Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций

Кафедра защиты информации

Лабораторная работа № 7

«МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ. DMZ»

Шифр: 173

Проверила:

Белоусова Е.С.

Выполнила:

ст. гр. 961401

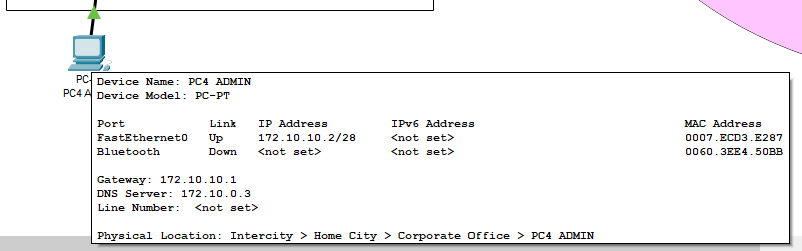
Савченко Е.А.

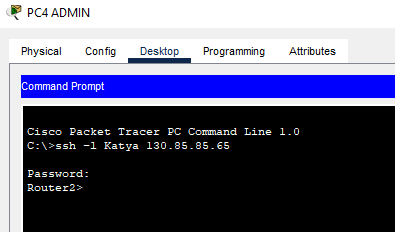
­

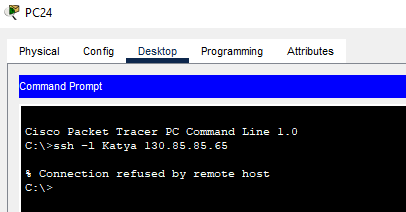
Минск 2022

***Цель*** *: изучить типы и принципы организации списков контроля доступа, овладеть практическими навыками конфигурации стандартных и расширенных списков контроля доступа.* **Ход работы:**

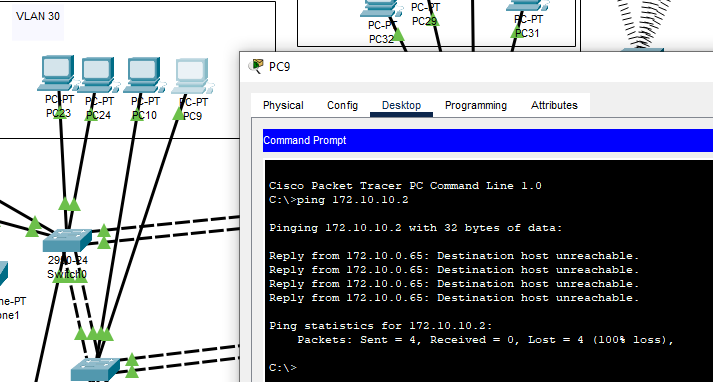
1. Конфигурация стандартных списков контроля доступа. Организовать следующие стандартные списки контроля доступа. 1.1. PC4 ADMIN выбран в качестве компьютера администратора, доступ по SSH разрешён только для данного устройства.

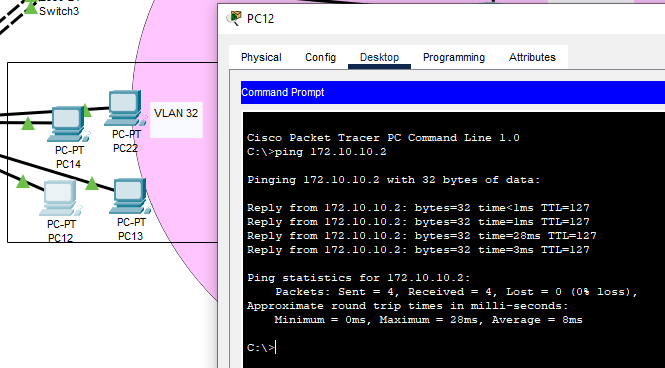




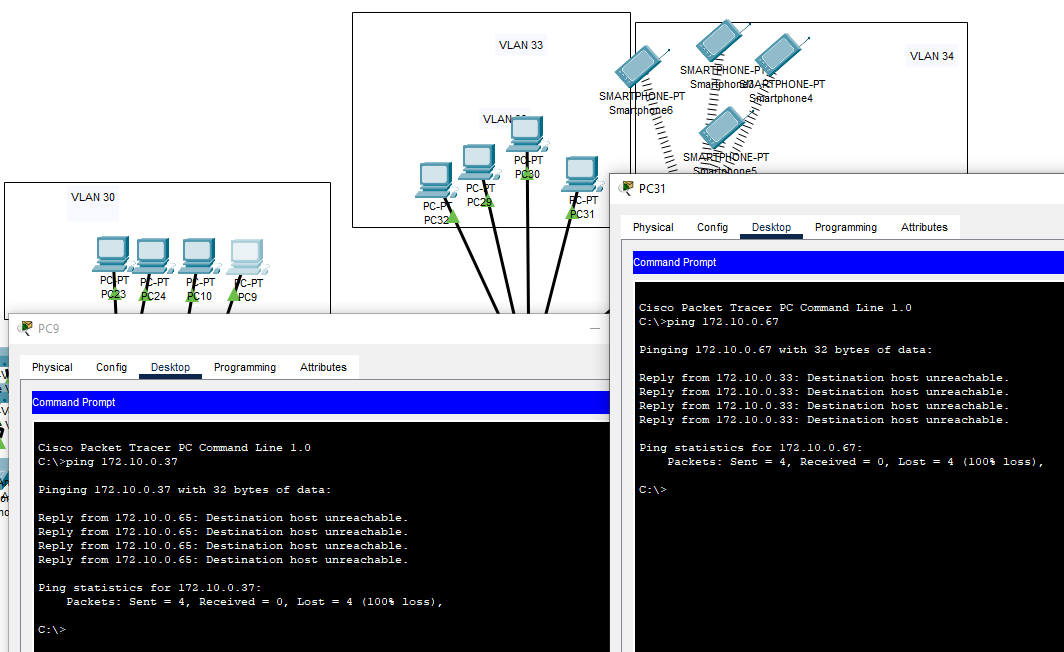


1.2 .Разрешаю доступ для VLAN 32, iot, security и адреса с радиуса

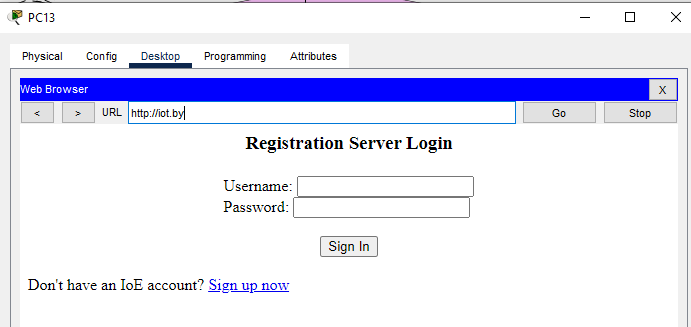


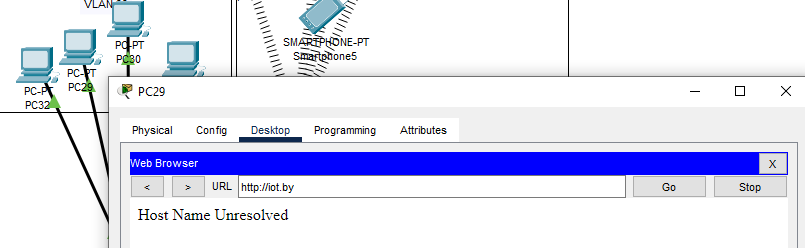


1.3 Запрещен взаимный доступ между VLAN 30 И VLAN 33



1.4 Доступ к серверам разрешен 172.10.0.34 и 172.10.0.75 (pc13), остальным устройствам из этих вланов-запрещен, всем остальным разрешен.





1.5 show access-lists

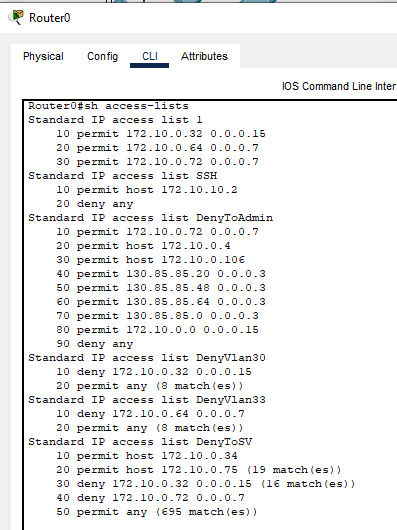
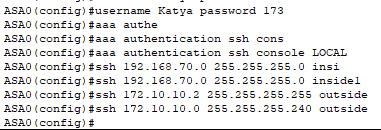


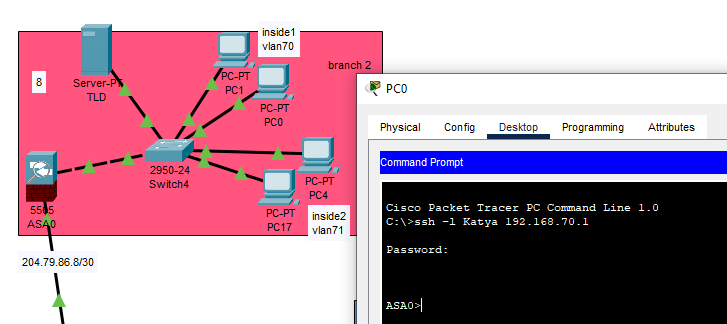
Таблица 1 – Настройка стандартных ACL

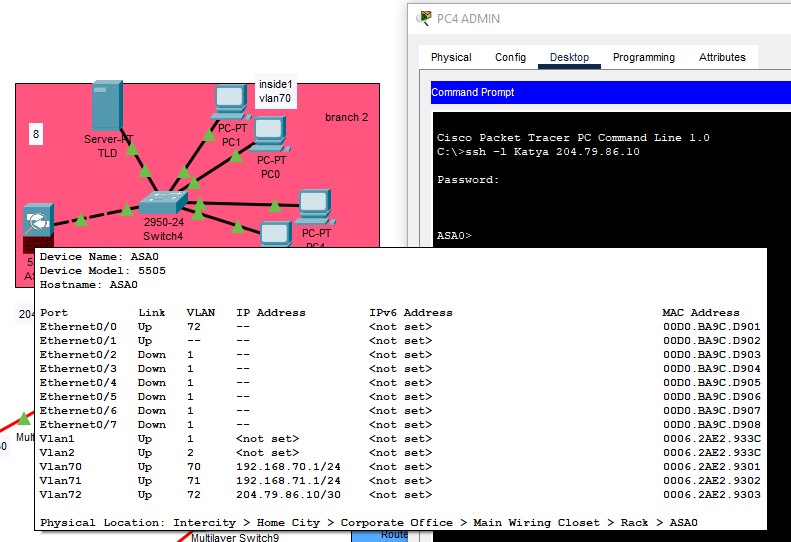
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Название ACL | Разрешить/ запретить доступ | Адресация | | Интерфейс маршрутизатора | |
| IP-адрес  устройства/сети | Обратная маска | Название | Направление |
| SSH | permit | 172.10.10.2 | 0.0.0.15 | VTY на каждом маршрутизаторе Branch1 | in |
| deny | any |  |
| Deny  ToAdmin | permit | 172.10.0.72  172.10.0.4  172.10.0.106  130.85.85.20  130.85.85.48  130.85.85.64  130.85.85.0  172.10.0.0 | 0.0.0.7  0.0.0.15  0.0.0.3  0.0.0.15 | fa 0/0.150 | out |
| deny | any |  |
| DenyVlan30 | deny | 172.10.0.32 | 0.0.0.15 | fa 0/0.30 | out |
| permit | any |  |
| DenyVlan33 | deny | 172.10.0.64 | 0.0.0.7 | fa 0/0.33 | out |
| permit | any |  |
| DenyToSV | permit | 172.10.0.34 |  | fa 0/0.38 | out |
| permit | 172.10.0.75 |  |
| deny | 172.10.0.32 | 0.0.0.15 |
| deny | 172.10.0.73 | 0.0.0.7 |
| permit | any |  |

2.1

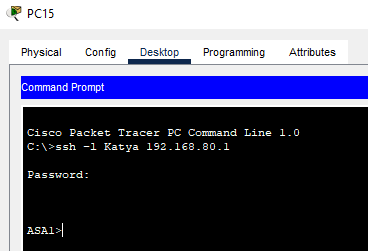
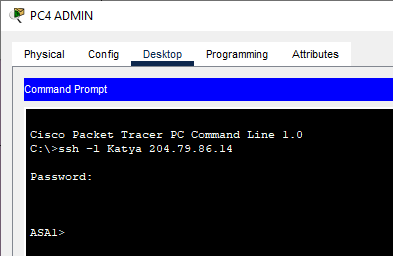


Разрешен доступ по ssh к asa0 из VLAN70 и PC4 ADMIN

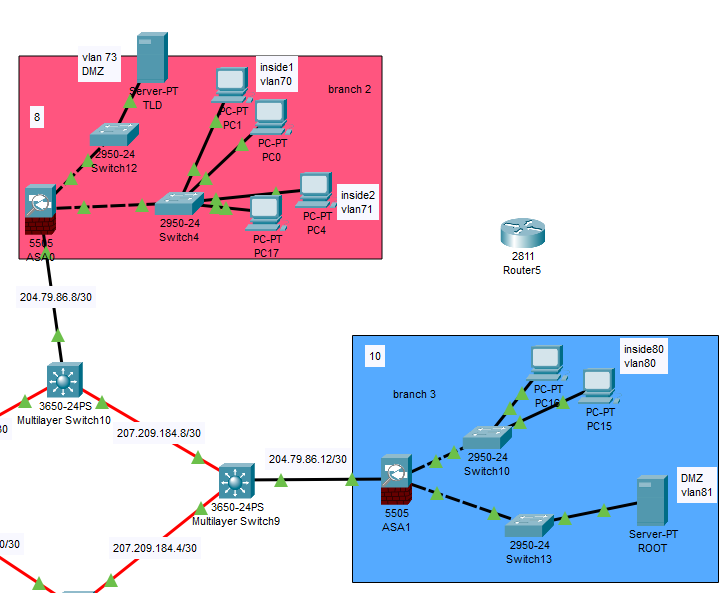


На R0 в ACL DenyToAdmin добавляю разрешение на ответ от внешнего интерфейса ASA

2.2

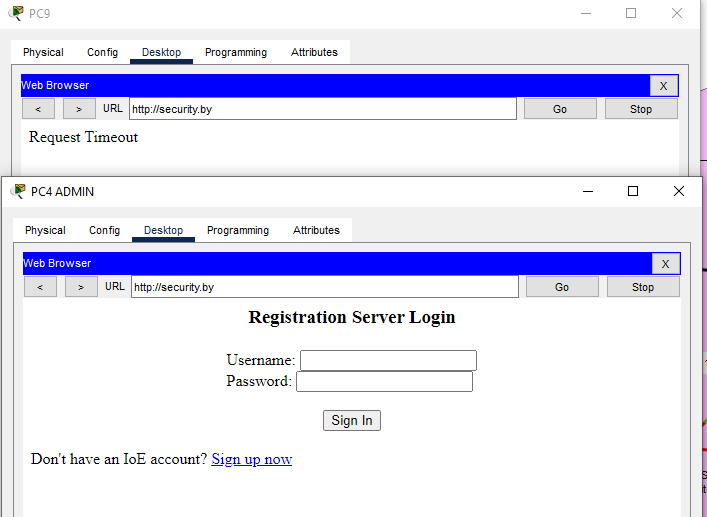


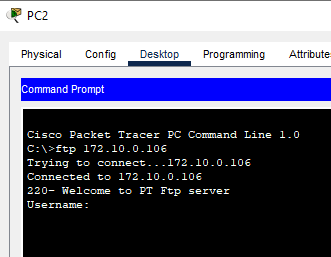
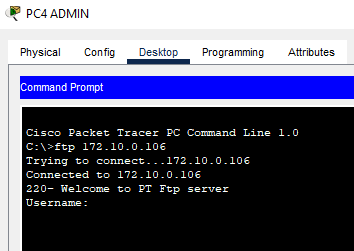
2.3 настроены DMZ

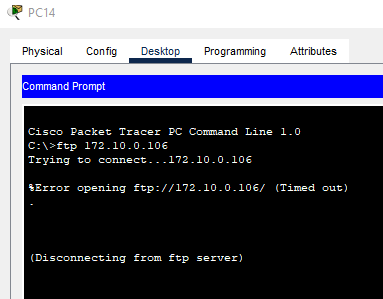


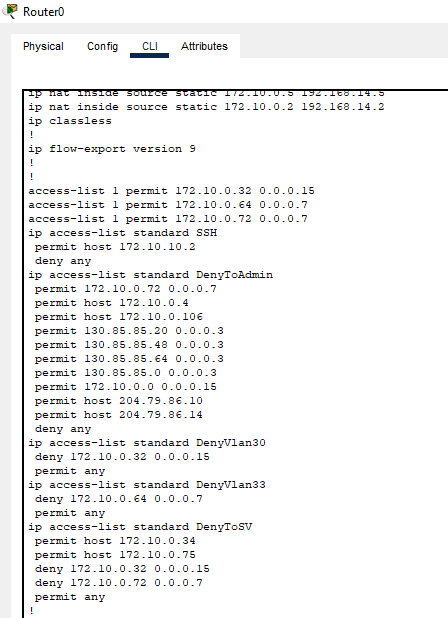
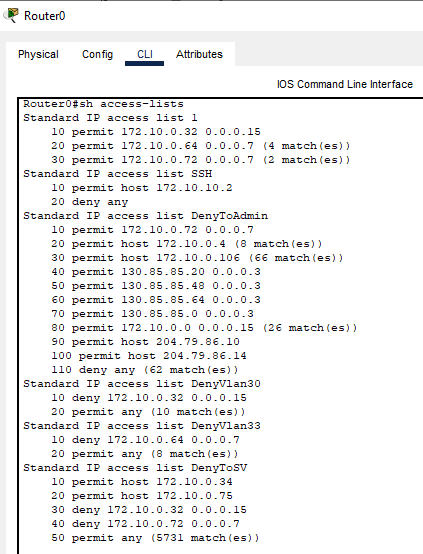
3. Конфигурация extended ACL

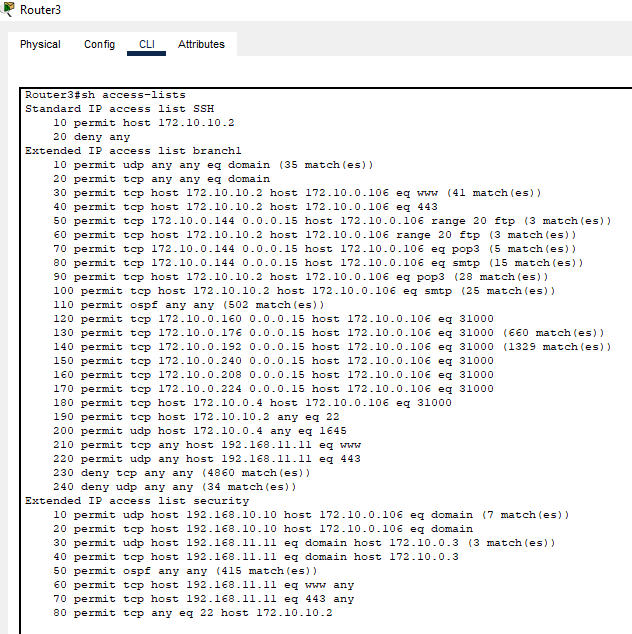
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| номер ACL | разрешить/  запретить | протокол/  номер прт | адресация | | название и направление интерфейса |
| ip-add/обр.маска отправителя | ----получателя |
| security | permit | udp/domain | 192.168.10.10 | 192.168.14.106 | gig 1/0/0 in |
| tcp/domain | 192.168.10.10 | 192.168.14.106 |
| udp/domain | 192.168.14.3 | 192.168.11.11 |
| tcp/domain | 192.168.14.3 | 192.168.11.11 |
| ospf | any | any |
| tcp/www | 192.168.11.11 | any |
| tcp/443 | 192.168.11.11 | any |
| tcp/22 | any | 172.10.10.2 |
| deny |  | any | any |
| branch1 | permit | udp/domain | any | any | gig 0/0/0  gig 0/2/0  in |
| tcp/domain | any | any |
| tcp/www | 172.10.10.2 | 192.168.14.106 |
| tcp/443 | 172.10.10.2 | 192.168.14.106 |
| tcp/range 20 21 | 172.10.0.145  0.0.0.15 | 192.168.14.106 |
| tcp/range 20 21 | 172.10.10.2 | 192.168.14.106 |
| tcp/pop3 | 172.10.10.2 | 192.168.14.106 |
| tcp/pop3 | 172.10.0.145  0.0.0.15 | 192.168.14.106 |
| tcp/smtp | 172.10.0.145  0.0.0.15 | 192.168.14.106 |
| tcp/smtp | 172.10.10.2 | 192.168.14.106 |
| ospf | any | any |
| tcp /31000 | 172.10.0.160 0.0.0.15  172.10.0.0.176  0.0.0.15  172.10.0.0.192  0.0.0.15  172.10.0.0.240  0.0.0.15  172.10.0.0.208  0.0.0.15  172.10.0.224  0.0.0.15  host 172.10.0.4 | 192.168.14.106 |
| tcp/22 | 172.10.10.2 | any |
| udp/1645 | 172.10.0.4 | any |
| tcp /www | any | 192.168.11.11 |
| udp/443 | any | 192.168.11.11 |
| deny | tcp  udp | any | any |

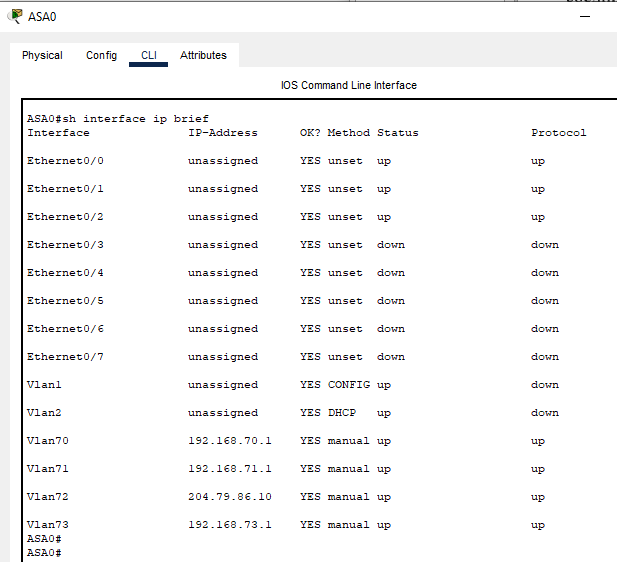
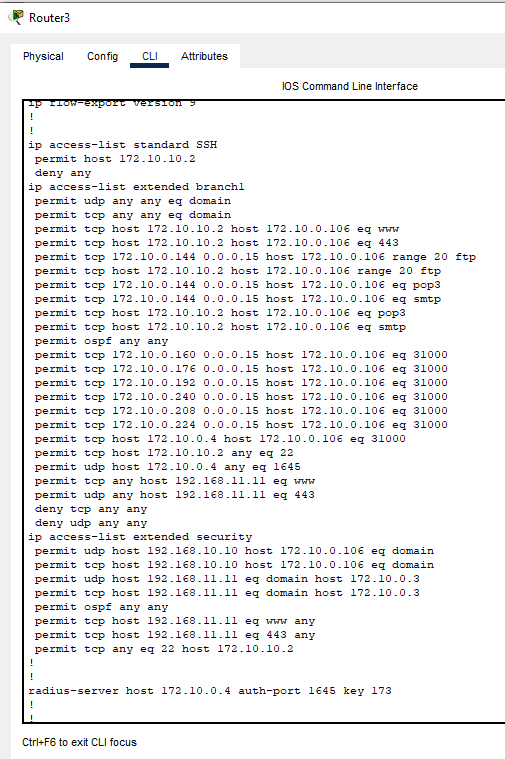


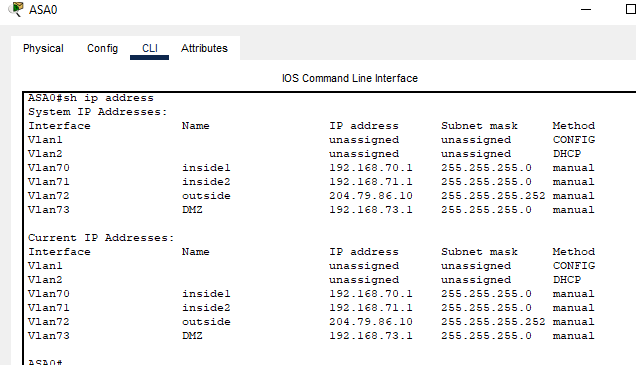


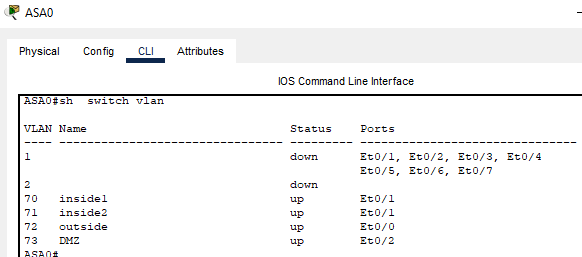


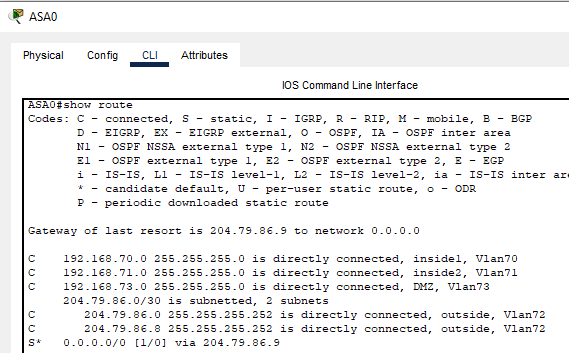


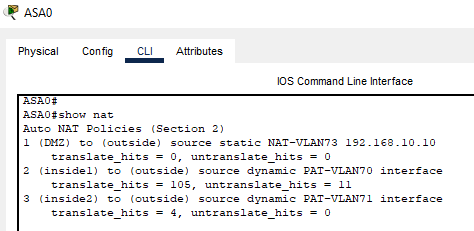


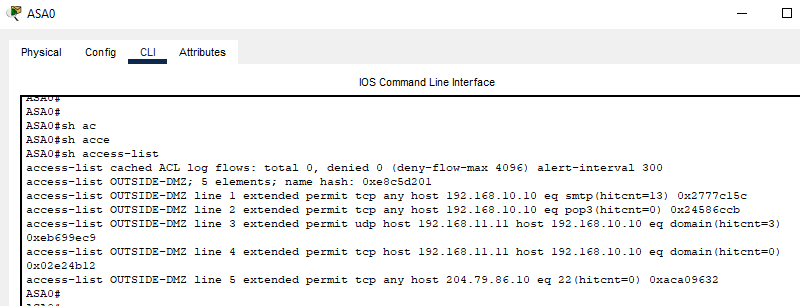


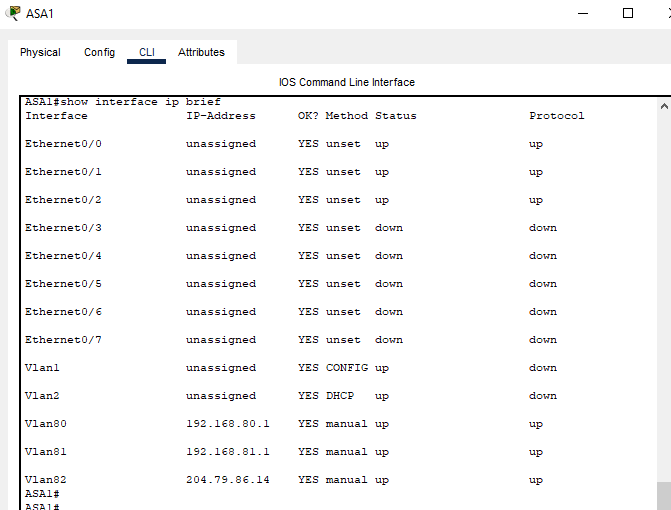


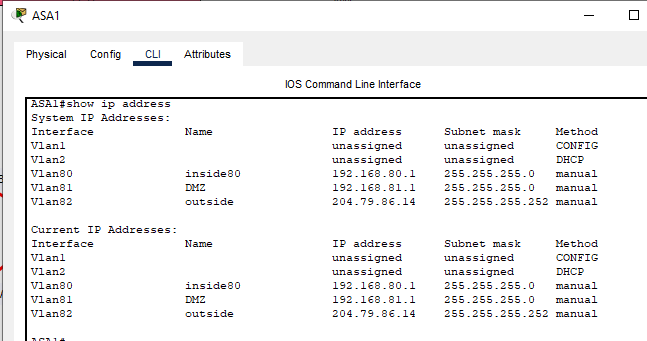


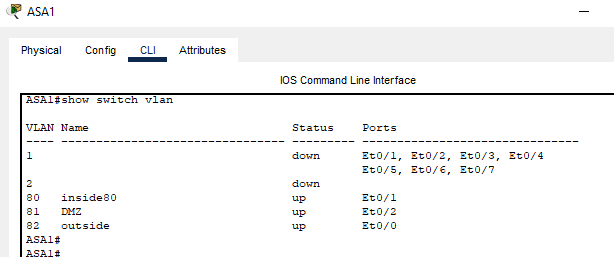


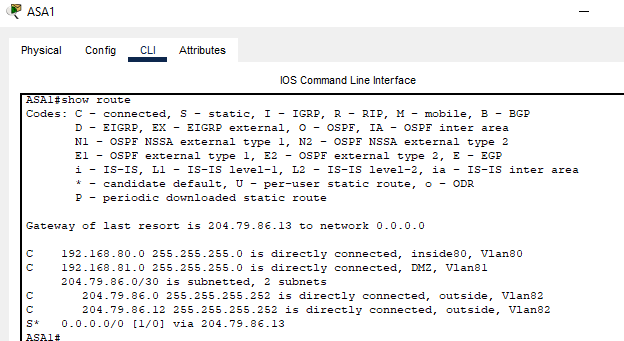


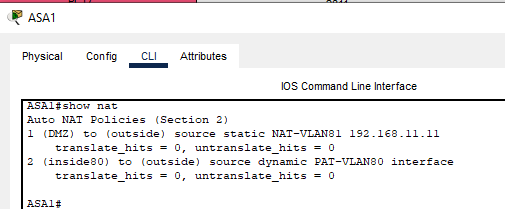


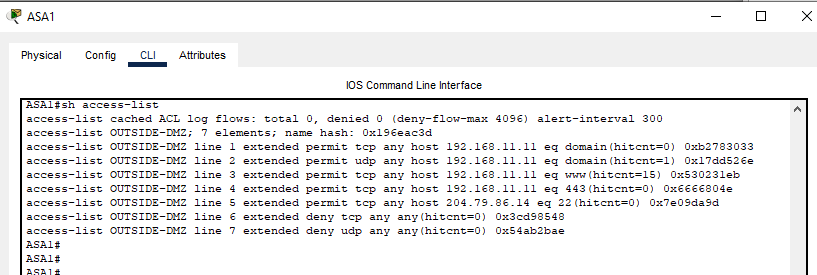












Вывод: в данной лабораторной работе я познакомилась с двумя основными типами списков доступа: стандартными (standart) и расширенными (extended). Стандартные - обрабатывают только входящие IP адреса источников и ищут соответствие правил, в которых указаны IP-адреса отправителя. Расширенные списки работают со IP-адресами источников и отправителей одновременно и дополнительно проверяют протоколы

