РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 10

**Настройка списков управления доступом (ACL)**

*дисциплина: Администрирование локальных сетей*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы**

Освоить настройку прав доступа пользователей к ресурсам сети.

**Выполнение работы**

1. В рабочей области проекта подключите ноутбук администратора с именем admin к сети к other-donskaya-1 с тем (Рис. 1), 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. 2).

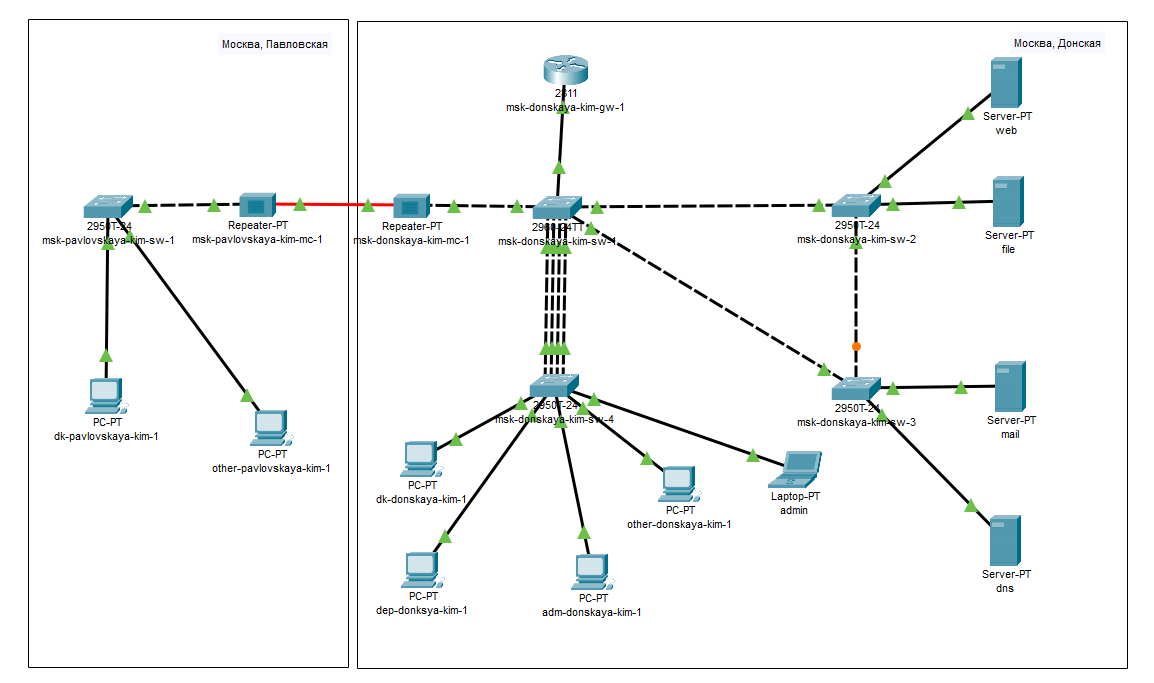


Рисунок 1

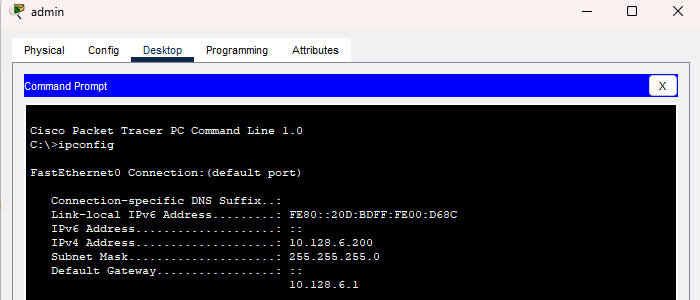


Рисунок 2

1. Настройка доступа к web-серверу по порту tcp 80 (Рис. 3):

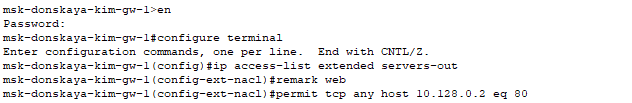


Рисунок 3

1. Добавление списка управления доступом к интерфейсу (Рис. 4):



Рисунок 4

Здесь: к интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out).

Можно проверить, 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 (Рис. 5-6).

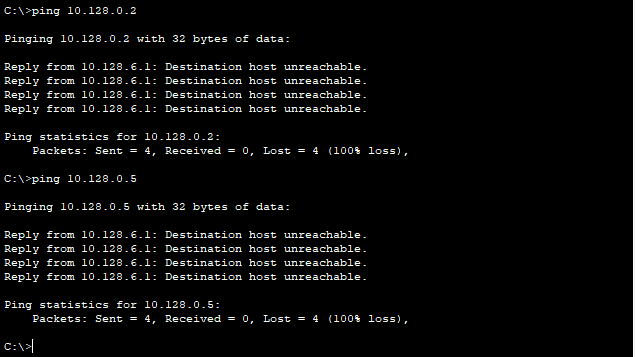


Рисунок 5

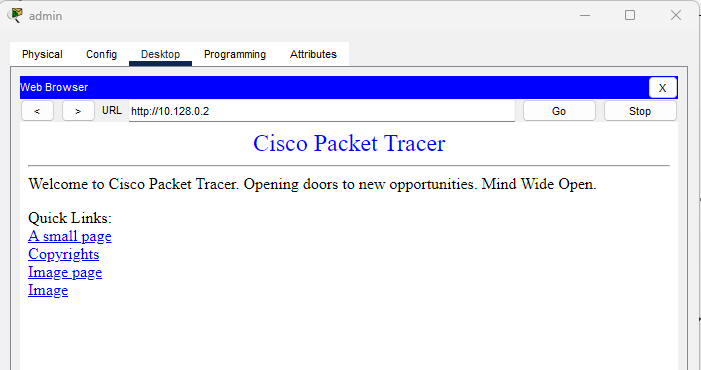


Рисунок 6

1. Дополнительный доступ для администратора по протоколам Telnet и FTP (Рис. 7):

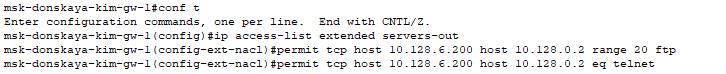


Рисунок 7

Здесь: 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.

Убедитесь, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введите ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (Рис. 8).

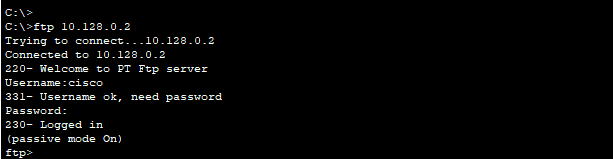


Рисунок 8

Попробуйте провести аналогичную процедуру с другого устройства сети (dk-donskaya-kim-1). Убедитесь, что доступ будет запрещён (Рис. 9).

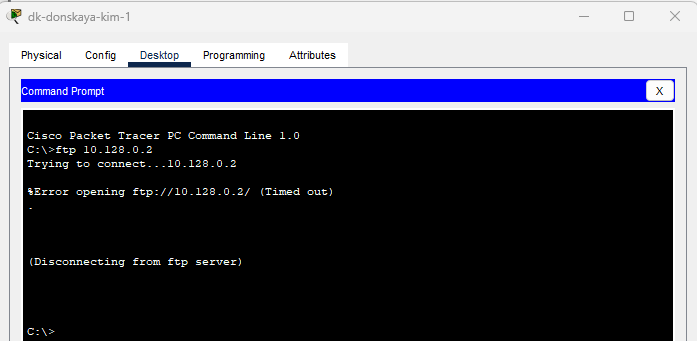


Рисунок 9

1. Настройка доступа к файловому серверу (рис. 10):

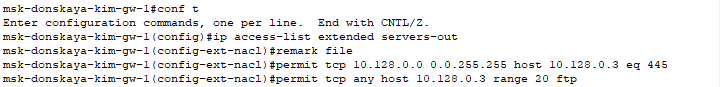


Рисунок 10

1. Настройка доступа к почтовому серверу (рис. 11):

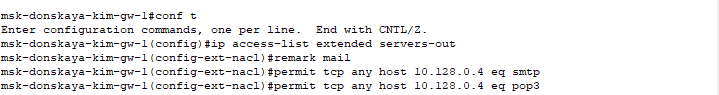


Рисунок 11

1. Настройка доступа к DNS-серверу (рис. 12):

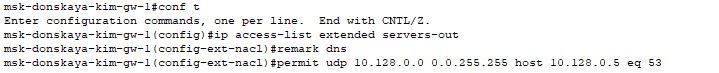


Рисунок 12

Здесь: 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.

Проверьте доступность web-сервера (через браузер) не только по ip-адресу, но и по имени (рис. 13-14).

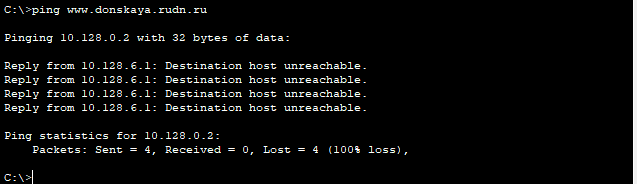


Рисунок 13

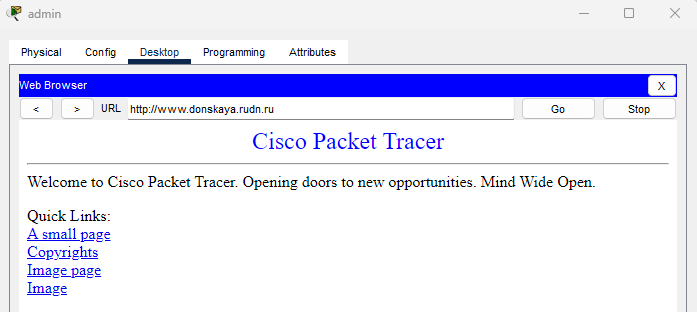


Рисунок 14

1. Разрешение icmp-запросов:



Рисунок 15

Здесь демонстрируется 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 (рис. 16):

msk−donskaya-kim−gw −1#show access −lists

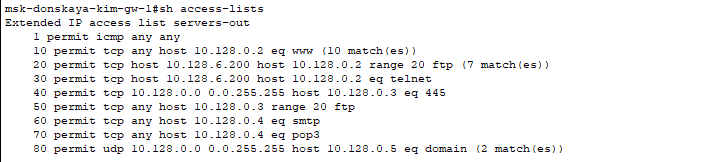


Рисунок 16

1. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-kim-gw-1 является входящим трафиком) (рис. 17):

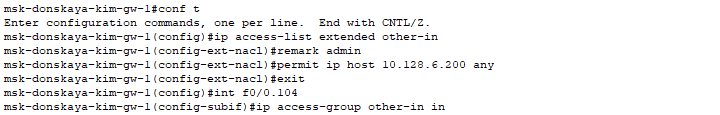


Рисунок 17

1. Настройка доступа администратора к сети сетевого оборудования (рис. 18):

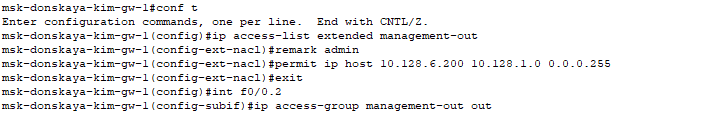


Рисунок 18

1. Схемы L1, таблицы IP и VLAN:

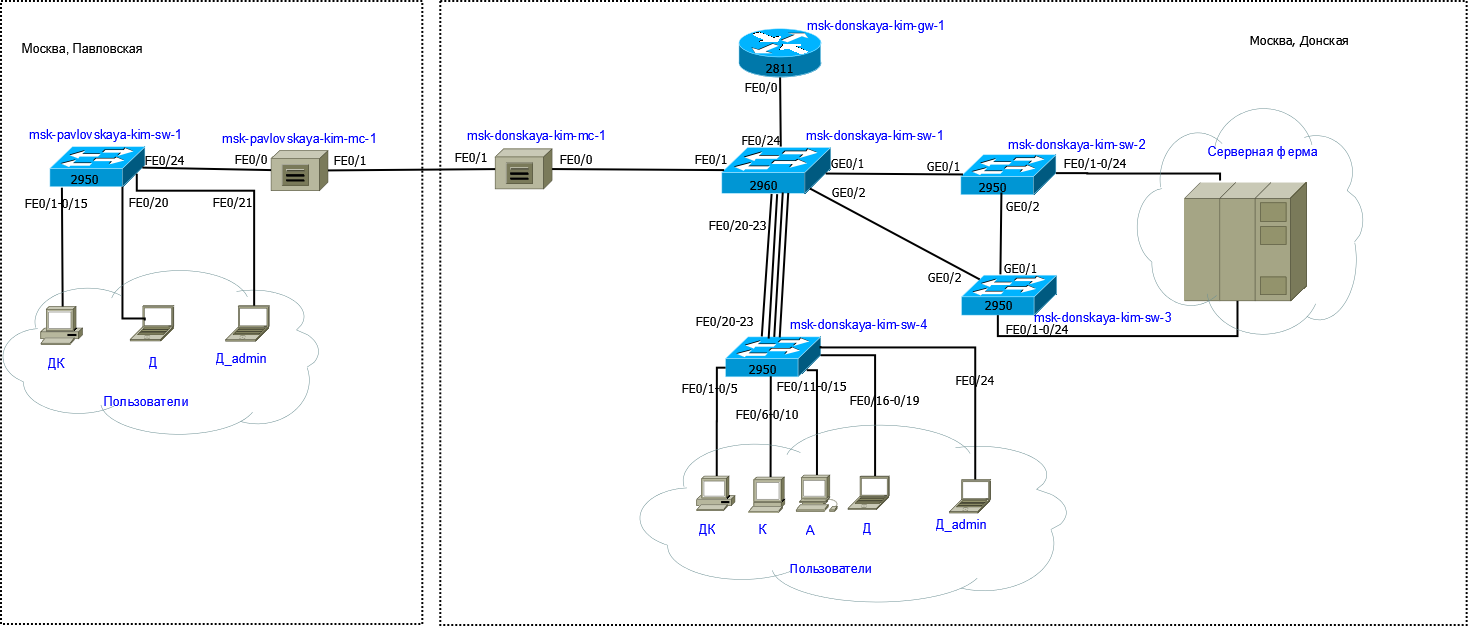


Рисунок 19: Layer 1

**Таблица IP**

|  |  |  |
| --- | --- | --- |
| IP-адреса | Примечание | VLAN |
| 10.128.0.0/16 | Вся сеть |  |
| 10.128.0.0/24  10.128.0.1  10.128.0.2  10.128.0.3  10.128.0.4  10.128.0.5  10.128.0.6-10.128.0.254 | Серверная ферма  Шлюз  Web  File  Mail  Dns  Зарезервировано | 3 |
| 10.128.1.0/24  10.128.1.1  10.128.1.2  10.128.1.3  10.128.1.4  10.128.1.5  10.128.1.6  10.128.1.7-10.128.1.254 | Управление  Шлюз  msk-donskaya-kim-sw-1  msk-donskaya-kim-sw-2  msk-donskaya-kim-sw-3  msk-donskaya-kim-sw-4  msk-pavlovskaya-kim-sw-1  Зарезервировано | 2 |
| 10.128.2.0/24  10.128.2.1  10.128.2.2-10.128.2.254 | Cеть Point-to-Point  Шлюз  Зарезервировано |  |
| 10.128.3.0/24  10.128.3.1  10.128.3.2-10.128.3.254 | Дисплейные классы (ДК)  Шлюз  Пул для пользователей | 101 |
| 10.128.4.0/24  10.128.4.1  10.128.4.2-10.128.4.254 | Кафедры (К)  Шлюз  Пул для пользователей | 102 |
| 10.128.5.0/24  10.128.5.1  10.128.5.2-10.128.5.254 | Администрация (А)  Шлюз  Пул для пользователей | 103 |
| 10.128.6.0/24  10.128.6.1  10.128.6.2-10.128.6.199  10.128.6.200  10.128.6.201 | Другие пользователи (Д)  Шлюз  Пул для пользователей  admin-donskaya-kim-1  admin-pavlovskaya-kim-1 | 104 |

**Таблица VLAN**

|  |  |  |
| --- | --- | --- |
| № VLAN | Имя VLAN | Примечание |
| 1  2  3  4-100  101  102  103  104  104 | default  management  servers  dk  departments  adm  other  admin | Не используется  Для управления устройствами  Для серверной фермы  Зарезервировано  Дисплейные классы (ДК)  Кафедры  Администрация  Для других пользователей |

**Самостоятельная работа**

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

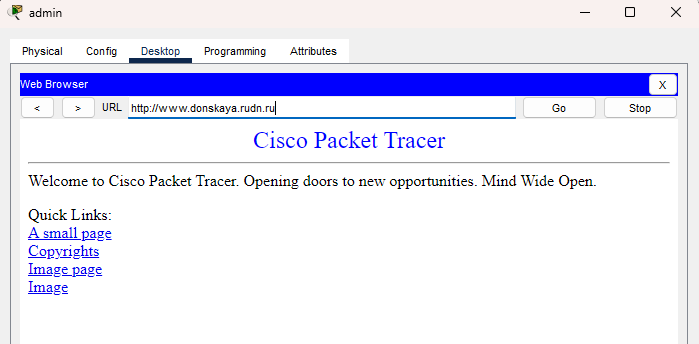


Рисунок 20

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

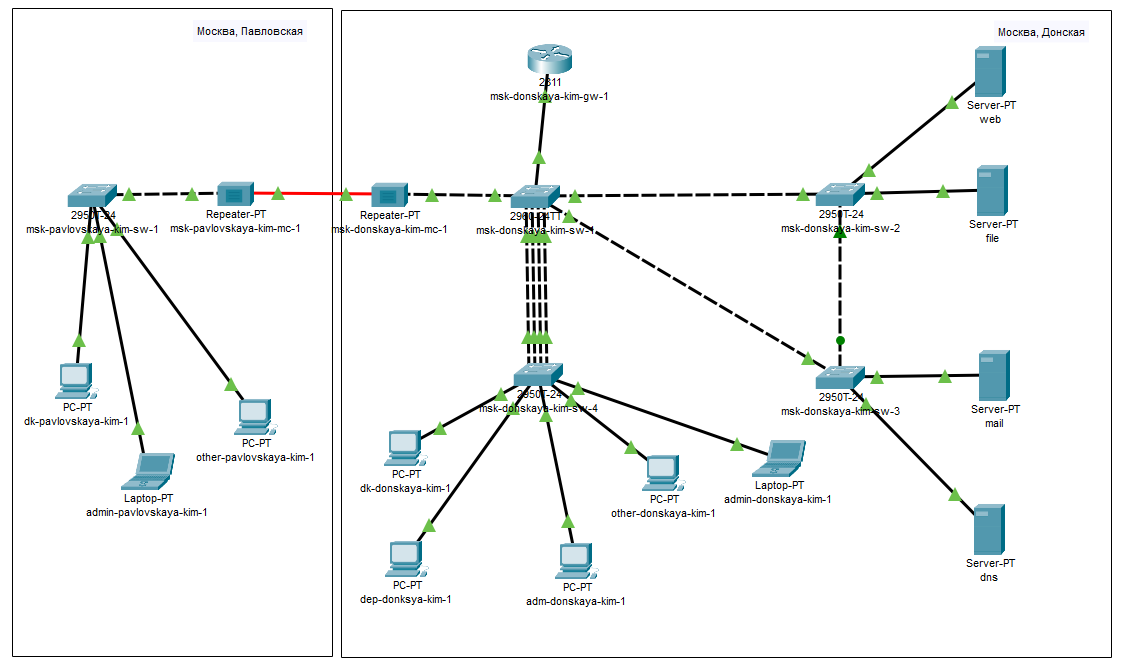


Рисунок 21

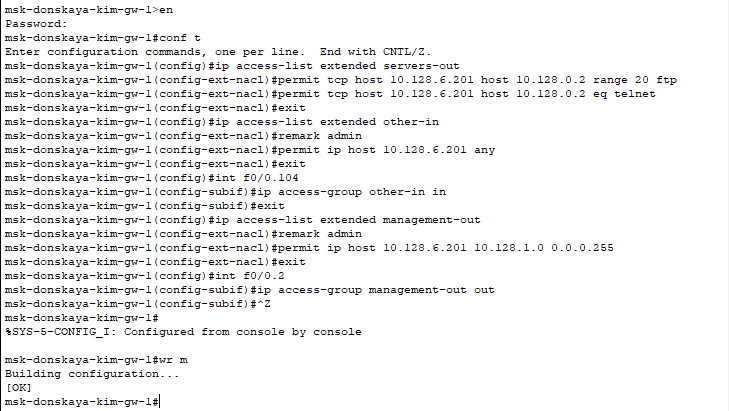


Рисунок 22

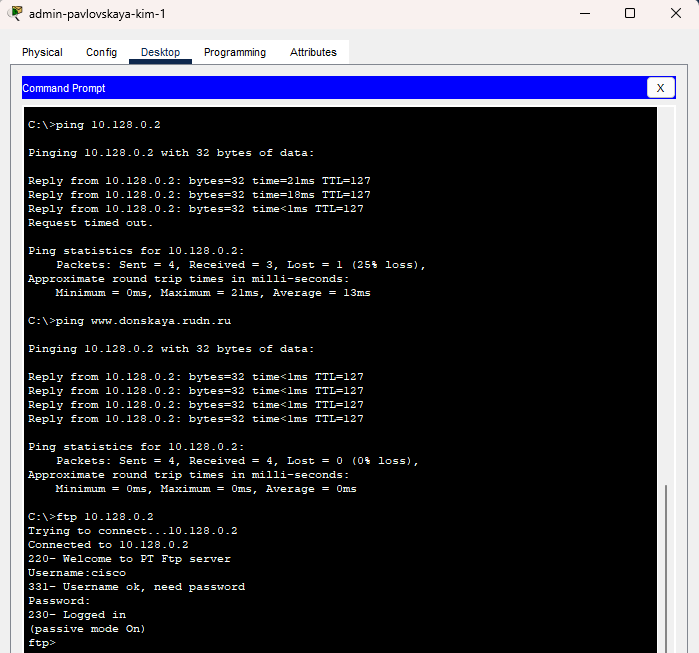


Рисунок 23

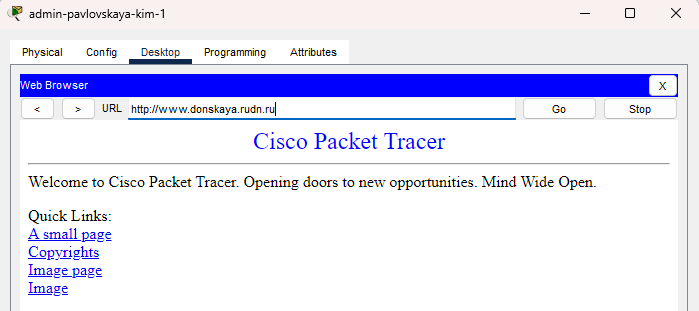


Рисунок 24

**Конфигурации оборудования**

* **msk-donskaya-kim-gw-1**

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname msk-donskaya-kim-gw-1

!

!

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

ip dhcp excluded-address 10.128.3.1 10.128.3.29

ip dhcp excluded-address 10.128.3.200 10.128.3.254

ip dhcp excluded-address 10.128.4.1 10.128.4.29

ip dhcp excluded-address 10.128.4.200 10.128.4.254

ip dhcp excluded-address 10.128.5.1 10.128.5.29

ip dhcp excluded-address 10.128.5.200 10.128.5.254

ip dhcp excluded-address 10.128.6.1 10.128.6.29

ip dhcp excluded-address 10.128.6.200 10.128.6.254

!

ip dhcp pool dk

network 10.128.3.0 255.255.255.0

default-router 10.128.3.1

dns-server 10.128.0.5

ip dhcp pool departments

network 10.128.4.0 255.255.255.0

default-router 10.128.4.1

dns-server 10.128.0.5

ip dhcp pool adm

network 10.128.5.0 255.255.255.0

default-router 10.128.5.1

dns-server 10.128.0.5

ip dhcp pool other

network 10.128.6.0 255.255.255.0

default-router 10.128.6.1

dns-server 10.128.0.5

!

!

!

ip cef

no ipv6 cef

!

!

!

username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

license udi pid CISCO2811/K9 sn FTX1017LG55-

!

!

!

!

!

!

!

!

!

ip domain-name donskaya.rudn.edu

ip name-server 10.128.0.5

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

!

interface FastEthernet0/0.2

description management

encapsulation dot1Q 2

ip address 10.128.1.1 255.255.255.0

ip access-group management-out out

!

interface FastEthernet0/0.3

description servers

encapsulation dot1Q 3

ip address 10.128.0.1 255.255.255.0

ip access-group servers-out out

!

interface FastEthernet0/0.101

description dk

encapsulation dot1Q 101

ip address 10.128.3.1 255.255.255.0

!

interface FastEthernet0/0.102

description departments

encapsulation dot1Q 102

ip address 10.128.4.1 255.255.255.0

!

interface FastEthernet0/0.103

description adm

encapsulation dot1Q 103

ip address 10.128.5.1 255.255.255.0

!

interface FastEthernet0/0.104

description other

encapsulation dot1Q 104

ip address 10.128.6.1 255.255.255.0

ip access-group other-in in

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

!

!

ip access-list extended servers-out

remark web

permit icmp any any

permit tcp any host 10.128.0.2 eq www

permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp

permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet

remark file

permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445

permit tcp any host 10.128.0.3 range 20 ftp

remark mail

permit tcp any host 10.128.0.4 eq smtp

permit tcp any host 10.128.0.4 eq pop3

remark dns

permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain

ip access-list extended other-in

remark admin

permit ip host 10.128.6.200 any

ip access-list extended management-out

remark admin

permit ip host 10.128.6.200 10.128.1.0 0.0.0.255

!

!

!

!

!

line con 0

password 7 0822455D0A16

login

!

line aux 0

!

line vty 0 4

password 7 0822455D0A16

login

transport input ssh

!

!

!

end

**Ответы на контрольные вопросы**

1. Как задать действие правила для конкретного протокола?

Использовать команду permit.

1. Как задать действие правила сразу для нескольких портов?

Задать в команде диапазон портов с помощью range.

1. Как узнать номер правила в списке прав доступа?

Команда show access-list

1. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Команда ip access-list resequence.

**Вывод**

Освоила настройку прав доступа пользователей к ресурсам сети.