Лабораторная работа. Настройка и проверка расширенных ACL-списков

Топология

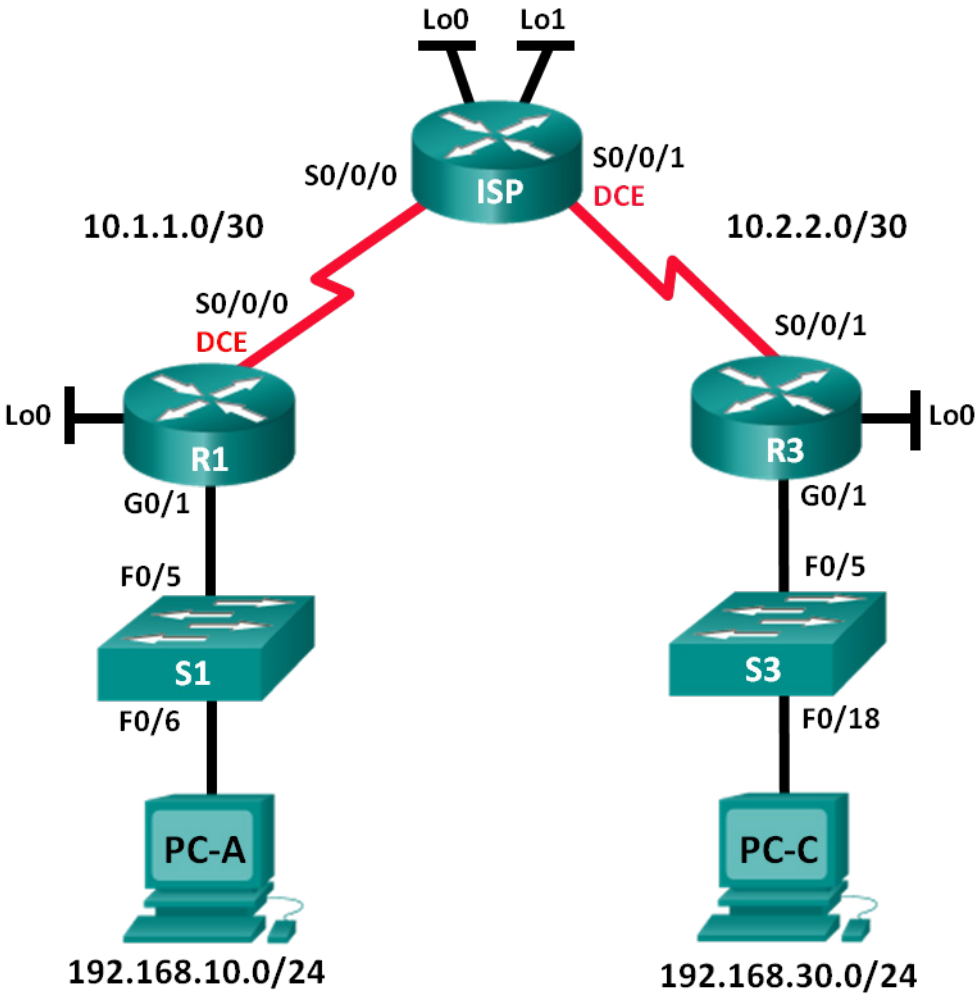

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

Часть 2. Конфигурация устройств и проверка подключения

- Настройте базовые параметры на компьютерах, маршрутизаторах и коммутаторах.
- Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

Часть 3. Настройка и проверка расширенных нумерованных и именованных ACL-списков

- Настройте, примените и проверьте нумерованные расширенные ACL-списки.
- Настройте, примените и проверьте именованные расширенные ACL-списки.

Часть 4. Изменение и проверка расширенных ACL-списков

Исходные данные/сценарий

Расширенные списки контроля доступа (ACL) демонстрируют высокую эффективность. Они предлагают более высокий уровень управления, чем стандартные ACL-списки, как по отношению к типам фильтруемого трафика, так и к тому, где трафик создан и куда он направлен.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, не настроены ACL-списки. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры на маршрутизаторе R1.

a. Отключите поиск DNS.

b. Настройте имя устройства в соответствии с топологией.

c. Создайте loopback-интерфейс на маршрутизаторе R1.

d. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

e. Установите пароль **class** для доступа к привилегированному режиму EXEC.

f. Установите тактовую частоту для интерфейса S0/0/0 на значение **128000**.

g. Назначьте **cisco** в качестве пароля для VTY и активируйте доступ к Telnet. Настройте **logging synchronous** для консоли и каналов vty.

h. Активируйте сетевой доступ на маршрутизаторе R1, чтобы смоделировать веб-сервер с локальной аутентификацией для пользователя **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Шаг 3: Настройте базовые параметры на ISP.

a. Настройте имя устройства в соответствии с топологией.

b. Создайте loopback-интерфейсы на ISP.

c. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

d. Отключите поиск DNS.

e. Назначьте **class** в качестве пароля привилегированного режима EXEC.

f. Установите тактовую частоту на значение **128000** для интерфейса S0/0/1.

g. Назначьте **cisco** в качестве пароля для VTY и активируйте доступ к Telnet. Настройте **logging synchronous** для консоли и каналов vty.

h. Активируйте веб-доступ на ISP. Используйте те же параметры, что и на шаге 2h.

Шаг 4: Настройте базовые параметры на маршрутизаторе R3.

a. Настройте имя устройства в соответствии с топологией.

b. Создайте loopback-интерфейс на маршрутизаторе R3.

c. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

d. Отключите поиск DNS.

e. Назначьте **class** в качестве пароля привилегированного режима EXEC.

f. Назначьте **cisco** в качестве пароля консоли и настройте **logging synchronous** на канале консоли.

g. Включите SSH на S3.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

h. Активируйте веб-доступ на R3. Используйте те же параметры, что и на шаге 2h.

Шаг 5: Настройте базовые параметры на коммутаторах S1 и S3 (дополнительно).

a. Настройте имена узлов в соответствии с топологией.

b. Настройте IP-адреса административного интерфейса в соответствии с топологией и таблицей адресации.

c. Отключите поиск DNS.

d. Установите пароль **class** для доступа к привилегированному режиму EXEC.

e. Настройте адрес основного шлюза.

Шаг 6: Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISP и R3. Отключите автоматическое суммирование маршрутов.

b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 7: Проверьте наличие подключения между всеми устройствами.

Примечание. Наличие соединения важно проверять **перед** настройкой и применением списков контроля доступа! Прежде чем приступить к фильтрации трафика, проверьте работоспособность сети.

a. От узла PC-A отправьте эхо-запросы на PC-C, loopback-интерфейс и последовательные интерфейсы на маршрутизаторе R3.

Успешно ли выполнены эхо-запросы?

b. От маршрутизатора R1 отправьте эхо-запросы на PC-C, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R3.

Успешно ли выполнены эхо-запросы?

c. От узла PC-C отправьте эхо-запросы на PC-A, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R1.

Успешно ли выполнены эхо-запросы?

d. От маршрутизатора R3 отправьте эхо-запросы на PC-A, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R1.

Успешно ли выполнены эхо-запросы?

e. От узла PC-A отправьте эхо-запросы на loopback-интерфейсы на маршрутизаторе ISP.

Успешно ли выполнены эхо-запросы?

f. От узла PC-C отправьте эхо-запросы на loopback-интерфейсы на маршрутизаторе ISP.

Успешно ли выполнены эхо-запросы?

g. Откройте веб-браузер на узле PC-A и перейдите по адресу http://209.165.200.225 интернет-провайдера. Появится окно с запросом имени пользователя и пароля. Используйте **admin** как имя пользователя и **class** как пароль. Если появится запрос принять подпись, подтвердите приём подписи. В отдельном окне маршрутизатор загрузит приложение Cisco Configuration Professional (CCP) Express. Появится окно с запросом имени пользователя и пароля. Используйте **admin** как имя пользователя и **class** как пароль.

h. Откройте веб-браузер на узле PC-C и перейдите по адресу http://10.1.1.1 на маршрутизаторе R1. Появится окно с запросом имени пользователя и пароля. Используйте **admin** как имя пользователя и **class** как пароль. Если появится запрос принять подпись, подтвердите приём подписи. В отдельном окне маршрутизатор загрузит приложение CCP Express. Появится окно с запросом имени пользователя и пароля. Используйте **admin** как имя пользователя и **class** как пароль.

Часть 3: Настройка и проверка расширенных нумерованных и расширенных именованных ACL-списков

Расширенные ACL-списки позволяют фильтровать трафик различными способами. Расширенные ACL-списки позволяют фильтровать трафик на основе IP-адреса отправителя, порта отправителя, IP-адреса назначения, порта назначения, а также на основе различных протоколов и служб.

Данные списки контроля доступа работают в соответствии со следующими правилами безопасности:

1. Разрешать доступ веб-трафика из сети 192.168.10.0/24 в любую сеть.
2. Разрешать подключение SSH к последовательному интерфейсу R3 от узла PC-A.
3. Разрешать пользователям в сети 192.168.10.0.24 сетевой доступ к сети 192.168.20.0/24.
4. Разрешать доступ веб-трафика из сети 192.168.30.0/24 к маршрутизатору R1 через веб-интерфейс и сеть интернет-провайдера 209.165.200.224/27. Доступ сети 192.168.30.0/24 к какой-либо другой сети должен быть ЗАПРЕЩЁН.

Для выполнения этих правил безопасности вам потребуется как минимум два ACL-списка. Рекомендуется разместить ACL-списки как можно ближе к источнику. Мы последуем этой рекомендации для соблюдения вышеупомянутых правил безопасности.

Шаг 1: Для расширенных нумерованных ACL-списков на маршрутизаторе R1 настройте номера 1 и 2.

На маршрутизаторе R1 вы будете использовать нумерованный расширенный список. Укажите диапазоны для расширенных ACL-списков.

a. Настройте ACL-список на маршрутизаторе R1. В качестве номера списка доступа используйте 100.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

Что означает 80 в вышеуказанных выходных данных?

На каких интерфейсах должен быть применён ACL-список под номером 100?

На каком направлении следует применить ACL-список 100?

b. Примените ACL-список 100 на интерфейсе S0/0/0.

```
R1(config)# int s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Проверьте работу ACL-списка 100.

1) Откройте веб-браузер на узле PC-A и проверьте доступ к http://209.165.200.225 (маршрутизатор ISP). Всё должно работать; в обратном случае выявите и устраните неполадки.

2) Установите SSH-подключение от узла PC-A к маршрутизатору R3, используя 10.2.2.1 в качестве IP-адреса. Войдите в систему, используя учётные данные **admin** и **class**. Всё должно работать; в обратном случае выявите и устраните неполадки.

3) Из командной строки привилегированного режима на маршрутизаторе R1 выполните команду **show access-lists**.

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
```

```
    20 permit tcp any any eq www (111 matches)
```

4) Из командной строки узла PC-A выполните эхо-запрос на адрес 10.2.2.1. Поясните полученные результаты.

Шаг 2: Настройте именованный расширенный ACL-список на маршрутизаторе R3 для соблюдения правила безопасности под номером 3.

a. Настройте политику безопасности на маршрутизаторе R3. Имя ACL-списка: WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Примените ACL-список WEB-POLICY на интерфейсе S0/0/1.

```
R3(config-ext-nacl)# int S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. Проверьте работу ACL-списка WEB-POLICY.

1) Из командной строки привилегированного режима маршрутизатора R3 выполните команду **show ip interface s0/0/1**.

Укажите имя ACL-списка (если имеется).

На каком направлении применён ACL-список?

2) Откройте веб-браузер на узле PC-C и получите доступ к http://209.165.200.225 (маршрутизатор ISP). Всё должно работать; в обратном случае выявите и устраните неполадки.

3) На узле PC-C откройте веб-сеанс на адрес http://10.1.1.1 (R1). Всё должно работать; в обратном случае выявите и устраните неполадки.

4) На узле PC-C откройте веб-сеанс на адрес http://209.165.201.1 (маршрутизатор ISP). Эхо-запрос не должен пройти; в противном случае выявите и устраните неполадки.

5) Из командной строки узла PC-C отправьте эхо-запрос на узел PC-A. Какой получен результат? Почему?

Часть 4: Изменение и проверка расширенных ACL-списков

Вследствие применения ACL-списков на маршрутизаторах R1 и R3, ни эхо-запросы, ни какие-либо другие виды трафика не могут проходить между локальными сетями на маршрутизаторах R1 и R3. Руководство решило разрешить весь трафик между сетями 192.168.10.0/24 и 192.168.30.0/24. Необходимо внести изменения в ACL-списки на маршрутизаторах R1 и R3.

Шаг 1: Измените ACL-список 100 на маршрутизаторе R1.

a. В привилегированном режиме маршрутизатора R1 выполните команду **show access-lists**.

Сколько строк имеется в списке контроля доступа?

b. Войдите в режим глобальной конфигурации и измените ACL-список на маршрутизаторе R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

c. Выполните команду **show access-lists**.

Где именно в ACL-списке 100 появился только что добавленный канал?

Шаг 2: Измените ACL-список WEB-POLICY на маршрутизаторе R3.

a. В привилегированном режиме маршрутизатора R3 выполните команду **show access-lists**.

Сколько строк имеется в списке контроля доступа?

b. Войдите в режим глобальной конфигурации и измените ACL-список на маршрутизаторе R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. Выполните команду **show access-lists**, чтобы убедиться, что в конце ACL-списка была добавлена новая строка.

Шаг 3: Проверьте работу изменённых ACL-списков.

a. От узла PC-A отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос?

b. От узла PC-C отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос?

Почему изменения ACL-списков незамедлительно подействовали на эхо-запросы?

Вопросы на закрепление

1. Почему необходимо тщательно планировать и проверять работу ACL-списков?

2. Какой тип ACL-списка лучше — стандартный или расширенный?

3. Почему скрытый запрет **deny any** или аналогичная явная запись ACL-списков, применённых на маршрутизаторах R1 и R3, не блокирует пакеты приветствия (hello) EIGRP и обновления маршрутизации?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.