**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,**

**СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Принципы организации глобальных вычислительных сетей

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

ACL

*(тема отчета)*

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студенты группы ИКТЗ-83:

Громов А. А

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С,

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А., ст. преп.

*(Ф.И.О., должн.) (подпись)*

Оглавление

[5.1.8 - Packet Tracer. Настройка нумерованных стандартных списков контроля доступа для IPv4 3](#_Toc98865256)

[5.1.9 - Packet Tracer. Настройка именованных стандартных списков контроля доступа (ACL) IPv4 6](#_Toc98865257)

[5.2.7 - Packet Tracer. Настройка и модификация стандартных списков контроля доступа для IPv4 9](#_Toc98865258)

[5.4.12 - Настройка расширенных списков контроля доступа. Сценарий 1 17](#_Toc98865259)

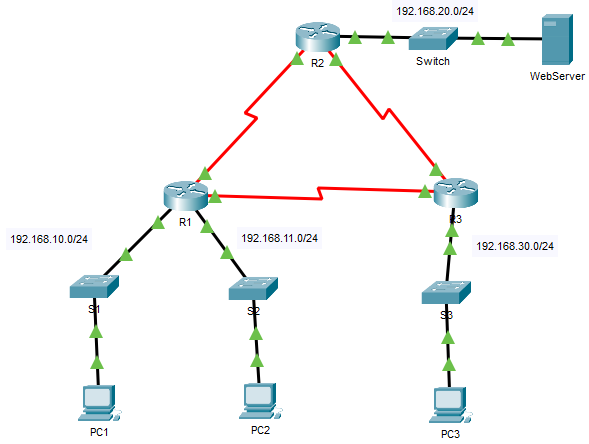
[5.4.13 - Packet Tracer. Настройка расширенных списков контроля доступа. Сценарий 2 21](#_Toc98865260)

[5.5.1 - Packet Tracer. Реализация ACL IPv4 (повышенный уровень сложности) 26](#_Toc98865261)

[5.5.2 - Packet Tracer. Настройка и проверка расширенных ACL IPv4 30](#_Toc98865262)

# 5.1.8 - Packet Tracer. Настройка нумерованных стандартных списков контроля доступа для IPv4

Топология сети



Задачи

Часть 1. Планирование реализации списка контроля доступа

Часть 2. Настройка, применение и проверка стандартных списков контроля доступа

Часть 1. Планирование реализации ACL

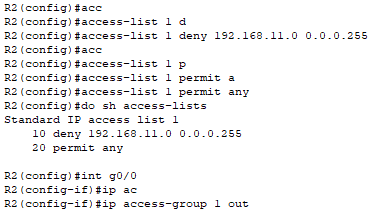
Для начала выполнения работы убедились, что ping-запросы проходят успешно, а на маршрутизаторах R2 и R3 настроены правила сетевой безопасности (ACL-списки), которые совпадают с условиями задания.

Часть 2. Настройка, применение и проверка стандартного ACL

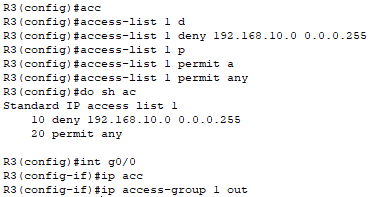
Наторим и применим нумерованный стандартный ACL на R2.

Создадим ACL-список с номером 1 на маршрутизаторе R2, установив запрет доступа к сети 192.168.20.0/24 от сети 192.168.11.0/24. Далее, необходимо создать правило, которое будет пропускать оставшийся трафик (не удовлетворяющий правилу выше).

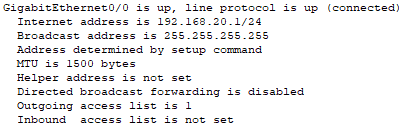
Просмотрим получившиеся правила и их настройку, а затем созданный ACL-список применим к интерфейсу g0/0/0

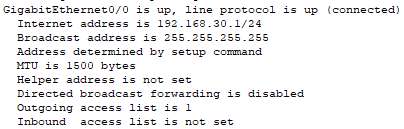


Аналогично создадим ACL-список на R3

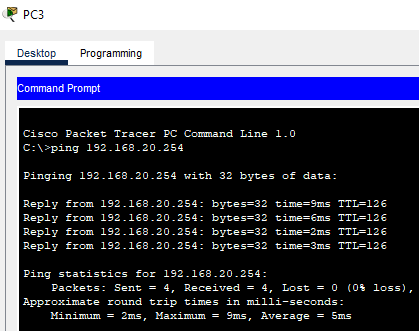
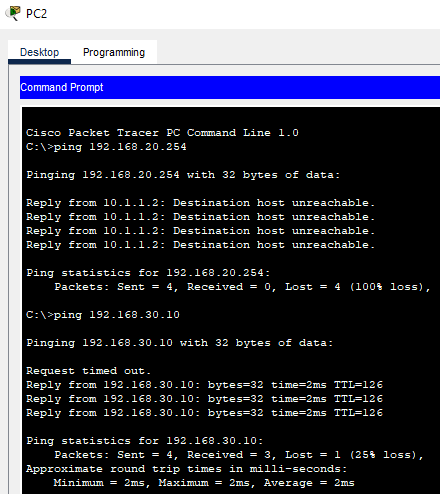
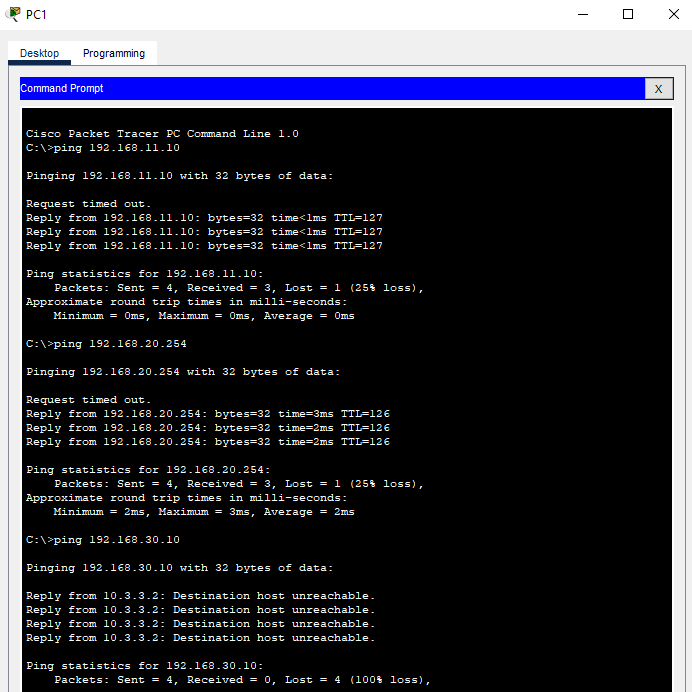


Просмотрим конфигурации маршрутизаторов, чтобы проверить успешность применения списков контроля доступа





Проверим связь, после размещения двух ACL-списков



Просмотрим конфигурации списков контроля доступа, чтобы убедиться в их работоспособности



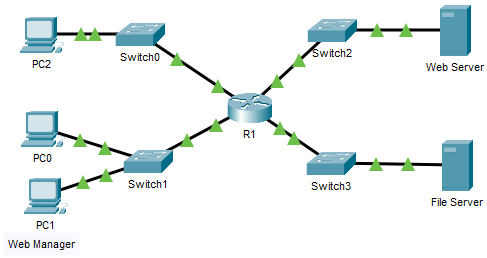


# 5.1.9 - Packet Tracer. Настройка именованных стандартных списков контроля доступа (ACL) IPv4

Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | F0/0 | 192.168.10.1 | 255.255.255.0 | — |
| *R1* | F0/1 | 192.168.20.1 | 255.255.255.0 | *—* |
| *R1* | E0/0/0 | 192.168.100.1 | 255.255.255.0 | *—* |
| *R1* | E0/1/0 | 192.168.200.1 | 255.255.255.0 | *—* |
| File Server | NIC | 192.168.200.100 | 255.255.255.0 | 192.168.200.1 |
| Web server | NIC | 192.168.100.100 | 255.255.255.0 | 192.168.100.1 |
| PC0 | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC1 | NIC | 192.168.20.4 | 255.255.255.0 | 192.168.20.1 |
| PC2 | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |

Топология сети



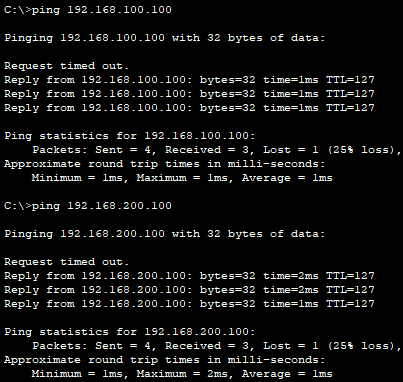
Задачи

Часть 1. Настройка и применение стандартного именованного списка контроля доступа

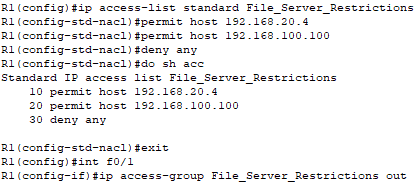
Часть 2. Проверка реализации списка контроля доступа

Часть 1. Настройка и применение именованного стандартного списка

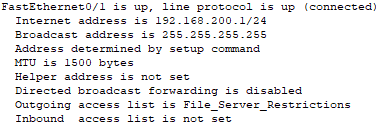
Перед выполнением работы проверим доступ к Web Server и File Server при помощи команды ping

****

Настроим на R1 список контроля доступа и применим его к интерфейсу f0/1

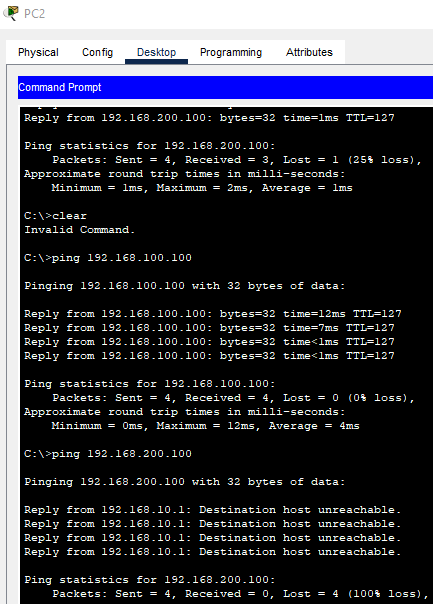
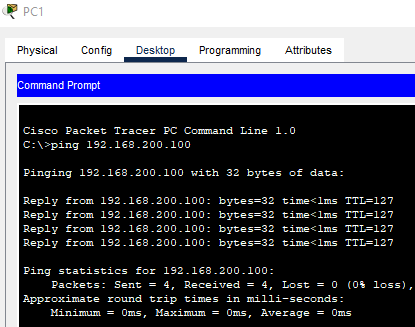
****

Проверим успешность выполнения команд:

****

Часть 2. Проверка реализации ACL

Проверим работоспособность созданных списков

****

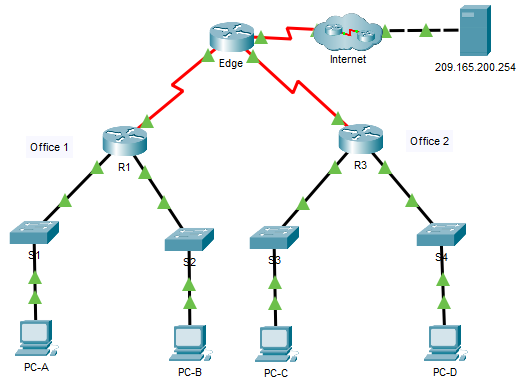
На рисунке видно, что списки контроля доступа работают успешно, так как адрес 192.168.200.100 перестал быть доступен для PC2.

# 5.2.7 - Packet Tracer. Настройка и модификация стандартных списков контроля доступа для IPv4

Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/0/0 | 192.168.10.1 | 255.255.255.0 | — |
| *R1* | G0/0/1 | 192.168.20.1 | 255.255.255.0 | *—* |
| *R1* | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | *—* |
| Edge | S0/1/0 | 10.1.1.2 | 255.255.255.252 | — |
| *Edge* | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | *—* |
| *Edge* | S0/2/1 | 209.165.200.225 | 255.255.255.224 | *—* |
| R3 | G0/0/0 | 192.168.30.1 | 255.255.255.0 | — |
| *R3* | G0/0/1 | 192.168.40.1 | 255.255.255.0 | *—* |
| *R3* | S0/1/1 | 10.2.2.1 | 255.255.255.252 | *—* |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S2 | VLAN 1 | 192.168.20.11 | 255.255.255.0 | 192.168.20.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| S4 | VLAN 1 | 192.168.40.11 | 255.255.255.0 | 192.168.40.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |
| PC-D | NIC | 192.168.40.3 | 255.255.255.0 | 192.168.40.1 |

Топология сети



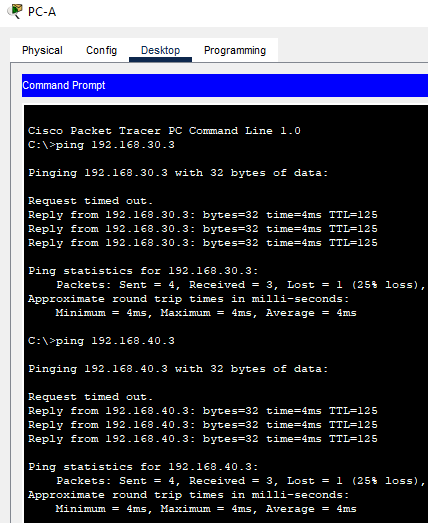
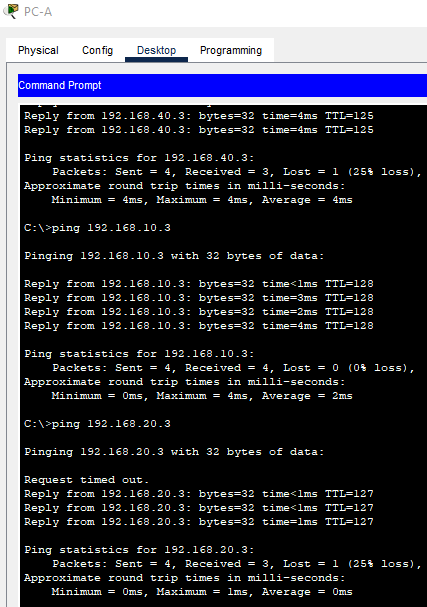
Задачи

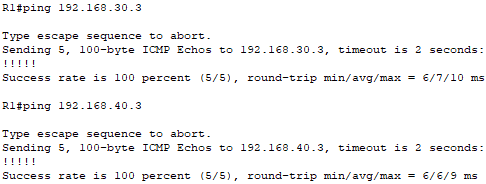
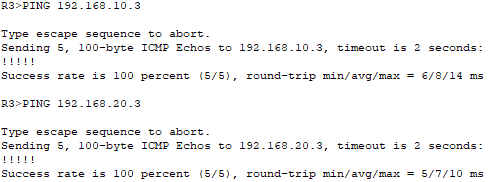
Часть 1. Проверка связи

Часть 2. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

Часть 3. Изменение стандартного ACL-списка

Часть 1. Проверка связи

****

****

Часть 2. Настройка и проверка стандартных нумерованных и именованных списков управления доступом

**Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?**

Ответ: 0.0.0.255

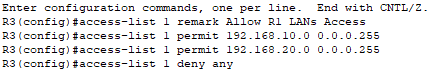
**Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?**

Ответ: R3

**На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?**

Ответ: на выход интерфейса g0/0/0.

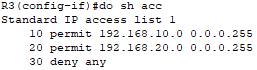
Настроим ACL на R3

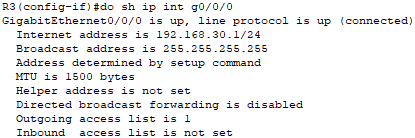
****

Далее, применим данный список к интерфейсу g0/0/0

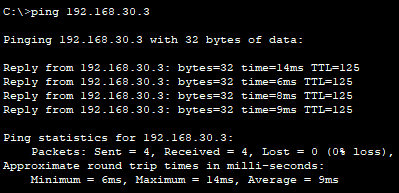
****

Для просмотра полного списка контроля доступа 1 необходимо использовать команду *show access-list*. Чтобы посмотреть, где и в каком направлении был применен ACL, нужно прописать *show ip interface <интерфейс>*

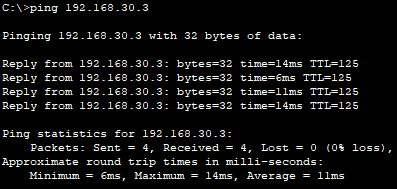
****

****

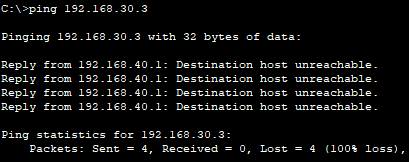
Проверим связь между сетями 192.168.10.0/24 и 192.168.30.0/24

****

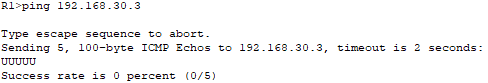
Проверим связь между сетями 192.168.20.0/24 и 192.168.30.0/24



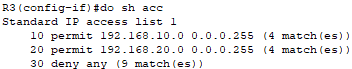
Проверим связь между PC-D и PC-С

****

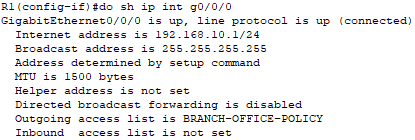
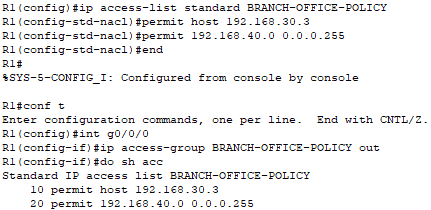
Проверим связь между R1 и PC-С

****

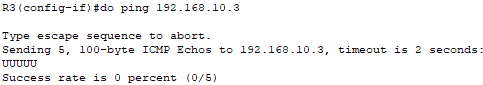
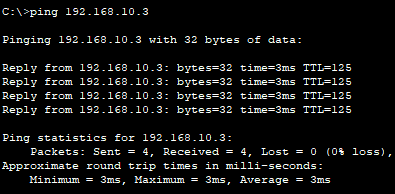
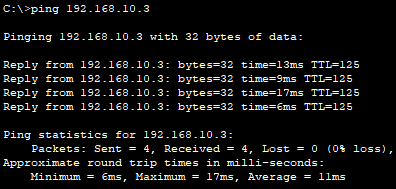
Проверим работу ACL на R3

****

Аналогично создадим именованный список контроля доступа на R1 и проверим его применение

****

Проверим связь после применения ACL:

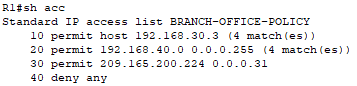


Часть 3. Изменение стандартного ACL-списка

Просмотрим текущее состояние списка контроля доступа на R1

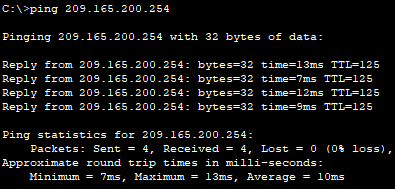


Добавим новые строки в ACL как на рисунке 25 и проверим его изменения



Исходя из этого, можно сделать вывод, что повторное применение списка к интерфейсу не требуется.

Проверим связь между сетями 209.165.200.224/27 и 192.168.10.0/24



Вопросы для повторения

**Как вы видите, стандартные ACL-списки достаточно эффективны и полезны. Зачем вам когда-либо понадобилось использовать расширенные списки ACL?**

Ответ: они могут понадобится для фильтрации трафика и ограничения доступа.

**В большинстве случаев при использовании именованного ACL-списка требуется введение большего количества строк, нежели при использовании нумерованного ACL-списка. Почему вы бы предпочли использовать именованный ACL-список, а не нумерованный?**

Ответ: потому что можно использовать только значащие имена, чтобы сразу определять для чего они используются.

# 5.4.12 - Настройка расширенных списков контроля доступа. Сценарий 1

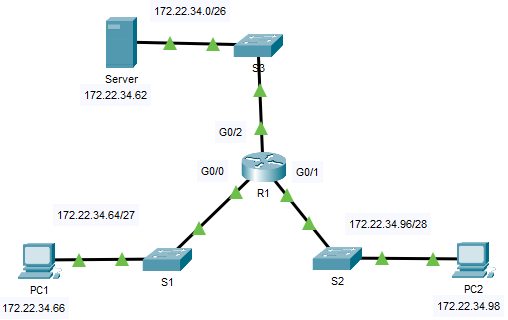


Рисунок – Топология сети

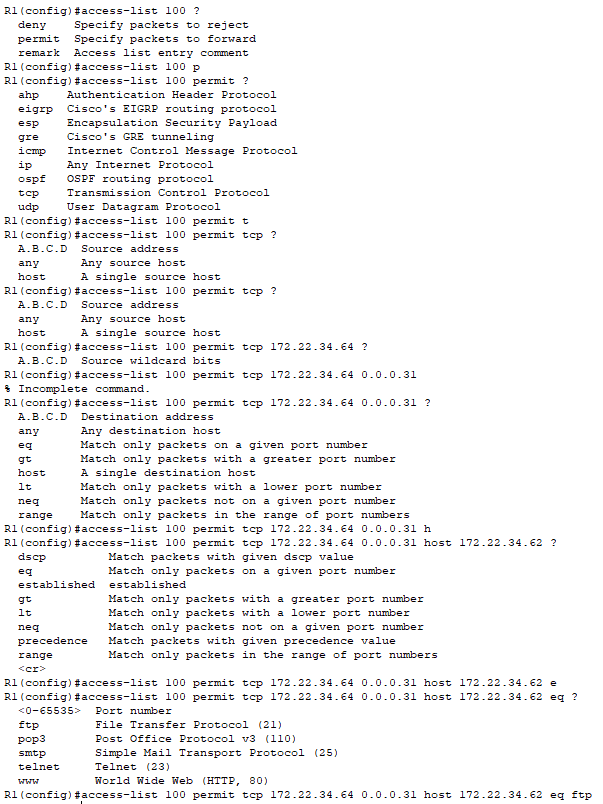
Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/0 | 172.22.34.65 | 255.255.255.224 | — |
| *R1* | G0/1 | 172.22.34.97 | 255.255.255.240 | *—* |
| *R1* | G0/2 | 172.22.34.1 | 255.255.255.192 | *—* |
| Сервер | NIC | 172.22.34.62 | 255.255.255.192 | 172.22.34.1 |
| PC1 | NIC | 172.22.34.66 | 255.255.255.224 | 172.22.34.65 |
| PC2 | NIC | 172.22.34.98 | 255.255.255.240 | 172.22.34.97 |

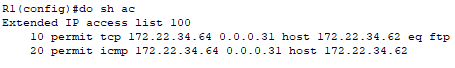
Задачи

Часть 1. Настройка, применение и проверка расширенного нумерованного списка ACL

На маршрутизаторе R1 настроим ACL-список, который будет разрешать FTP и ICMP



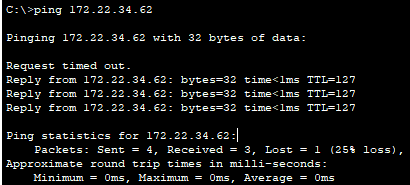
Проверим их создание при помощи команды *show access-list*

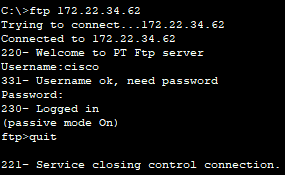


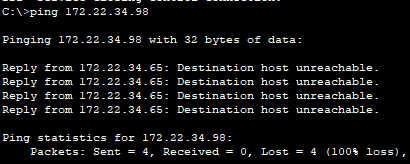
Применим данный список на вход к интерфейсу g0/0



Проверим его реализацию

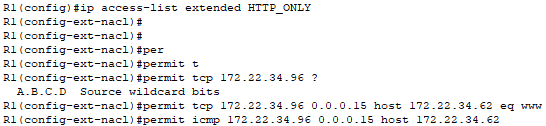




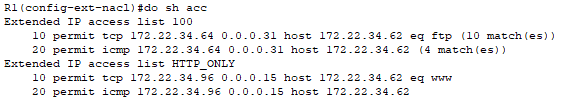


Часть 2. Настройка, применение и проверка расширенного именованного ACL

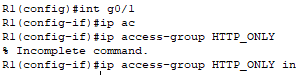
Создадим расширенный именной список контроля доступа для разрешения HTTP и ICMP трафика



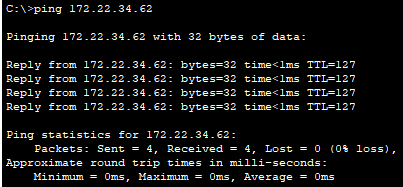
Проверим его создание

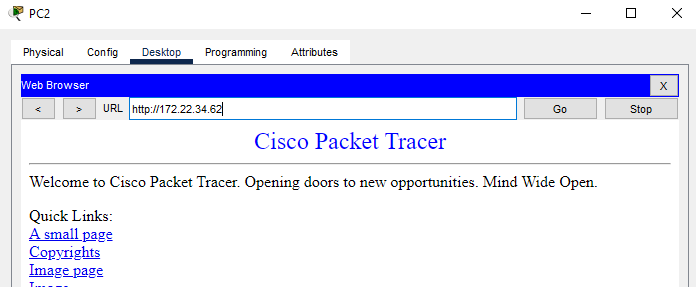


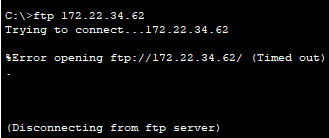
Применим созданный список к интерфейсу g0/1



Проверим реализацию списка контроля доступа







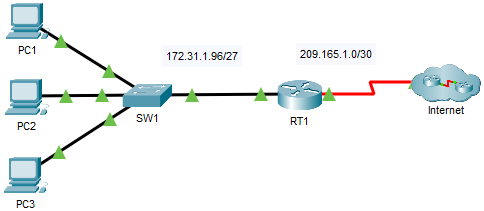
Получаем списки контроля доступа, которые полностью удовлетворяют поставленному заданию.

# 5.4.13 - Packet Tracer. Настройка расширенных списков контроля доступа. Сценарий 2

Таблица адресации

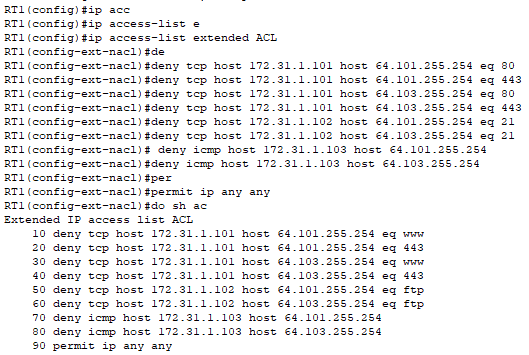
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| RT1 | G0/0 | 172.31.1.126 | 255.255.255.224 | — |
| RT1 | S0/0/0 | 209.165.1.2 | 255.255.255.252 | — |
| PC1 | NIC | 172.31.1.101 | 255.255.255.224 | 172.31.1.126 |
| PC2 | NIC | 172.31.1.102 | 255.255.255.224 | 172.31.1.126 |
| PC3 | NIC | 172.31.1.103 | 255.255.255.224 | 172.31.1.126 |
| Server1 | NIC | 64.101.255.254 | Пустой экран | Пустой экран |
| Server2 | NIC | 64.103.255.254 | Пустой экран | пусто |

Топология сети



Часть 1. Настройка именованного расширенного списка контроля доступа

Создадим список контроля доступа согласно условиям задания и проверим его создание.

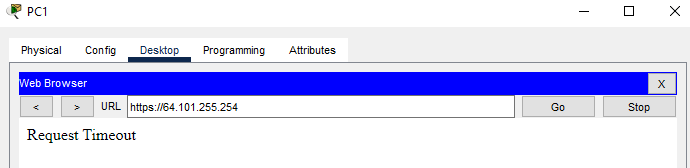


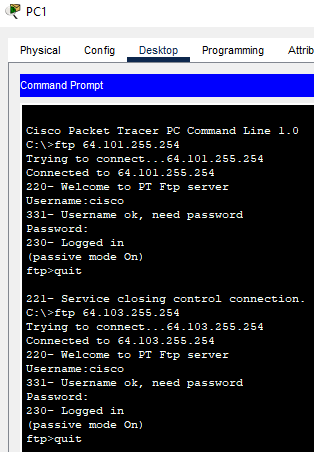
Данный список запрещает доступ от PC1 к Server1 и Server2 по HTTP и HTTPS, от PC2 к сервисам FTP, а PC3 отправлять эхо-запросы.

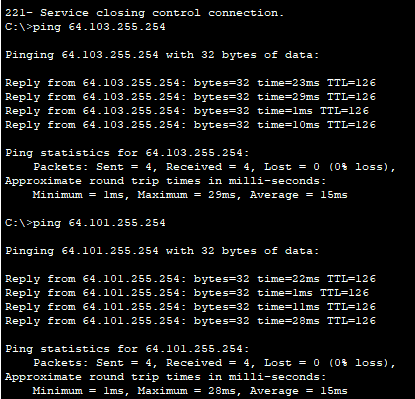
Применим данный список на вход интерфейса g0/0

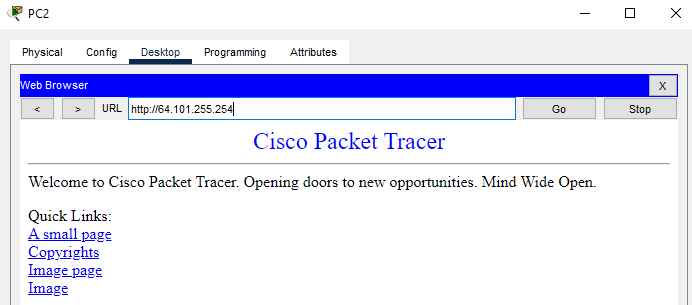


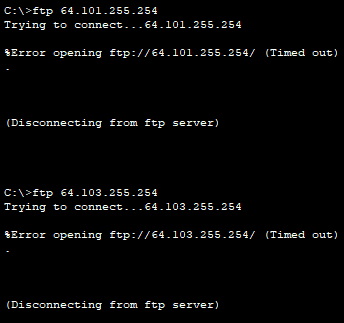
Проверим его работоспособность

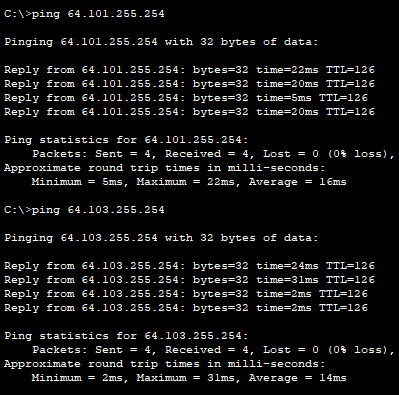


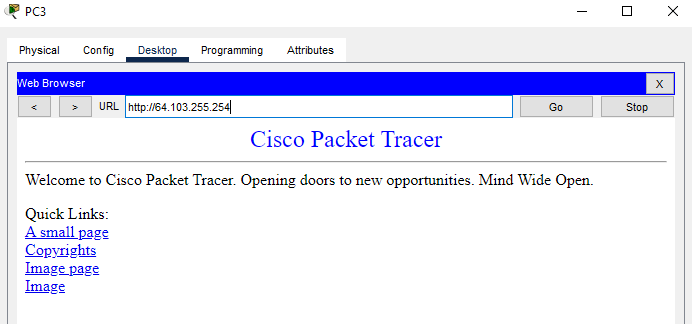


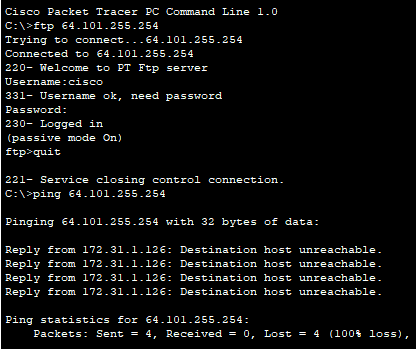




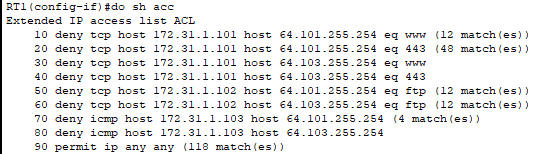








Просмотрим на маршрутизаторе, как работал ACL



# 5.5.1 - Packet Tracer. Реализация ACL IPv4 (повышенный уровень сложности)

Топология сети

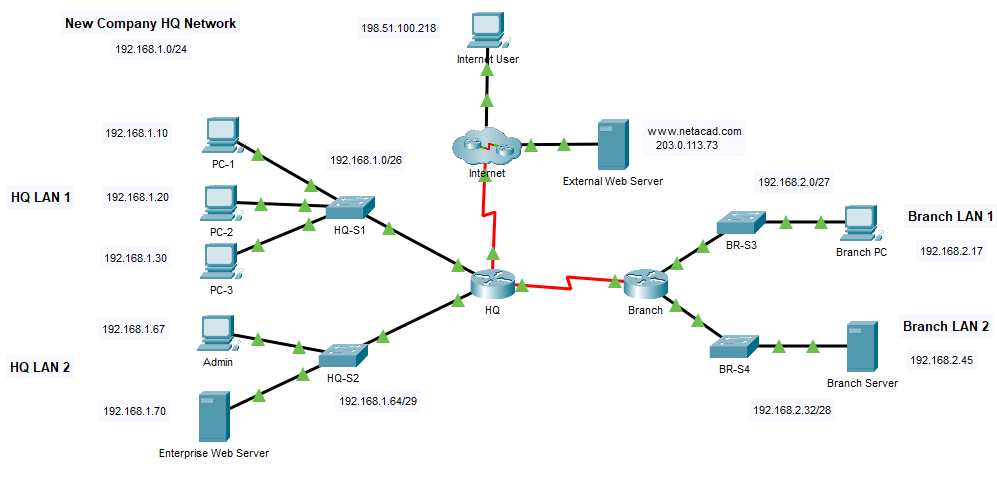


Таблица адресации

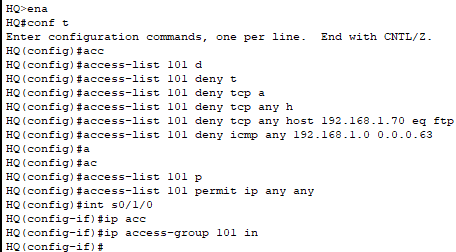
| Устройство | Интерфейс | IP-адрес |
| --- | --- | --- |
| Branch | G0/0/0 | 192.168.1.1/26 |
|  | G0/0/1 | 192.168.1.65/29 |
|  | S0/1/0 | 192.0.2.1/30 |
|  | S0/1/1 | 192.168.3.1/30 |
| HQ | G0/0/0 | 192.168.2.1/27 |
|  | G0/0/1 | 192.168.2.33/28 |
|  | S0/1/1 | 192.168.3.2/30 |
| PC-1 | NIC | 192.168.1.10/26 |
| PC-2 | NIC | 192.168.1.20/26 |
| PC-3 | NIC | 192.168.1.30/26 |
| Admin | NIC | 192.168.1.67/29 |
| Enterprise Web Server | NIC | 192.168.1.70/29 |
| Branch PC | NIC | 192.168.2.17/27 |
| Branch Server | NIC | 192.168.2.45/28 |
| Internet User | NIC | 198.51.100.218/24 |
| External Web Server | NIC | 203.0.113.73/24 |

Задачи

* Настройка маршрутизатора со стандартными именованными ACL.
* Настройка маршрутизатора с расширенными именованными ACL.
* Настройте маршрутизатор с расширенными ACL в соответствии с конкретными требованиями.
* Настройка ACL для управления доступом к терминальным линиям сетевых устройств.
* Настройте соответствующие интерфейсы маршрутизатора с ACL в соответствующем направлении.
* Проверка работы настроенных списков ACL.

Выполним настройку маршрутизатора HQ. Для этого необходимо сконфигурировать списки контроля доступа.

Настроим первый ACL



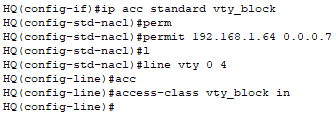
Данным списком был заблокирован доступ к FTP к Enterprise Web Server и запрещен ICMP трафик из сети LAN 1 HQ.

Настроим второй ACL



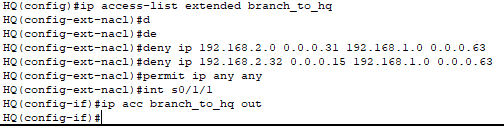
Данное правило блокирует весь трафик из сети LAN 1 HQ к Branch Server.

Настроим третий ACL



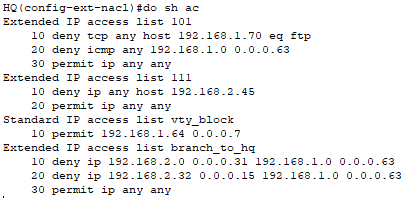
Данное правило разрешает доступ к линям VTY из сети HQ LAN 2.

Настроим четвертый ACL

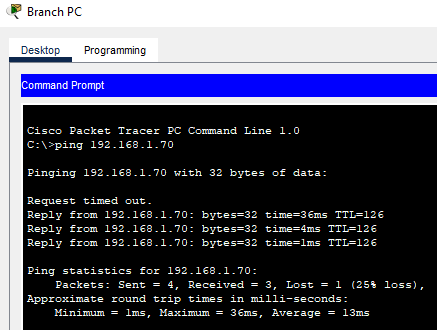


Данное правило блокирует все подключения к HQ 1 из других сетей.

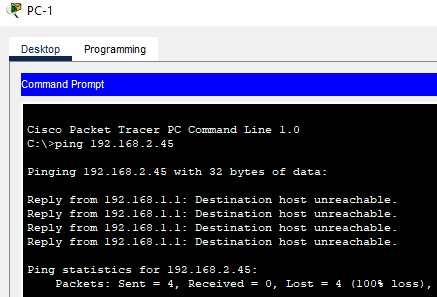
Просмотрим созданные списки

****

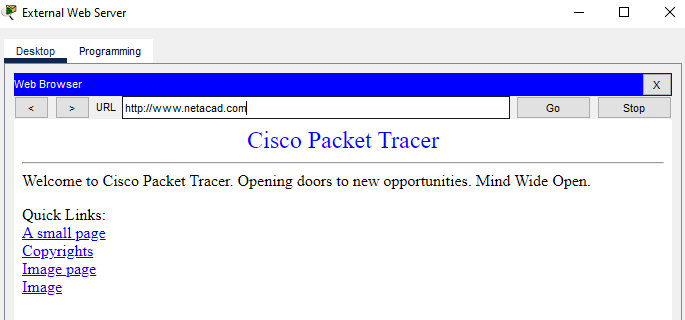
Проверим работу ACL

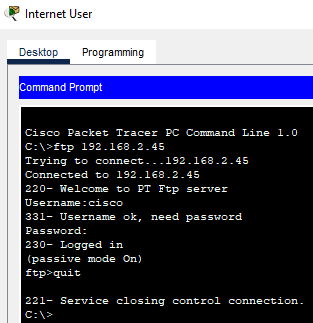


Ping оказался успешным, так как нет запретов на ICMP из данной сети.



Трафик не проходит, так как он был запрещен.



****

# 5.5.2 - Packet Tracer. Настройка и проверка расширенных ACL IPv4

Топология сети

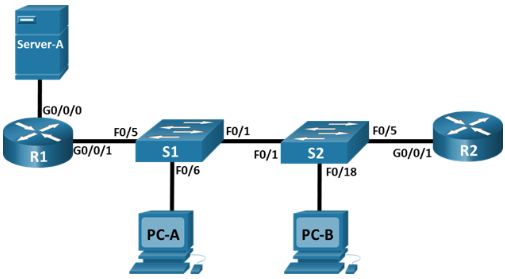


Таблица адресация

| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| --- | --- | --- | --- | --- |
| R1 | G0/0/1 | — | — | — |
| *R1* | G0/0/1.20 | 10.20.0.1 | 255.255.255.0 | *—* |
| *R1* | G0/0/1.30 | 10.30.0.1 | 255.255.255.0 | *—* |
| *R1* | G0/0/1.40 | 10.40.0.1 | 255.255.255.0 | *—* |
| *R1* | G0/0/1.1000 | — | — | *—* |
| *R1* | G0/0/0 | 172.16.1.1 | 255.255.255.0 | *—* |
| R2 | G0/0/1 | 10.20.0.4 | 255.255.255.0 | — |
| S1 | VLAN 20 | 10.20.0.2 | 255.255.255.0 | 10.20.0.1 |
| S2 | VLAN 20 | 10.20.0.3 | 255.255.255.0 | 10.20.0.1 |
| PC-A | NIC | 10.30.0.10 | 255.255.255.0 | 10.30.0.1 |
| PC-B | NIC | 10.40.0.10 | 255.255.255.0 | 10.40.0.1 |
| Server-A | NIC | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |

Таблица VLAN

| **VLAN** | **Имя** | **Назначенный интерфейс** |
| --- | --- | --- |
| 20 | Management | S2: F0/5 |
| 30 | Operations | S1: F0/6 |
| 40 | Sales | S2: F0/18 |
| 999 | ParkingLot | S1: F0/2-4, F0/7-24, G0/1-2  S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2 |
| 1000 | Native | — |

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка сетей VLAN на коммутаторе

Часть 3. Настройка магистральных каналов

Часть 4. Настройка маршрутизации

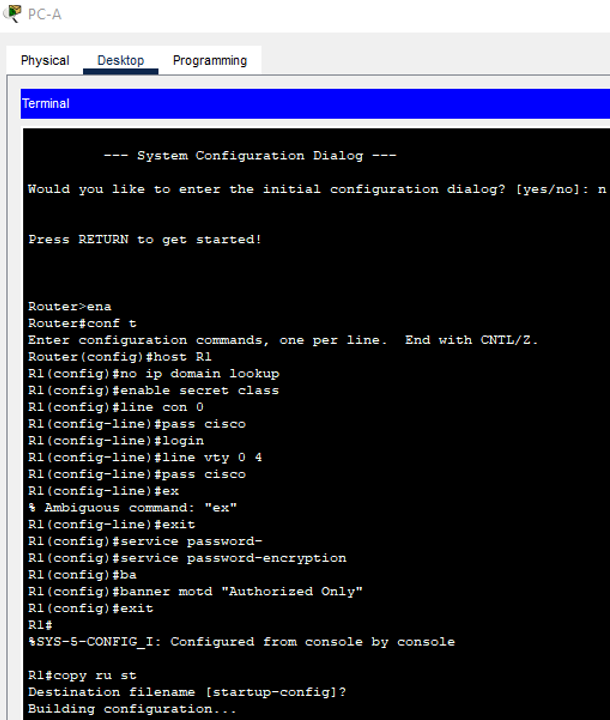
Часть 5. Настройка удаленного доступа

Часть 6. Проверка связи

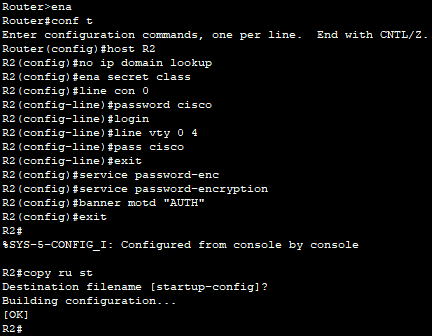
Часть 7. Настройка и проверка списков расширенного контроля доступа

Часть 1. Создание сети и настройка основных параметров устройства

Совершим базовую настройку маршрутизаторов

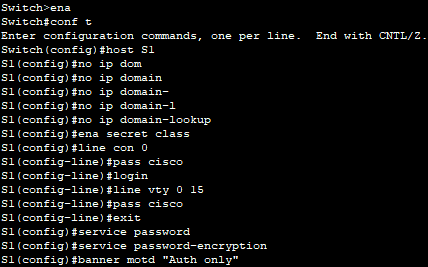


Базовая настройка R1

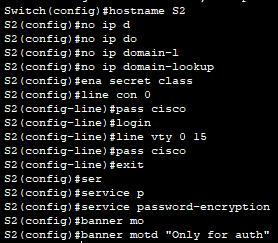
****

Базовая настройка R2

Базовая настройка коммутаторов

****

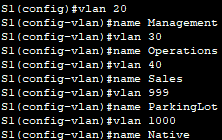
Базовая настройка S1

****

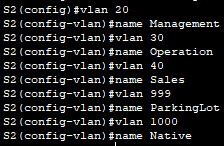
Базовая настройка S2

Часть 2. Настройка сетей VLAN на коммутаторах

Создадим VLAN на обоих коммутаторах

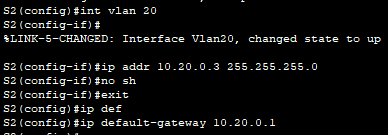
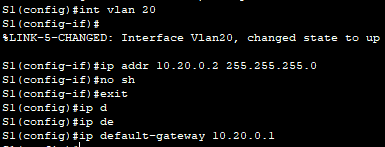
****

Настройка VLAN на S1

****

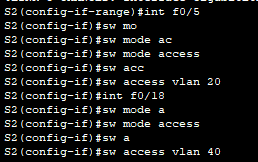
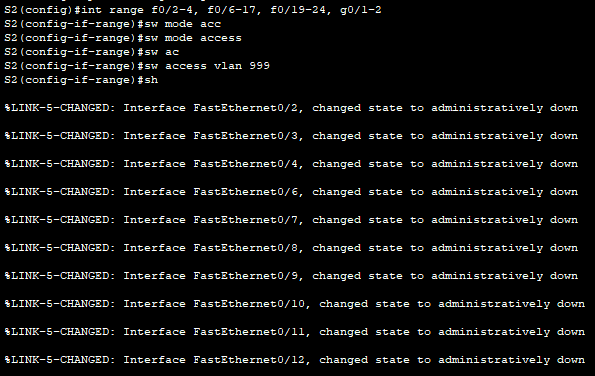
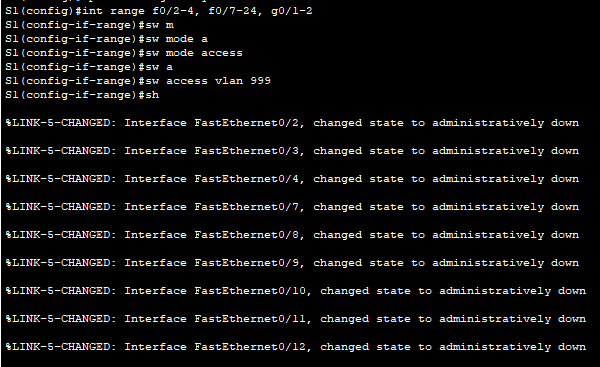
Настройка VLAN на S2

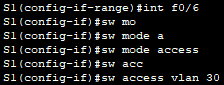
Настроим интерфейс управления и шлюз по умолчанию на каждом коммутаторе

****

Настройка интерфейса управления и шлюза по умолчанию на коммутаторах

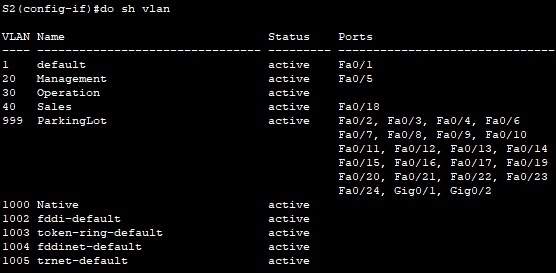
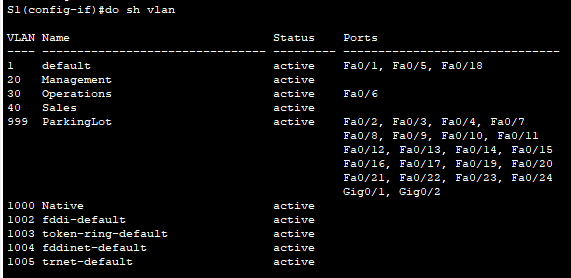
Применим созданные списки к интерфейсам на обоих коммутаторах

****

****

Настройка VLAN

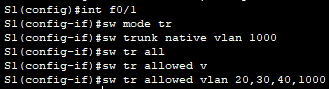
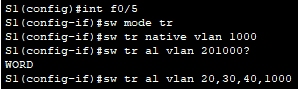
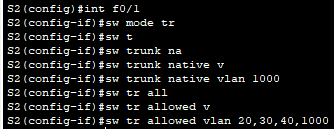
Выполните команду *show vlan brief*, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

****

Настройка VLAN

Часть 3. ·Настройте транки (магистральные каналы)

Настройка транков

****

Настройка магистральных каналов

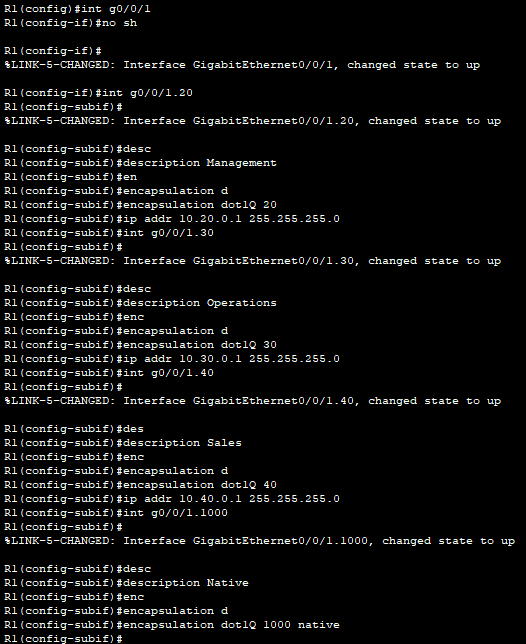
Часть 4. Настройте маршрутизацию

Активируем интерфейс g0/0/1 на R1

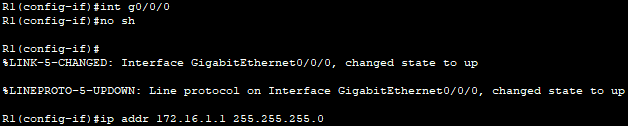


Включение интерфейса

Настроим интерфейсы согласно таблице адресации

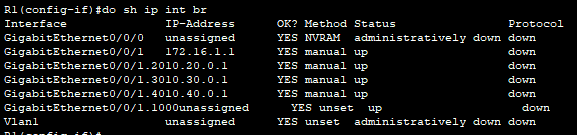


Настройка сабинтерфейсов



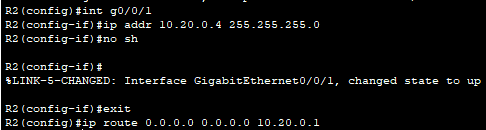
Настройка интерфейса

 С помощью команды *show ip interface brief* проверим конфигурацию интерфейсов



Интерфейсы R1

Настроим интерфейс g0/0/1 и создадим маршрут



Настройка интерфейса и маршрута

Часть 5. Настройте удаленный доступ

Создадим пользователя с зашифрованным паролем

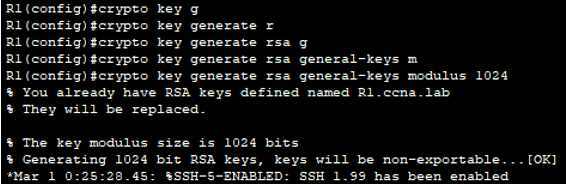


Создание пользователя

Используем в качестве доменного имя ccna-lab.com и зададим ключи шифрования

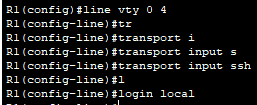


Задание доменного имени



Задание ключей шифрования

Настроим первые пять линий VTY на каждом устройстве

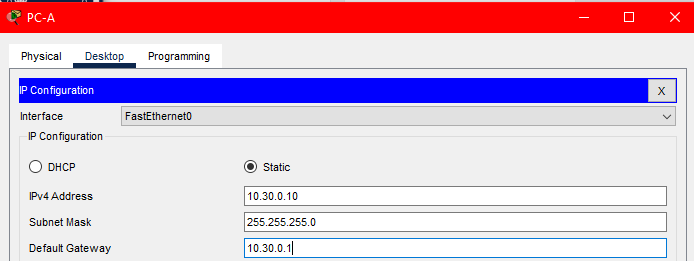


Настройка линий VTY

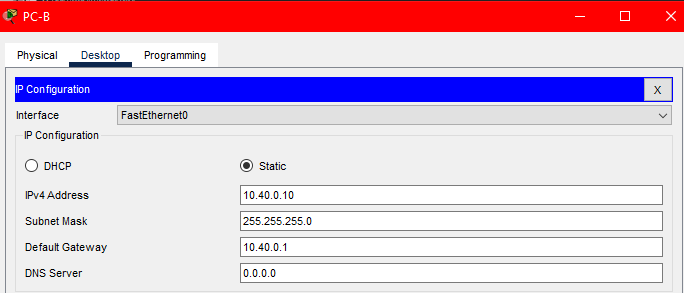
Вышеописанные действия произвели на R2, S1 и S2.

Часть 6. Проверка подключения

Настроим ПК согласно таблице маршрутизации



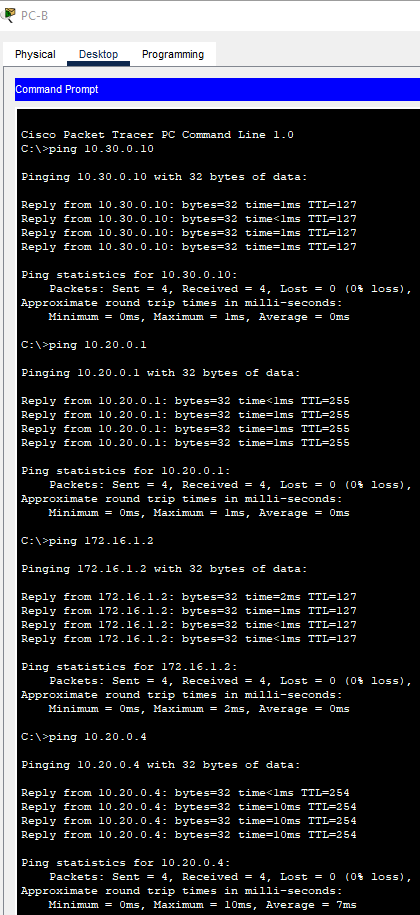
Настройка PC-A



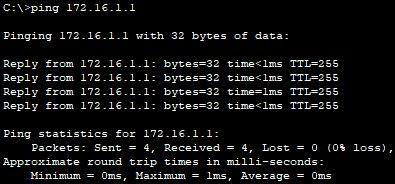
Настройка PC-B

Произведем тесты согласно таблице

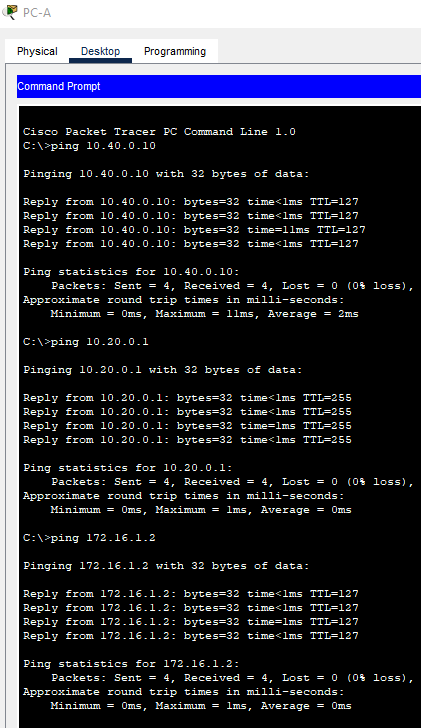
| **От** | **Протокол** | **Назначение** | **Результат** |
| --- | --- | --- | --- |
| PC-A | Ping | 10.40.0.10 | Успех |
| PC-A | Ping | 10.20.0.1 | Успех |
| PC-B | Ping | 10.30.0.10 | Успех |
| PC-B | Ping | 10.20.0.1 | Успех |
| PC-B | Ping | 172.16.1.1 | Успех |
| PC-B | HTTPS | 172.16.1.2 | Успех |
| PC-A | HTTPS | 172.16.1.2 | Успех |
| PC-B | SSH | 10.20.0.4 | Успех |
| PC-B | SSH | 172.16.1.1 | Успех |



Ping с PC-B



Ping с PC-B



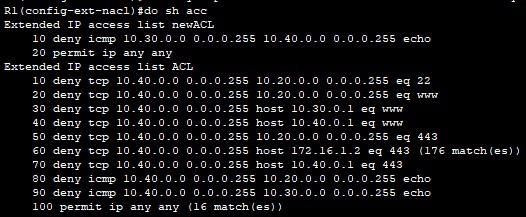
Ping с PC-A

Часть 7. Настройка и проверка списков расширенного контроля доступа

Реализуем следующие политики безопасности:

1. Сеть Sales не может использовать SSH в сети Management (но в другие сети SSH разрешен).
2. Сеть Sales не имеет доступа к server -A с помощью любого веб-протокола (HTTP/HTTPS). Весь остальной веб-трафик должен быть разрешен.
3. Сеть Sales не может отправлять эхо-запросы ICMP в сети Operations или Management. Разрешены эхо-запросы ICMP к другим адресатам.
4. Сеть Operations не может отправлять ICMP эхо-запросы в сеть Sales. Разрешены эхо-запросы ICMP к другим адресатам.

Создадим ACLs (рис. 94):



ACLs

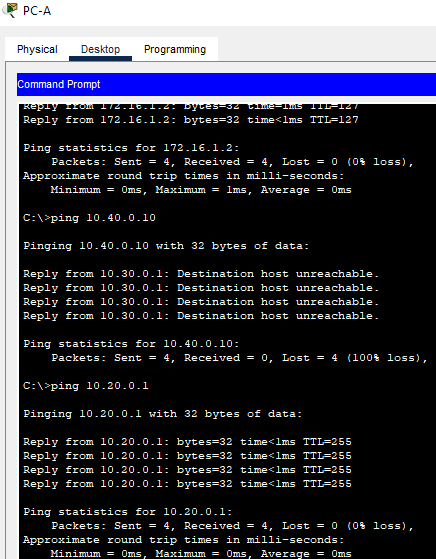
Проверим созданные списки контроля доступа на тестах, указанных в таблице ниже.

| **От** | **Протокол** | **Назначение** | **Результат** |
| --- | --- | --- | --- |
| PC-A | Ping | 10.40.0.10 | Сбой |
| PC-A | Ping | 10.20.0.1 | Успех |
| PC-B | Ping | 10.30.0.10 | Сбой |
| PC-B | Ping | 10.20.0.1 | Сбой |
| PC-B | Ping | 172.16.1.1 | Успех |
| PC-B | HTTPS | 172.16.1.2 | Сбой |
| PC-A | HTTPS | 172.16.1.2 | Успех |
| PC-B | SSH | 10.20.0.4 | Сбой |
| PC-B | SSH | 172.16.1.1 | Успех |

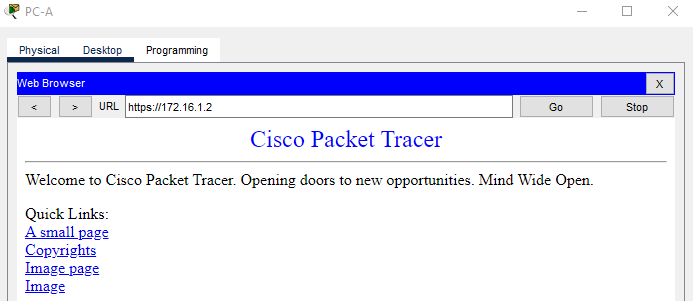
*Конец документа*

*Конец документа*

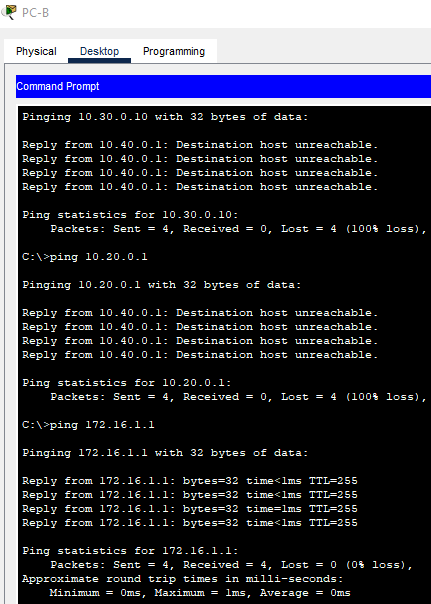
Проверка

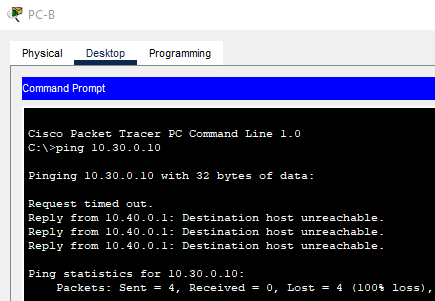
****

Проверка эхо-запросов для PC-A

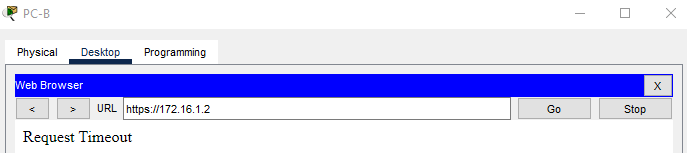
****

Проверка подключения к веб-серверу для PC-A

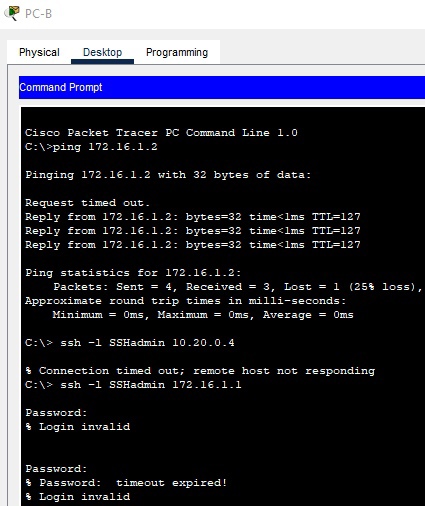
****



Проверка эхо-запросов для PC-B

****

Проверка подключения к веб-серверу для PC-B



Проверка SSH на PC-B.

На рисунке 100 видно, что все пункты выполнены правильно, что означает о корректной настройке ACL.