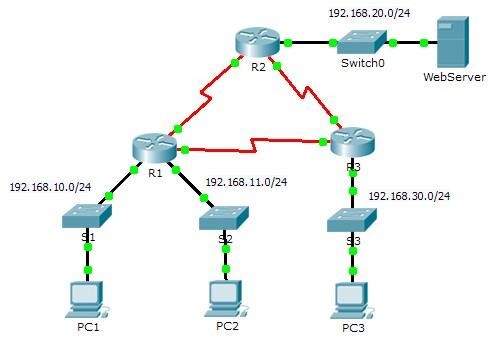
[Packet Tracer –](https://ccnav6.com/7-2-1-6-packet-tracer-configuring-numbered-standard-ipv4-acls-instructions-answers.html) Создание стандартных номерованных и именованных ACL

## Топология



. All rights reserved. This document is Cisco Public.

## Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | G0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
| G0/1 | 192.168.11.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| S0/0/1 | 10.3.3.1 | 255.255.255.252 | N/A |
| R2 | G0/0 | 192.168.20.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| R3 | G0/0 | 192.168.30.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.3.3.2 | 255.255.255.252 | N/A |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| PC1 | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |
| PC2 | NIC | 192.168.11.10 | 255.255.255.0 | 192.168.11.1 |
| PC3 | NIC | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 |
| WebServer | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |

**Цели:**

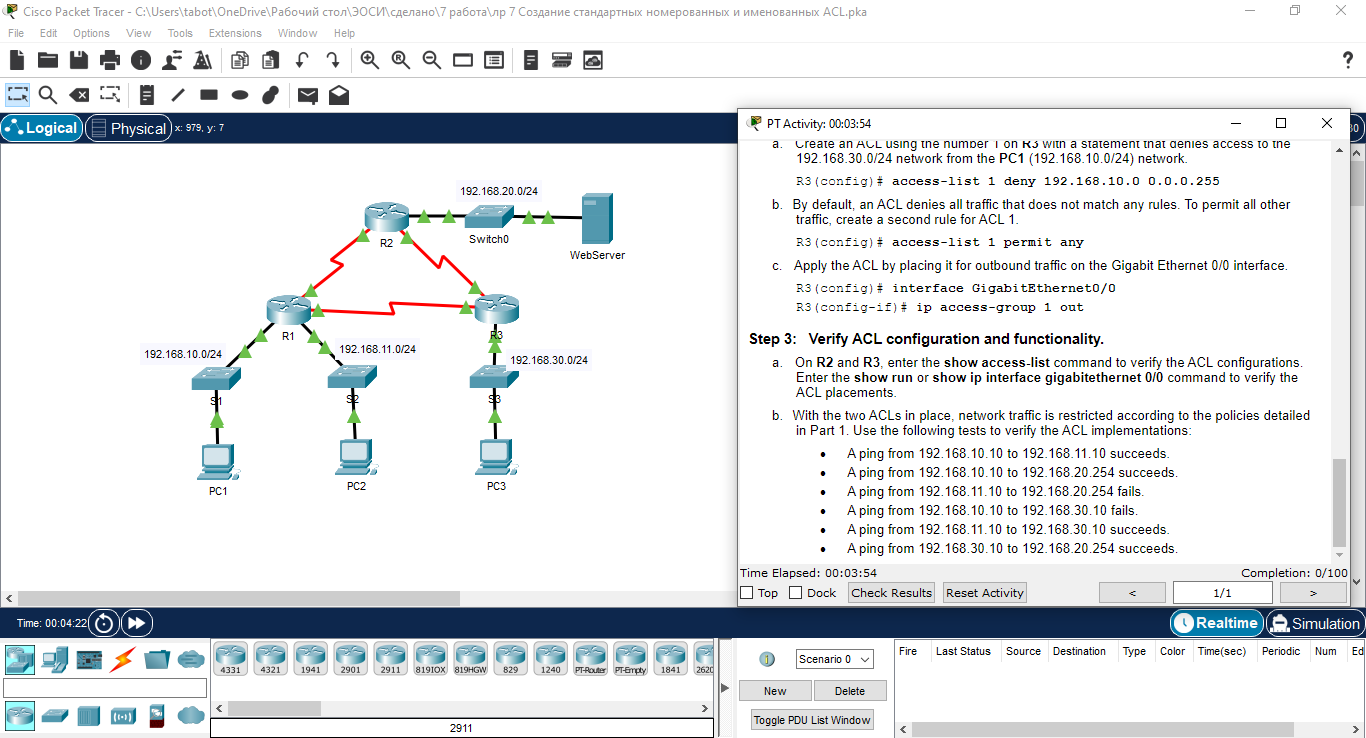
**1: Спланировать ACL**

**2: Создать, применить и проверить стандартные ACL**

# Часть 1: Планирование ACL

### 1: Ознакомится с текущей конфигурацией сети.

Перед применением ACL проверить работоспособность сети.



**2: Разработать две сетевых политики и спланировать реализацию ACL.**

1. Сетевые политики для применения на **R2**:
   * Запретить подсети 192.168.11.0/24 доступ к **WebServer** расположенном в подсети 192.168.20.0/24.
   * Остальное разрешить.

Почему для данной политики запись ACL необходимо разместить на **R2?**

Для какого интерфейса нужно будет применить политику? Для какого трафика (входящего, исходящего) и почему?

1. Сетевые политики для применения на **R3**:
   * Запретить доступ из подсети 192.168.10.0/24 к подсети 192.168.30.0/24.
   * Остальное разрешить.

Почему для данной политики запись ACL необходимо разместить на **R3?**

Для какого интерфейса нужно будет применить политику? Для какого трафика (входящего, исходящего) и почему?

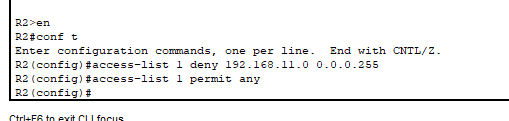
# Часть 2: Создание, применение и проверка стандартных ACL

### 1: Создать и применить ACL на R2.

1. Создать ACL с номером 1 на **R2.**

R2(config)# **access-list 1 deny 192.168.11.0 0.0.0.255**

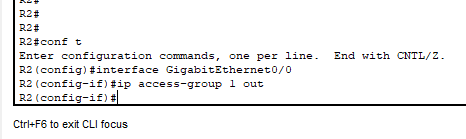
R2(config)# **access-list 1 permit any**

****

1. Применить ACL к интерфейсу.

R2(config)# **interface GigabitEthernet0/0**

R2(config-if)#**ip access-group 1 out**

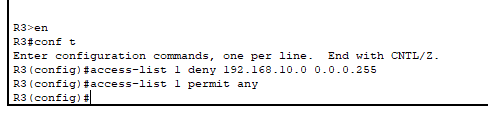
****

### 2: Создать и применить ACL на R3.

1. Создать ACL с номером 1 на.

R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**

R3(config)# **access-list 1 permit any**

****

1. Применить ACL к интерфейсу.

R3(config)# **interface GigabitEthernet0/0**

R3(config-if)#**ip access-group 1 out**

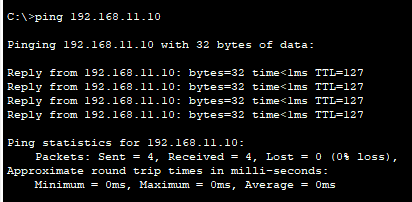
****

### 3: Проверка ACL.

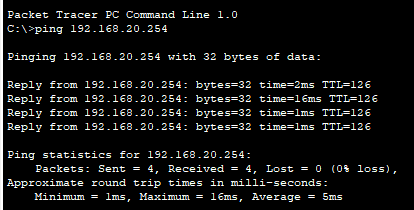
1. Посмотреть настройки на маршрутизаторах **R2** и **R3** с помощью команд **show access-list**,**show run**, **show ip interface gigabitethernet 0/0** (Скриншеты).

|  |  |
| --- | --- |
| R2 | R3 |
|  |  |
|  |  |
|  |  |

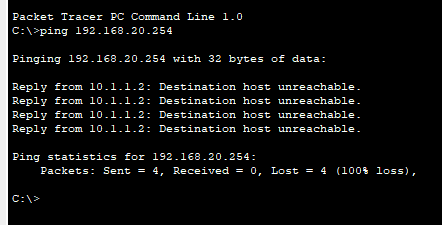
1. Проверить достижимость с помощью команды ping.
   * A ping from 192.168.10.10 to 192.168.11.10 succeeds.



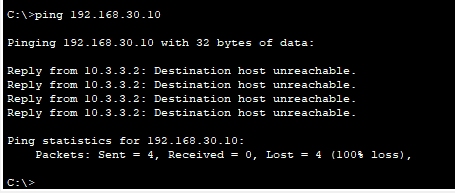
* + A ping from 192.168.10.10 to 192.168.20.254 succeeds.



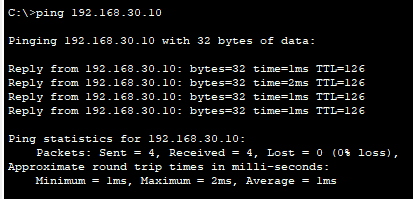
* + A ping from 192.168.11.10 to 192.168.20.254 fails.



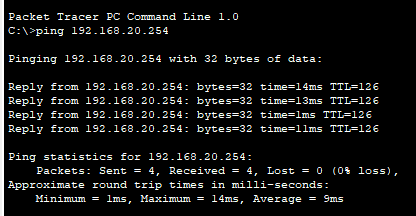
* + A ping from 192.168.10.10 to 192.168.30.10 fails.



* + A ping from 192.168.11.10 to 192.168.30.10 succeeds.



* + A ping from 192.168.30.10 to 192.168.20.254 succeeds.



# Часть 3: Создание, применение и проверка именованных стандартных ACL

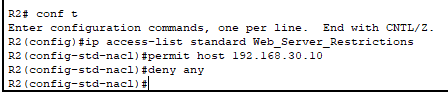
### 1: Создание именованного ACL.

Разрешить доступ к Web Server только с PC3. Создадим именованный ACL на **R2**.

R2(config)# **ip access-list standard Web\_Server\_Restrictions**

R2(config-std-nacl)# **permit host 192.168.30.10**

R2(config-std-nacl)# **deny any**

****

### 2: Применить именованную ACL.

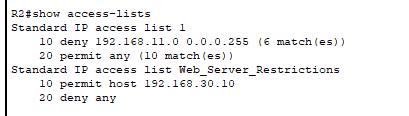
Применить ACL для исходящего трафика к интерфейсу GigabitEthernet0/0.

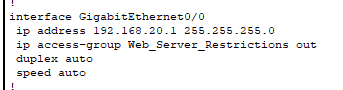
R2(config-if)# **ip access-group Web\_Server\_Restrictions out**

****

### 3: Проверить конфигурацию ACL.

Использовать команды **show access-lists**, **show run, show ip interface Gi0/0.**

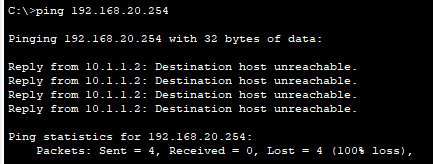
****

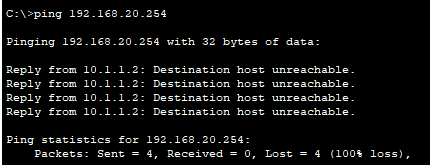
****

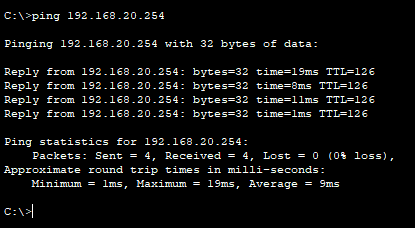
****

### 4: Проверить правильно ли работает ACL.

Доступ к **Web Server** должен быть только с **PC3**. Проверить с помощью ping.



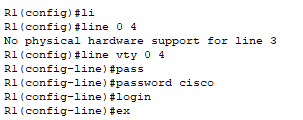




# Часть 4: Создание и применение ACL к VTY Lines

### 1: Настроить доступ к R1 по Telnet.

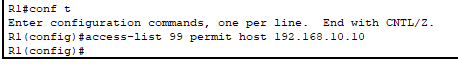
VTY - VirtualTeletYpe, виртуальный интерфейс, который обеспечивает удаленный доступ к устройству. Компьютер **PC1** должны иметь доступ к маршрутизатору по Telnet. Пароль cisco.



Проверить перед созданием ACL.

### 2: Создать номерованный стандартный ACL на R1.

Router(config)# **access-list 99 permit host 192.168.10.10**

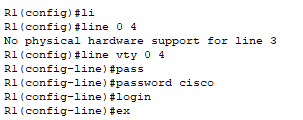
****

### 3: Применение ACL.

Доступ к интерфейсам маршрутизатора должен быть разрешен, а доступ к Telnet должен быть ограничен. Поэтому мы должны поместить ACL на линии Telnet с 0 по 4.

R1(config)# **line vty 0 15**

R1(config-line)# **access-class 99 in**

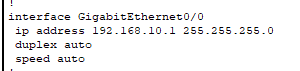
****

****

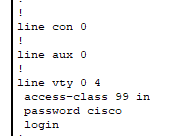
### 4: Проверьте конфигурацию ACL на VTY-line.

Использовать команды **show access-lists, show run**.



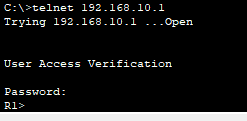


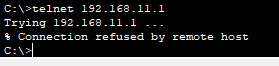




### 5: Убедитесь, что ACL работает правильно.

Все компьютеры должны иметь возможность пинговать маршрутизатор, но только **PC1** должен иметь возможность использовать Telnet.





# Вывод: