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. 1) (рис. 2).

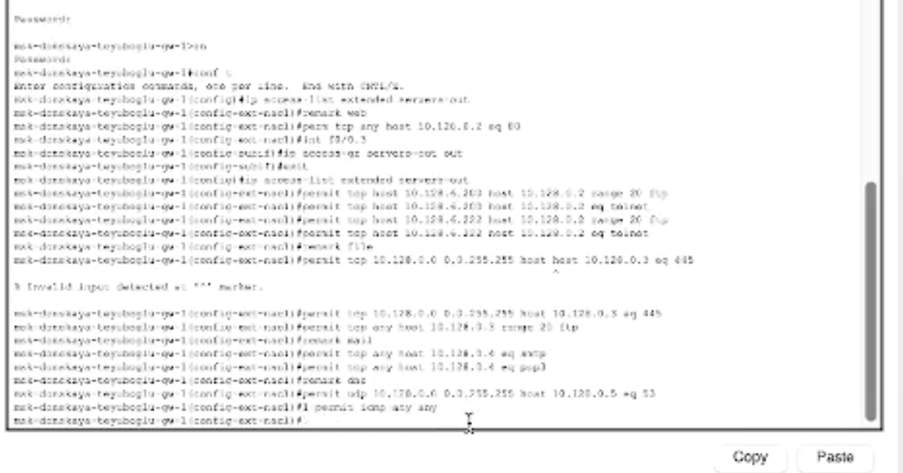


Рис. 1: Списки доступа



Рис. 2: Списки доступа

1. Проверяем работу списков доступа. Компьютеры могут получить доступ к сайту организации (рис. 3) (рис. 4).

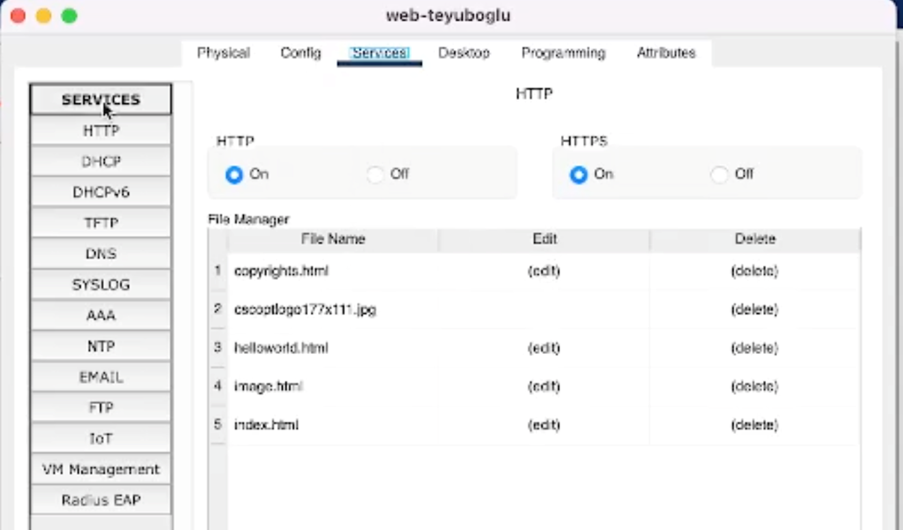


Рис. 3: Проверка работы



Рис. 4: Проверка работы

1. При этом по FTP подключиться к web-серверу не получилось (рис. 5).

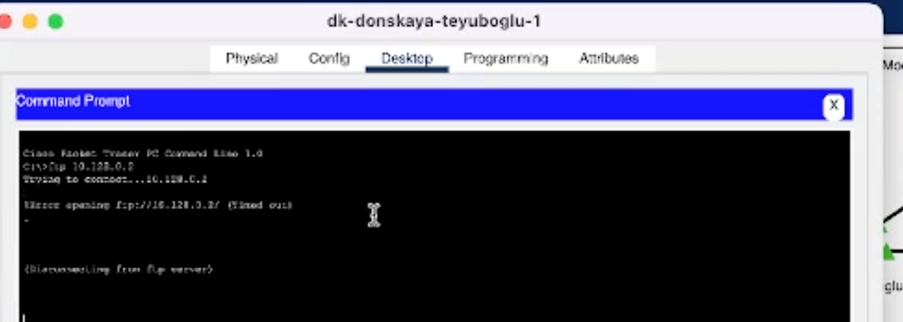


Рис. 5: Неудачное подключение

1. Устанавливаем компьютер администратора (рис. 6).

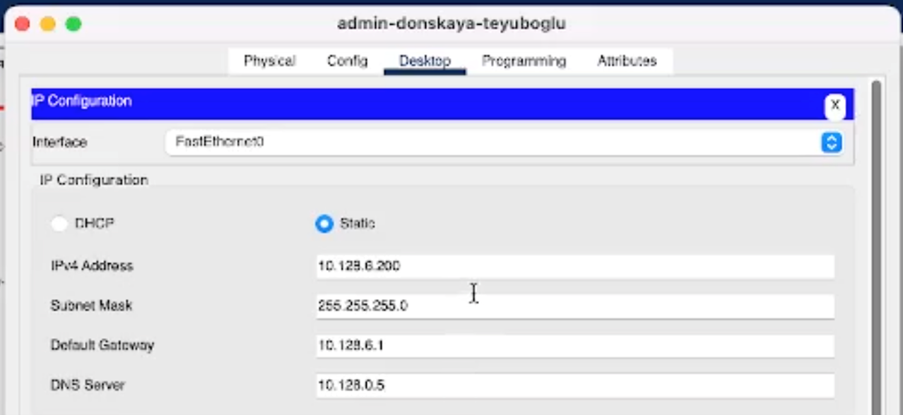


Рис. 6: Компьютер администратора

1. У администратора FTP работает (рис. 7).

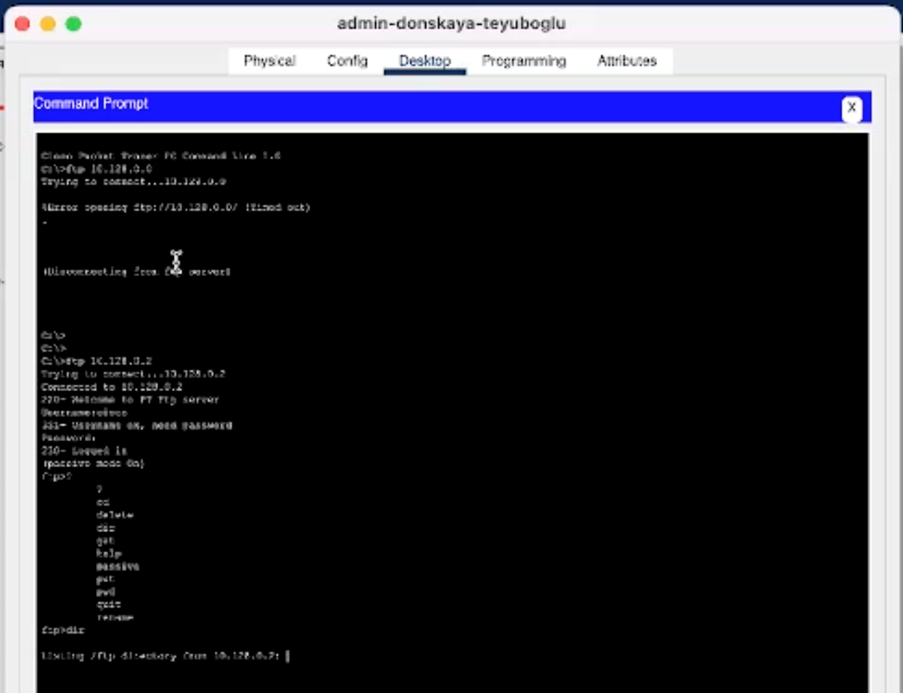


Рис. 7: FTP

1. На файловый сервер по FTP могут подключаться и остальные пользователи (рис. 8).

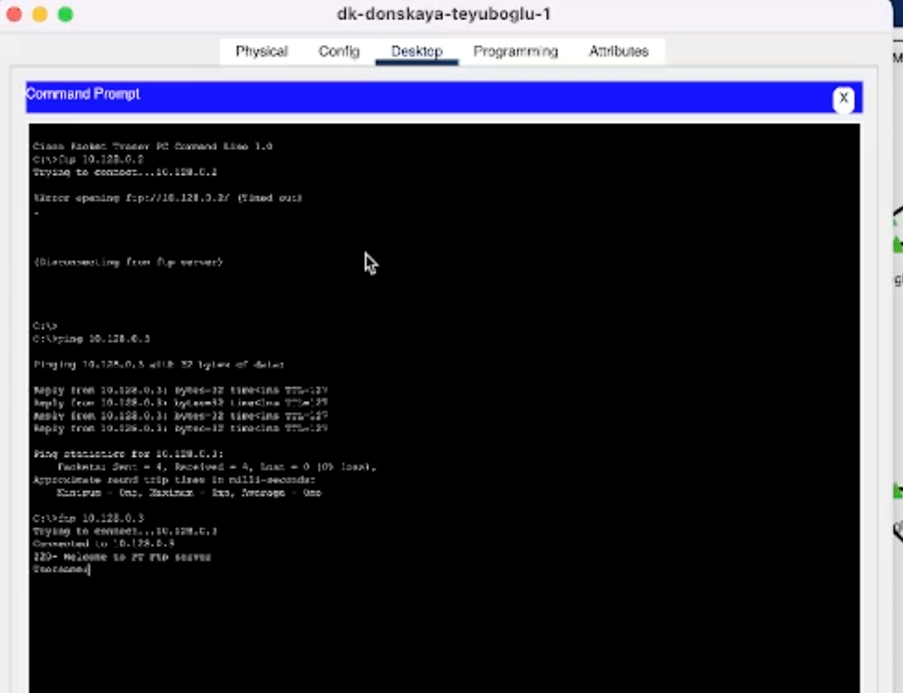


Рис. 8: FTP

1. Пользователям из группы other(vlan 104) запрещены любые действия(рис. 9).

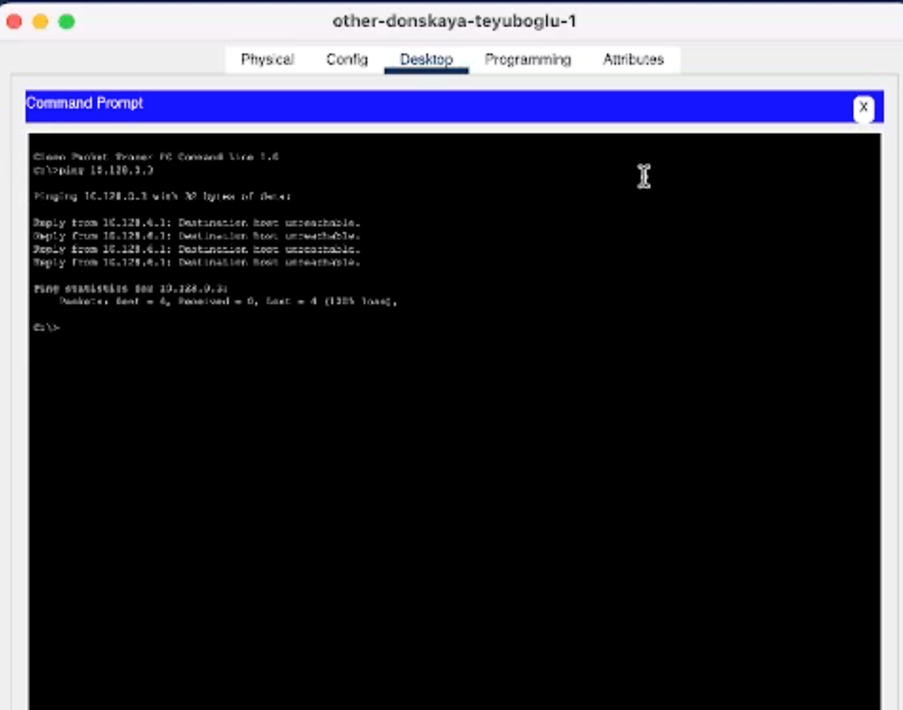


Рис. 9: Other

1. Настроим почтовый сервер (рис. 10).

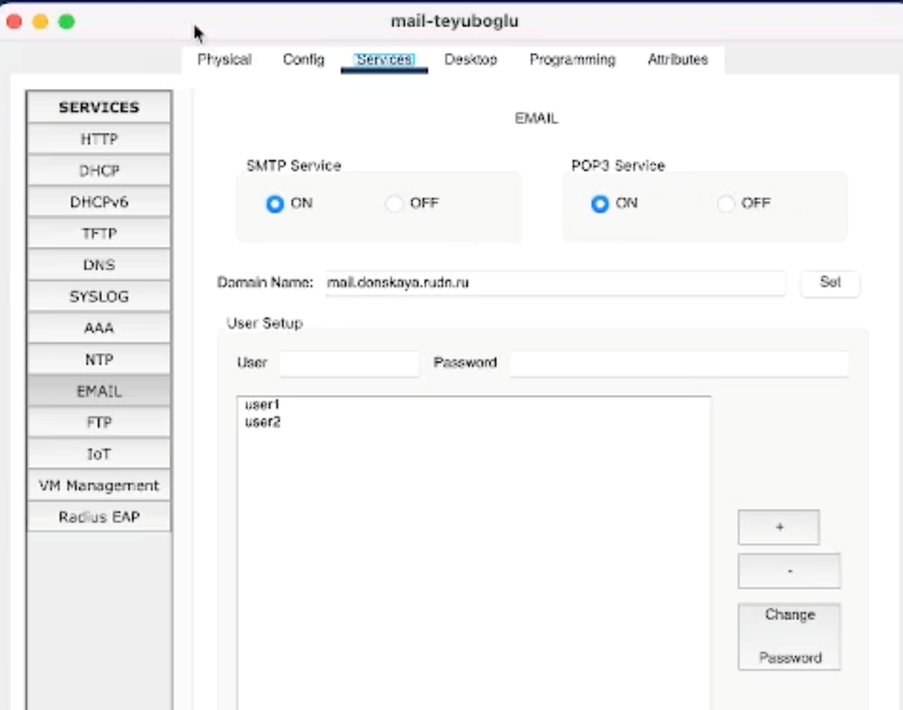


Рис. 10: Почтовый сервер

1. Обмен письмами (рис. 11).

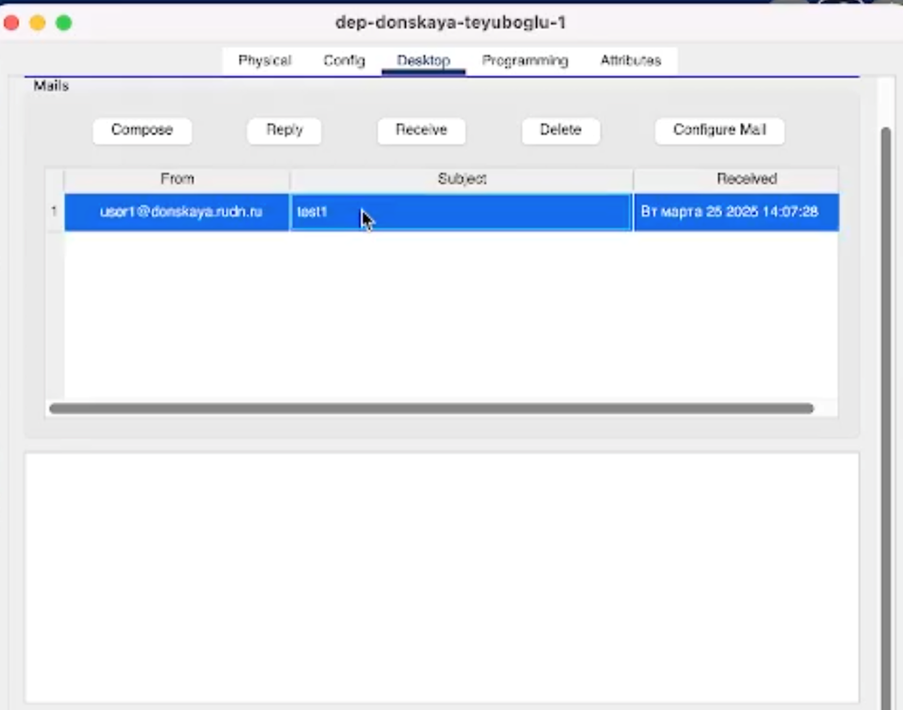


Рис. 11: Обмен письмами

1. Добавляем второго администратора (рис. 12).

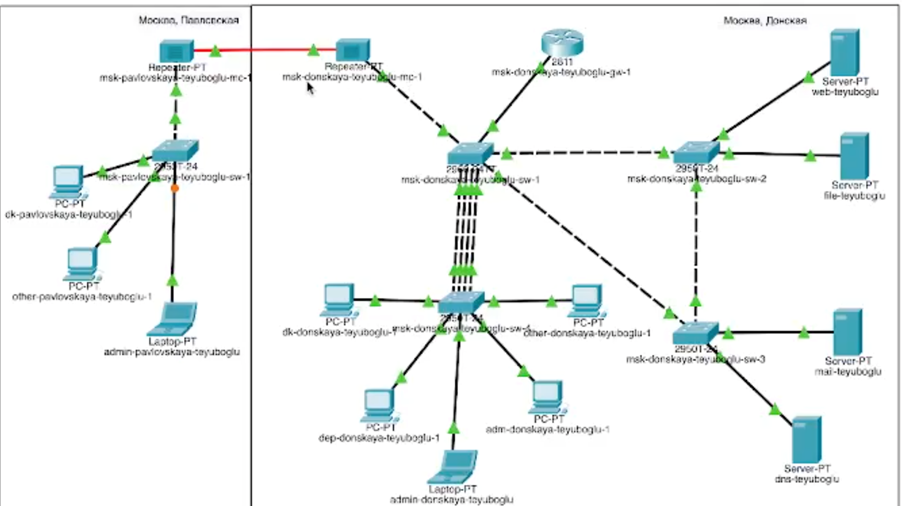


Рис. 12: Второй администратор

1. Он работает по FTP и SSH (рис. 13).

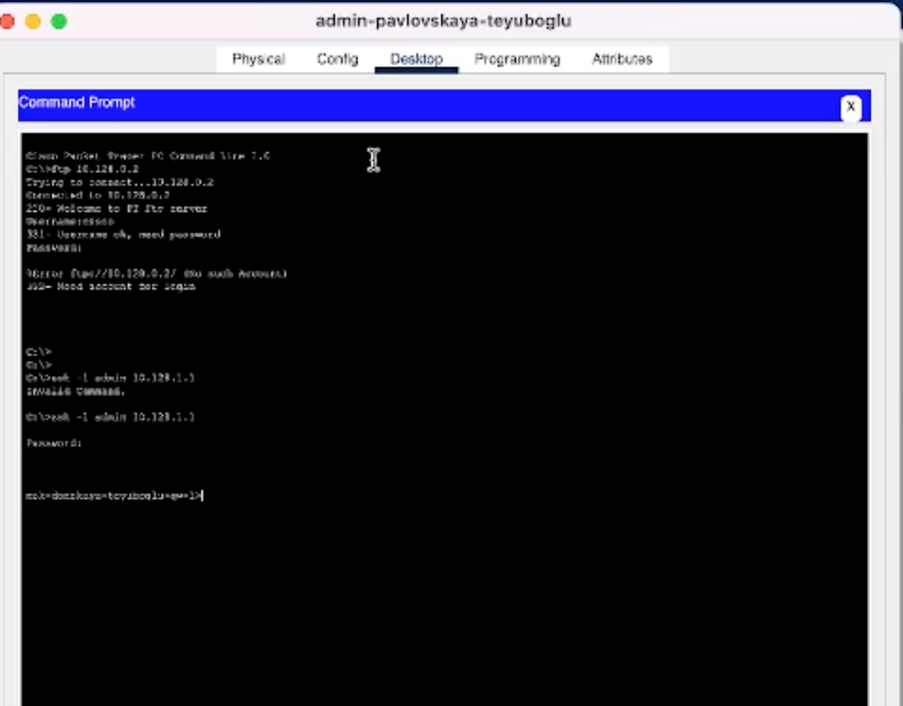


Рис. 13: Второй администратор

1. Пользователи могут работать по SSH только с роутером (рис. 14).

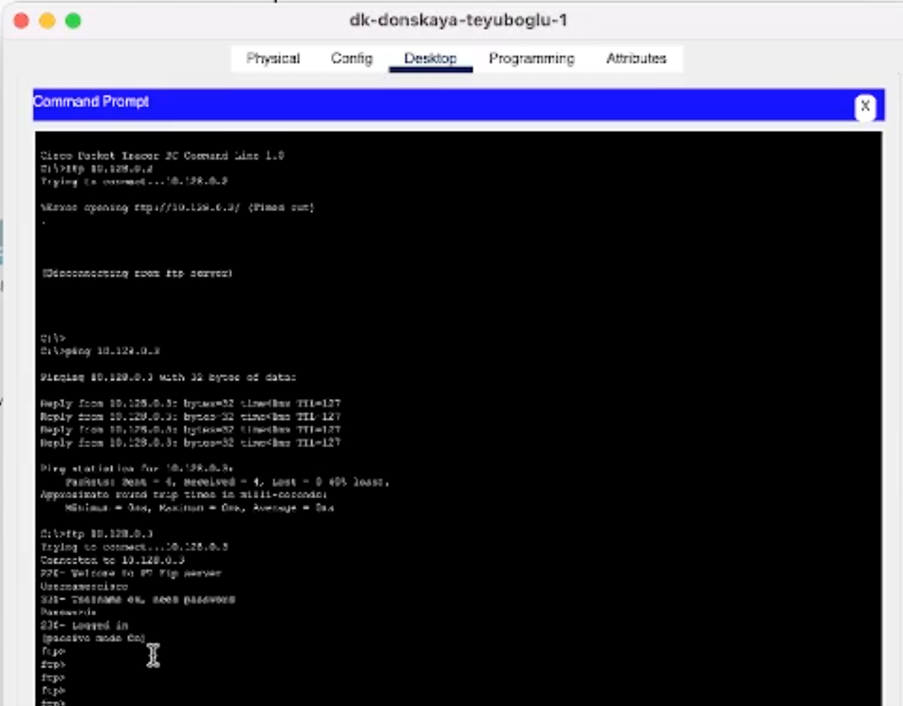


Рис. 14: Пользователи

# 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