

Packet Tracer. Настройка расширенных ACL-списков.

Сценарий 1

Топология

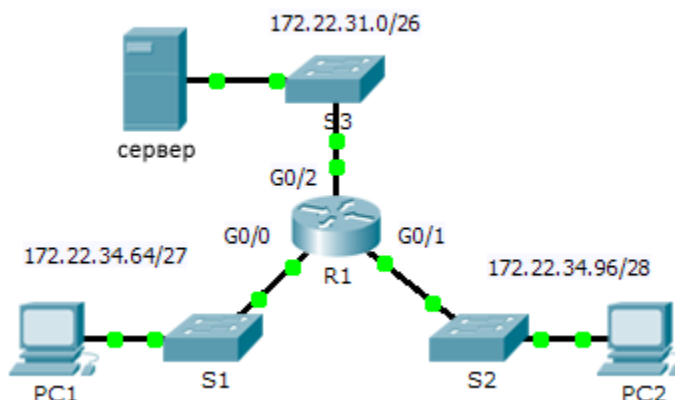


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	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 ACL-списка

Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка

Исходные данные/сценарий

Двум работникам предприятия требуется доступ к службам, предоставляемым сервером. Узлу **PC1** требуется доступ только к FTP, в то время как **PC2** нужен доступ только к веб-сети. Оба компьютера могут отправлять эхо-запросы серверу, но не друг другу.

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

Шаг 1: Настройте ACL-список на разрешение FTP и ICMP.

- a. В режиме глобальной конфигурации на маршрутизаторе **R1** введите следующую команду, чтобы определить первый допустимый номер для расширенного списка доступа.

```
R1(config)# access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
```

- b. Добавьте **100** к команде, а затем поставьте вопросительный знак.

```
R1(config)# access-list 100 ?
deny        Specify packets to reject
permit      Specify packets to forward
remark      Access list entry comment
```

- c. Чтобы разрешить трафик FTP, введите **permit**, после которого поставьте вопросительный знак.

```
R1(config)# access-list 100 permit ?
ahp         Authentication Header Protocol
eigrp       Cisco's EIGRP routing protocol
esp         Encapsulation Security Payload
gre         Cisco's GRE tunneling
icmp        Internet Control Message Protocol
ip          Any Internet Protocol
ospf        OSPF routing protocol
tcp         Transmission Control Protocol
udp         User Datagram Protocol
```

- d. Данный ACL-список разрешает FTP и ICMP. ICMP включён в список, указанный выше, в отличие от FTP, который использует протокол TCP. Таким образом, необходимо ввести TCP. Введите **tcp**, чтобы обновить ACL-список.

```
R1(config)# access-list 100 permit tcp ?
A.B.C.D     Source address
any         Any source host
host        A single source host
```

- e. Обратите внимание, что мы могли бы настроить фильтрацию только для **PC1**, используя ключевое слово **host**, а также могли бы разрешить доступ для **любого** узла. В этом случае доступ разрешён любому устройству с адресом, принадлежащим сети 172.22.34.64/27. Введите сетевой адрес со знаком вопроса в конце.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
A.B.C.D     Source wildcard bits
```

- f. Рассчитайте шаблонную маску, определяющую двоичную противоположность маски подсети.

```
11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31
```

- g. Введите шаблонную маску со знаком вопроса в конце.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
```

```
A.B.C.D  Destination address
any      Any destination host
eq       Match only packets on a given port number
gt       Match only packets with a greater port number
host     A single destination host
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
range    Match only packets in the range of port numbers
```

- h. Настройте адрес узла-назначения. В этом сценарии мы фильтруем трафик в пользу только одного адресата — сервера. Введите ключевое слово **host**, за которым следует IP-адрес сервера.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
```

```
dscp      Match packets with given dscp value
eq        Match only packets on a given port number
established established
gt        Match only packets with a greater port number
lt        Match only packets with a lower port number
neq       Match only packets not on a given port number
precedence Match packets with given precedence value
range     Match only packets in the range of port numbers
<cr>
```

- i. Обратите внимание на параметр **<cr>** (возврат каретки). Другими словами, вы можете нажать клавишу **ВВОД**, и согласно правилу будет разрешён весь трафик TCP. Однако мы хотим разрешить только трафик FTP. Поэтому введите ключевое слово **eq**, после которого поставьте вопросительный знак, чтобы отобразить доступные параметры. Затем введите **ftp** и нажмите **ВВОД**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
```

```
<0-65535> Port number
ftp       File Transfer Protocol (21)
pop3      Post Office Protocol v3 (110)
smtp      Simple Mail Transport Protocol (25)
telnet    Telnet (23)
www       World Wide Web (HTTP, 80)
```

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

- j. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от **PC1** на **сервер**. Обратите внимание на то, что номер списка доступа остается неизменным, конкретный тип трафика ICMP не требует определения.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

- k. Остальной трафик запрещён по умолчанию.

Шаг 2: Примените ACL-список на соответствующем интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора **R1**, трафик, к которому применяется список ACL 100, является входящим из сети, подключённой к интерфейсу Gigabit Ethernet 0/0. Войдите в режим настройки интерфейса и примените ACL-список.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Шаг 3: Проверьте работу ACL-списка.

- Отправьте эхо-запрос от узла **PC1** на **сервер**. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.
- Отправьте FTP-трафик от узла **PC1** на **сервер**. Имя пользователя и пароль — **cisco**.
PC> **ftp 172.22.34.62**
- Выйдите из службы FTP на **сервере**.
ftp> **quit**
- Отправьте эхо-запрос от узла **PC1** на **PC2**. Узел назначения должен быть недоступен, поскольку отсутствует разрешение на трафик в явном виде.

Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка

Шаг 1: Настройте ACL-список на разрешение HTTP-доступа и ICMP.

- Именованные ACL-списки начинаются с ключевого слова **ip**. В режиме глобальной конфигурации маршрутизатора **R1** введите следующую команду, после которой поставьте вопросительный знак.

```
R1(config)# ip access-list ?
extended   Extended Access List
standard   Standard Access List
```

- Можно настроить именованные стандартные и расширенные ACL-списки. Посредством этого списка доступа фильтруются как IP-адреса источника, так и IP-адреса узла-назначения; таким образом, список должен быть расширенным. Введите **HTTP_ONLY** в качестве имени. (для оценки работы в Packet Tracer должно задаваться имя, чувствительное к регистру).

```
R1(config)# ip access-list extended HTTP_ONLY
```

- Командная строка изменится. Теперь активирован режим настройки именованного расширенного ACL-списка. Всем устройствам в локальной сети узла **PC2** требуется доступ TCP. Введите сетевой адрес со знаком вопроса в конце.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
A.B.C.D   Source wildcard bits
```

- Другой способ расчёта маски заключается в вычитании маски подсети из 255.255.255.255.

```
255.255.255.255
- 255.255.255.240
-----
=    0.    0.    0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?
```

- е. Допишите правило, определив адрес сервера как в части 1, и настроив фильтрацию трафика **www**.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

- ф. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от **PC2** на **сервер**. Примечание. Командная строка не меняется, отсутствует необходимость задавать конкретный тип трафика ICMP.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

- г. Остальной трафик запрещён по умолчанию. Выйдите из режима настройки именованного расширенного ACL-списка.

Шаг 2: Примените ACL-список на соответствующем интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора **R1**, трафик, к которому применяется ACL-список **HTTP_ONLY**, является входящим из сети, подключённой к интерфейсу Gigabit Ethernet 0/1. Войдите в режим настройки интерфейса и примените ACL-список.

```
R1(config)# interface gigabitEthernet 0/1  
R1(config-if)# ip access-group HTTP_ONLY in
```

Шаг 3: Проверьте работу ACL-списка.

- Отправьте эхо-запрос от узла **PC2** на **сервер**. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.
- Отправьте FTP-трафик от **PC2** на **сервер**. Подключение не должно установиться.
- Откройте веб-браузер на узле **PC2** и введите IP-адрес **сервера** в виде URL. Подключение должно быть успешным.