Лабораторная работа № 7 (вторая часть)

Тема: Настройка списков контроля доступа ACL для ограничения сетевого трафика в Cisco Packet Tracer

Цель работы: изучить принципы фильтрации сетевого трафика с помощью списков контроля доступа ACL (Access Control List), освоить создание стандартных и расширенных ACL, научиться разрешать и запрещать обмен данными между локальными сетями и проверять действие правил фильтрации.

1. Теоретические сведения

ACL (Access Control List) представляет собой список правил, с помощью которых маршрутизатор контролирует передачу сетевых пакетов.

С помощью ACL можно:

- запретить доступ одной локальной сети к другой;
- разрешить доступ к определённому серверу;
- ограничить обмен данными между компьютерами;
- разрешить или запретить определённые протоколы;
- повысить безопасность локальной сети.

В Cisco Packet Tracer используются два основных типа ACL.

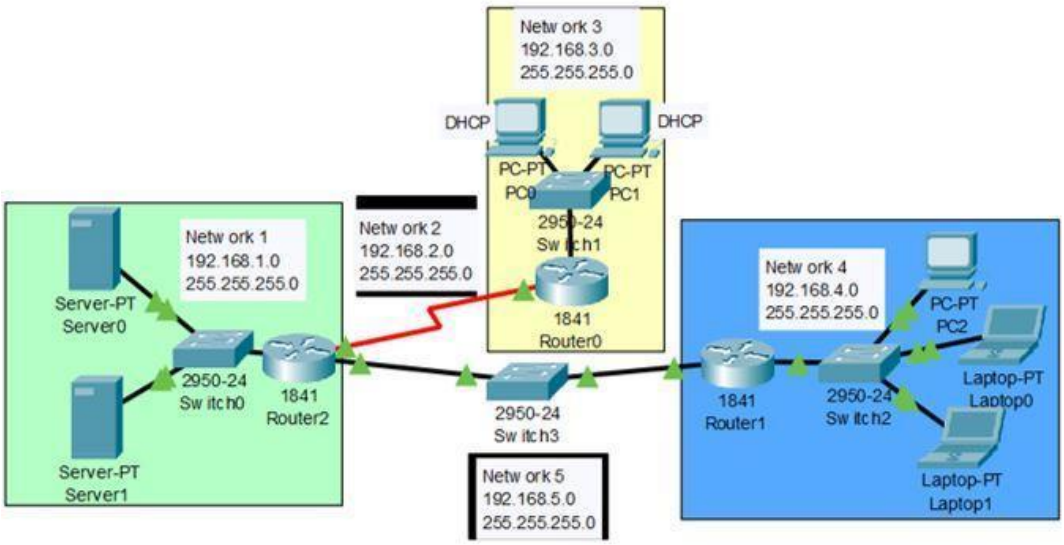
Тип ACL	Назначение
Standard ACL	Фильтрация по IP-адресу источника
Extended ACL	Фильтрация по адресу источника, адресу назначения и протоколу

Важно: стандартный ACL проверяет только IP-адрес отправителя. Если необходимо запретить одной подсети доступ к другой, но разрешить доступ к конкретному серверу, удобнее использовать расширенный ACL.

В этой работе мы сначала изучим стандартный ACL, а затем применим расширенный ACL для более точной фильтрации.

2. Построение сети

Создадим корпоративную сеть из одного маршрутизатора, одного коммутатора, трёх локальных подсетей и одного сервера.



Структура сети:

- LAN 1: сеть административного отдела.
- LAN 2: сеть учебного отдела.
- LAN 3: серверная сеть.
- R1: маршрутизатор, который обеспечивает связь между тремя подсетями.
- Server: сервер, доступ к которому необходимо сохранить.

3. Таблица IP-адресации

Для выполнения работы используйте следующую адресацию.

Устройство	Интерфейс	IP-адрес
R1	G0/0	192.168.10.1/24
R1	G0/1	192.168.20.1/24
R1	G0/2	192.168.30.1/24
PC1	FastEthernet0	192.168.10.10/24
PC2	FastEthernet0	192.168.10.11/24
PC3	FastEthernet0	192.168.20.10/24
PC4	FastEthernet0	192.168.20.11/24
Server	FastEthernet0	192.168.30.10/24

Маска для всех устройств: `255.255.255.0`.

Шлюзы по умолчанию:

- PC1 и PC2: `192.168.10.1`
- PC3 и PC4: `192.168.20.1`
- Server: `192.168.30.1`

4. Практическая часть

Задание 1. Создание топологии

1. Запустить Cisco Packet Tracer.
2. Разместить маршрутизатор Cisco 2911.
3. Разместить три коммутатора Cisco 2960.
4. Добавить четыре компьютера.
5. Добавить один сервер.
6. Подключить каждый коммутатор к отдельному интерфейсу маршрутизатора.
7. Подключить компьютеры к соответствующим коммутаторам.
8. Подключить сервер к третьему коммутатору.

Задание 2. Настройка маршрутизатора

Открыть CLI маршрутизатора R1 и выполнить следующие команды:

```
enable
configure terminal
hostname R1

interface gigabitEthernet 0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
exit

interface gigabitEthernet 0/1
ip address 192.168.20.1 255.255.255.0
no shutdown
exit

interface gigabitEthernet 0/2
ip address 192.168.30.1 255.255.255.0
no shutdown
exit

end
```

Проверить состояние интерфейсов:

```
show ip interface brief
```

Все три интерфейса должны иметь состояние `up/up`.

Задание 3. Настройка компьютеров и сервера

Для каждого компьютера выполнить следующие действия:

1. Открыть вкладку Desktop.
2. Выбрать IP Configuration.
3. Ввести IP-адрес.
4. Указать маску подсети.
5. Указать шлюз по умолчанию.

На сервере выполнить аналогичные действия.

Для проверки связи между подсетями с PC1 выполнить:

```
ping 192.168.20.10
ping 192.168.30.10
```

Ожидаемый результат

До настройки ACL все компьютеры должны обмениваться данными между подсетями, а сервер должен отвечать на запросы.

5. Настройка стандартного ACL

Задание 4. Создание стандартного ACL

Поставим следующую задачу:

- подсети административного отдела `192.168.10.0/24` запрещено обращаться к учебному отделу `192.168.20.0/24`;
- остальным подсетям разрешён доступ к учебному отделу;
- доступ административного отдела к серверу `192.168.30.10` должен сохраниться.

Для этого создадим стандартный ACL с номером 10.

На маршрутизаторе R1 выполнить:

```
enable
configure terminal

access-list 10 deny 192.168.10.0 0.0.0.255
access-list 10 permit any
```

Пояснение команд:

Команда	Назначение
`access-list 10`	Создание стандартного ACL № 10
`deny`	Запрет передачи пакетов
`192.168.10.0`	Адрес исходной подсети
`0.0.0.255`	Wildcard mask для подсети /24
`permit any`	Разрешение остального трафика

Обратите внимание: если не добавить `permit any`, все остальные адреса будут запрещены по умолчанию.

Задание 5. Применение ACL к интерфейсу

Теперь необходимо применить созданный список к интерфейсу G0/1, который подключён к учебному отделу.

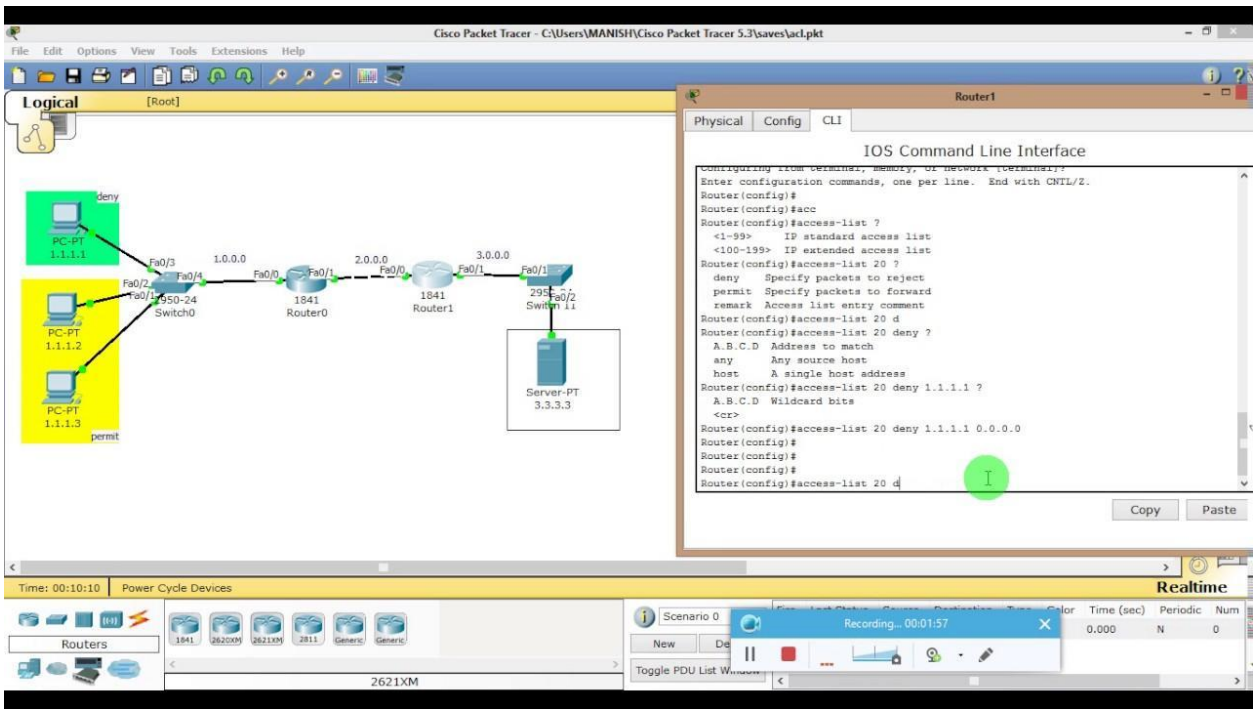
```
interface gigabitEthernet 0/1
ip access-group 10 out
exit
end
```

Почему используется `out`?

Потому что мы хотим проверить пакеты, которые выходят из маршрутизатора в сеть `192.168.20.0/24`.

Таким образом:

- пакеты от PC1 и PC2 в учебную сеть будут запрещены;
- пакеты из других подсетей в учебную сеть будут разрешены;
- трафик к серверу через G0/2 не будет заблокирован этим ACL.



6. Проверка работы ACL

Задание 6. Проверка запрещённого доступа

На компьютере PC1 открыть Command Prompt и выполнить:

```
ping 192.168.20.10
```

Ожидаемый результат: доступ запрещён

Запросы от PC1 к PC3 не должны проходить.

Причина: исходный адрес принадлежит подсети `192.168.10.0/24`, для которой настроен запрет.

Задание 7. Проверка разрешённого доступа

С компьютера PC3 выполнить:

```
ping 192.168.10.10
```

Затем с PC1 выполнить:

```
ping 192.168.30.10
```

Ожидаемый результат: доступ разрешён

PC3 может обращаться к PC1, поскольку фильтрация настроена только на выход интерфейса G0/1.

PC1 может обращаться к серверу, поскольку его трафик выходит через G0/2, где ACL не применён.

Задание 8. Просмотр списка ACL

На маршрутизаторе выполнить:

```
show access-lists
```

Команда покажет созданные правила и количество совпадений с ними.

Также выполнить:

```
show ip interface gigabitEthernet 0/1
```

С помощью этой команды можно проверить, какой ACL назначен интерфейсу и в каком направлении он действует.

7. Дополнительное задание: расширенный ACL

Теперь необходимо изменить условия фильтрации.

Новая задача:

1. Запретить PC1 доступ к PC3.
2. Разрешить PC1 доступ к серверу.
3. Запретить PC2 доступ к серверу.
4. Разрешить остальным компьютерам обмен данными.

Для выполнения задания используйте расширенный ACL № 101.

Сначала удалите применение старого списка:

```
configure terminal
interface gigabitEthernet 0/1
no ip access-group 10 out
exit
no access-list 10
```

Создайте расширенный ACL:

```
access-list 101 deny ip host 192.168.10.10 host 192.168.20.10
access-list 101 permit ip host 192.168.10.10 host 192.168.30.10
access-list 101 deny ip host 192.168.10.11 host 192.168.30.10
access-list 101 permit ip any any
```

Примените его на интерфейсе G0/0 во входящем направлении:

```
interface gigabitEthernet 0/0
ip access-group 101 in
exit
end
```

Объяснение расширенного ACL:

Правило	Действие
PC1 → PC3	Запрет
PC1 → Server	Разрешение
PC2 → Server	Запрет
Остальной IP-трафик	Разрешение

Здесь используется `host`, поскольку фильтрация выполняется для конкретных компьютеров, а не для целых подсетей.

8. Проверка расширенного ACL

Выполнить следующие команды на компьютерах.

На PC1:

```
ping 192.168.20.10
ping 192.168.30.10
```

На PC2:

```
ping 192.168.30.10
```

На PC3:

```
ping 192.168.10.11
```

Ожидаемые результаты:

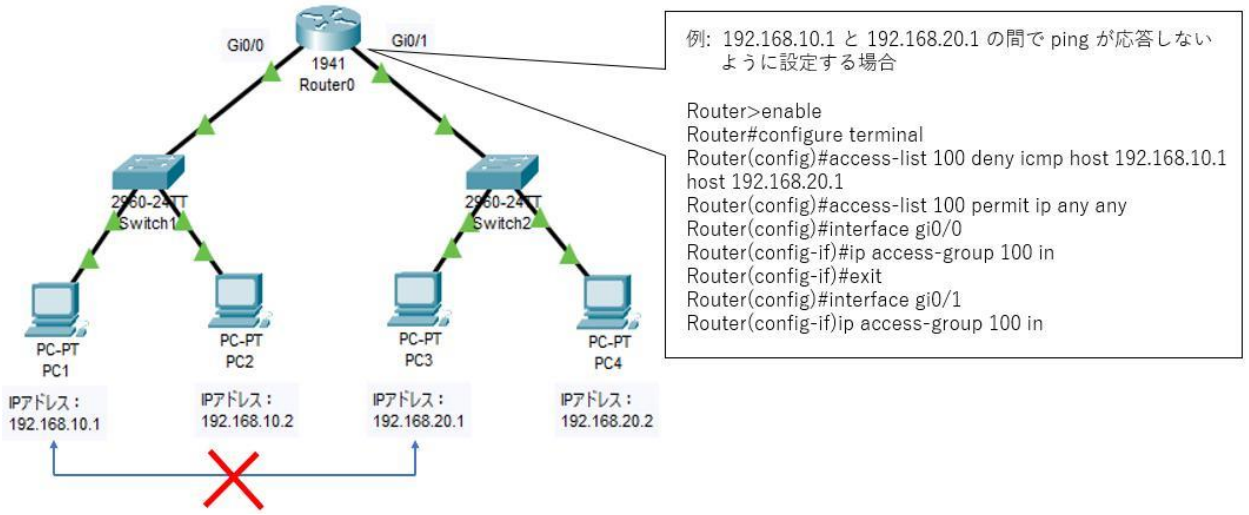
Проверка	Результат
PC1 → PC3	Запрещено
PC1 → Server	Разрешено
PC2 → Server	Запрещено
PC3 → PC2	Разрешено

Для проверки счётчиков ACL выполнить:

```
show access-lists
```

Важно: в стандартном ACL фильтрация выполняется только по адресу источника. Поэтому в первой части лабораторной работы запрет для подсети PC1 и PC2 затрагивает также ответные пакеты от этих компьютеров к учебной сети. Из-за этого двусторонний обмен между PC1 и PC3 не работает. Это одно из ограничений стандартного ACL. Расширенный ACL позволяет точнее задавать условия фильтрации.

9. Проверка в режиме Simulation



1. Перейти в режим Simulation.
2. Выбрать фильтр ICMP.
3. Отправить пакет от PC1 к PC3.
4. Нажать Capture/Forward.
5. Проследить прохождение пакета через маршрутизатор.
6. Изучить результат обработки ACL.
7. Повторить проверку при передаче пакета от PC1 к серверу.

Студент должен определить, на каком устройстве пакет был отклонён и какое правило ACL было применено.

10. Контрольные вопросы

1. Что такое ACL?
2. Для чего используются списки контроля доступа?
3. Чем стандартный ACL отличается от расширенного ACL?
4. Что означают команды `permit` и `deny`?
5. Для чего используется Wildcard Mask?
6. Что означает команда `access-group`?
7. Чем отличаются направления `in` и `out`?
8. Почему в конце ACL действует неявный запрет?
9. Почему расширенный ACL позволяет точнее фильтровать трафик?
10. В каких случаях ACL используется для защиты корпоративной сети?

11. Содержание отчёта

В отчёте по лабораторной работе студент должен представить:

1. Титульный лист.
2. Название и цель работы.
3. Схему созданной сети.
4. Таблицу IP-адресации.
5. Команды настройки маршрутизатора.
6. Команды создания стандартного ACL.
7. Команды создания расширенного ACL.

8. Результаты проверки связи между компьютерами.
9. Скриншоты команды `show access-lists`.
10. Результаты работы в режиме Simulation.
11. Вывод по лабораторной работе.

12. Итоговое задание для самостоятельной работы

Изменить условия фильтрации:

- PC1 не должен иметь доступ к PC3 и PC4.
- PC2 должен иметь доступ к PC3, но не должен иметь доступ к серверу.
- PC3 и PC4 должны иметь доступ к серверу.
- Все остальные соединения должны быть разрешены.

Создать соответствующий расширенный ACL и проверить его работу.