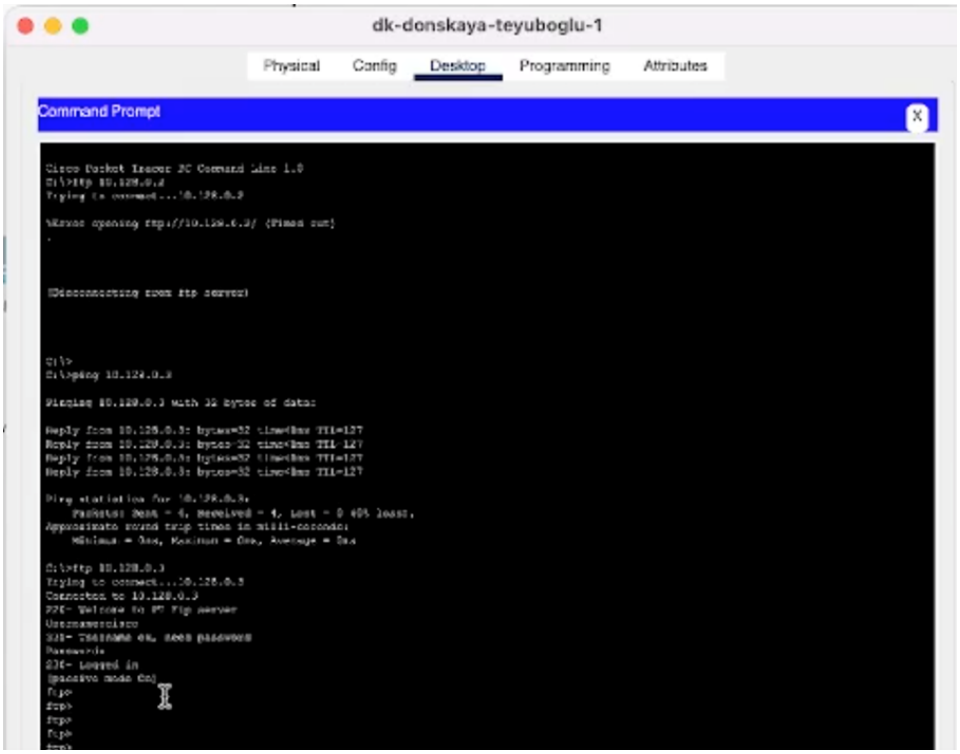

Рис. 3.14: Пользователи

4 Контрольные вопросы

1 Как задать действие правила для конкретного протокола? #permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet после указания хостов пишется атрибут eq и после него протокол 2 Как задать действие правила сразу для нескольких портов? #permit tcp any host 10.128.0.3 range 20 21 после указания хостов пишется атрибут range и диапазон портов 3 Как узнать номер правила в списке прав доступа? командой show access-list 4 Каким образом можно изменить порядок применения правил в списке контроля доступа? поставить цифру, указывающую на номер будущего правила, перед его формулировкой. Либо нужно экспортировать файл конфигурации и отредактировать его на другом устройстве, после чего импортировать обратно.

5 Выводы

Благодаря выполнению данной лабораторной работы, мы освоили настройку прав доступа пользователей к ресурсам сети