ГЛАВА 8

Расширенные списки управления доступом

Маршрутизаторы Cisco используют *списки управления доступом* (Access Control List — ACL) IP для многих целей: распознавания пакетов для принятия решения о фильтрации, распознавания пакетов для *трансляции сетевых адресов* (Network Address Translation — NAT), распознавания пакетов для принятия решения о *качестве обслуживания* (Quality of Service — QoS) и по некоторым другим причинам.

Большинство списков ACL IP являются либо стандартными, либо расширенными. Стандартные списки управления доступом ищут соответствие только по IP-адресу отправителя, а расширенные — по множеству полей заголовка пакета. В то же время списки ACL IP могут быть нумерованными или именованными. На рис. 8.1 в продолжение темы предыдущей главы представлены категории и основные возможности каждого из типов.

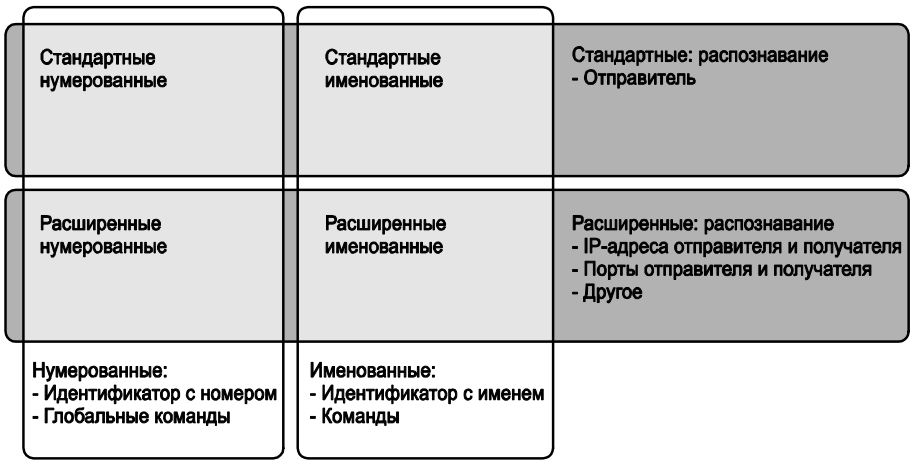

Рис. 8.1. Сравнения типов списков ACL IP

В этой главе обсуждаются три других категории списков ACL, кроме стандартных нумерованных списков ACL IP, а также несколько других тем, связанных со списками ACL IP.

Контрольные вопросы: знаете ли вы темы этой главы

Данный раздел предназначен для того, чтобы читатель мог предварительно оценить свои знания и решить, нужно ли ему читать главу целиком. Если ответы на де-

вять из десяти вопросов даны правильно, можно сразу же перейти к последнему разделу, “Подготовка к экзамену”. Основные темы этой главы и предварительных контрольных вопросов перечислены в табл. 8.1. Отвечая на контрольные вопросы и используя таблицу, читатель сможет достаточно точно оценить свои знания в той или иной области. Ответы на вопросы приведены в приложении А.

Таблица 8.1. Темы контрольных вопросов

Основная тема	Вопросы
Расширенные нумерованные списки управления доступом IP	1–3
Именованные списки ACL и их редактирование	4-5
Дополнительные темы, связанные со списками управления доступом	6-7

1. Для каких из следующих полей не может быть проведено сравнение на основе расширенного списка управления доступом IP? (Выберите несколько ответов.)
   а) Протокол.
   б) IP-адрес отправителя.
   в) IP-адрес получателя.
   г) Байт TOS.
   д) URL.
   е) Имя файла для передачи по протоколу FTP.
2. Какая из следующих команд `access-list` разрешает передачу пакетов от хоста 10.1.1.1 на все веб-серверы, IP-адреса которых начинаются с октетов 172.16.5? (Выберите несколько ответов.)
   а) `access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www.`
   б) `access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www.`
   в) `access-list 2523 permit ip host 10.1.1.1 eq www 172.16.5.0 0.0.0.255.`
   г) `access-list 2523 permit tcp host 10.1.1.1 eq www 172.16.5.0 0.0.0.255.`
   д) `access-list 2523 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www.`
3. Какая из следующих команд `access-list` разрешает передачу пакетов любому веб-клиенту ото всех веб-серверов сети, IP-адреса которых начинаются с октетов 172.16.5?
   а) `access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www.`
   б) `access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www.`
   в) `access-list 2523 permit tcp any eq www 172.16.5.0 0.0.0.255.`
   г) `access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www 172.16.5.0 0.0.0.255.`
   д) `access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www any.`

4. Для каких из следующих полей может быть проведено сравнение с использованием именованного расширенного списка управления доступом IP, но не нумерованного расширенного списка управления доступом IP?

   а) Протокол.

   б) IP-адрес отправителя.

   в) IP-адрес получателя.

   г) Байт TOS.

   д) Ни один из приведенных выше ответов не верен.

5. В маршрутизаторе, работающем под управлением операционной системы IOS версии 12.3, инженер должен удалить вторую строку в списке управления доступом ACL 101, в конфигурацию которого в настоящее время входят четыре команды. Какие из следующих вариантов могут использоваться для этого? (Выберите несколько ответов.)

   а) Удаление всего списка управления доступом и повторный ввод в конфигурацию трех операторов ACL, которые должны остаться в списке управления доступом.

   б) Удаление одной строки из списка управления доступом с помощью команды `no access-list...global`.

   в) Удаление одной строки из списка управления доступом за счет перехода в режим настройки конфигурации списка применительно к данному списку управления доступом и последующего удаления только второй строки с указанием ее порядкового номера.

   г) Удаление последних трех строк из списка управления доступом в режиме настройки конфигурации списка управления доступом и добавление в дальнейшем двух последних операторов снова в список управления доступом.

6. Какими общими рекомендациями следует руководствоваться при использовании расширенных списков управления доступом IP?

   а) Выполнять всю фильтрацию на выходе устройства, если это вообще возможно.

   б) Помещать более общие операторы ближе к началу списка управления доступом.

   в) Фильтровать пакеты на устройстве, расположенном как можно ближе к устройству-отправителю.

   г) Упорядочивать команды ACL с учетом IP-адреса отправителя, от самых низких номеров к самым высоким, для повышения производительности.

7. Для применения каких из указанных ниже инструментальных средств конечный пользователь должен подключиться по протоколу Telnet к маршрутизатору, чтобы получить доступ к хостам, находящимся с другой стороны от маршрутизатора?

   а) Именованные списки управления доступом.

   б) Рефлексивные списки управления доступом.

   в) Динамические списки управления доступом.

   г) Контролируемые по времени списки управления доступом.

Основные темы

Расширенные нумерованные списки управления доступом IP

Расширенные списки управления доступом IP очень похожи на стандартные нумерованные списки ACL, обсуждавшиеся в предыдущей главе. Как и в случае стандартных списков, расширенные списки управления доступом вводятся в действие применительно к интерфейсам для пакетов, либо входящих в интерфейс, либо исходящих из интерфейса. Система IOS проводит поиск в этом списке последовательно. Расширенные списки доступа также используют логику первого соответствия, поскольку маршрутизатор останавливает поиск по списку, как только обнаруживается первый соответствующий оператор, и предпринимает определенное в нем действие. Все эти особенности верны также для стандартных нумерованных списков управления доступом (и именованных списков ACL).

Расширенные списки доступа отличаются от стандартных бо́льшим разнообразием полей заголовка пакета, применяемых для распознавания. Один оператор расширенного списка ACL может задать проверку нескольких элементов заголовка пакета, требуя точного соответствия всех параметров правилам данного оператора ACL. Такая мощная логика распознавания делает расширенные списки управления доступом и более полезными, и более сложными, чем стандартные списки ACL.

Распознавание протокола, IP-адреса отправителя и получателя

Подобно стандартному нумерованному списку ACL IP, расширенный нумерованный список ACL IP также использует глобальную команду `access-list`. Синтаксис тот же, по крайней мере, в использовании ключевых слов `permit` и `deny`. Список параметров распознавания команд, конечно, отличается. В частности, расширенная команда ACL `access-list` требует трех параметров соответствия: тип протокола IP, IP-адрес отправителя и IP-адрес получателя.

Поле Protocol заголовка IP идентифицирует заголовок, который следует за заголовком IP. На рис. 8.2 представлены расположение поля Protocol в заголовке IP, концепция указания на тип следующего заголовка, а также некоторые подробности заголовка IP для справки.

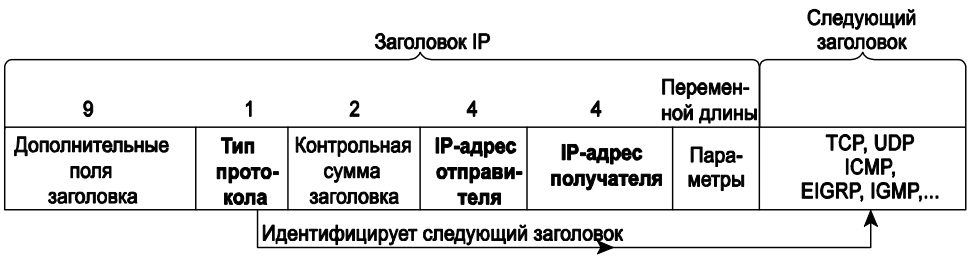

Рис. 8.2. Заголовок IP с выделенными полями, необходимыми для расширенного списка ACL

Операционная система IOS требует настройки параметров для трех частей, выделенных на рис. 8.2. Для типа протокола используется такое ключевое слово, как `tcp`, `udp` или `icmp`, для пакетов IP, у которых после заголовка IP есть заголовок TCP,

UDP или ICMP соответственно. Либо можно использовать ключевое слово `ip`, означающее "все пакеты IP". Необходимо также настроить несколько значений для расположенных далее полей IP-адреса отправителя и получателя. Для этих полей используется тот же синтаксис и параметры распознавания IP-адреса, которые обсуждались в главе 7. Синтаксис представлен на рис. 8.3.

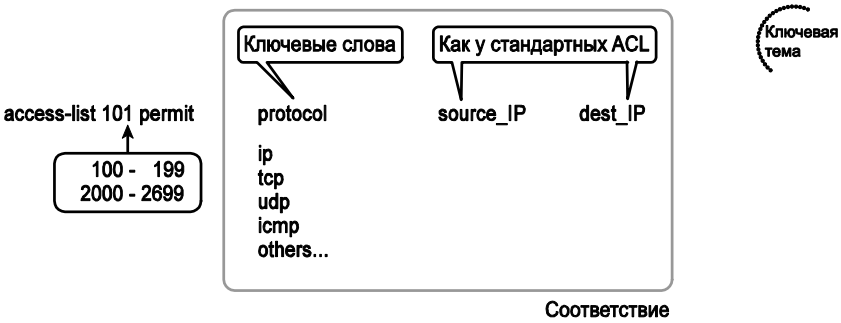

Рис. 8.3. Синтаксис расширенных списков ACL с необходимыми полями

ВНИМАНИЕ!

В распознавании полей IP-адресов отправителя и получателя есть одно различие со стандартными списками ACL: при поиске определенного IP-адреса расширенные списки ACL требуют использования ключевого слова `host`. Нельзя просто указать один IP-адрес.

В табл. 8.2 приведено несколько команд `access-list`, которые используют только необходимые параметры распознавания. Можно закрыть правую сторону таблицы и использовать ее для обучения или изучить объяснения, чтобы понять логику некоторых типичных команд.

Таблица 8.2. Команды `access-list` расширенного списка управления доступом и пояснения к применяемым принципам распознавания

Оператор `access-list`	Какой пакет соответствует правилу
`access-list 101 deny tcp any any`	Любой пакет IP, имеющий заголовок TCP
`access-list 101 deny udp any any`	Любой пакет IP, имеющий заголовок UDP
`access-list 101 deny icmp any any`	Любой пакет IP, имеющий заголовок ICMP
`access-list 101 deny ip 1.1.1.1 2.2.2.2`	Все пакеты IP от хоста 1.1.1.1, следующие на хост 2.2.2.2, независимо от заголовка после заголовка IP
`access-list 101 deny udp 1.1.1.0 0.0.0.255 any`	Все пакеты IP, у которых есть заголовок UDP после заголовка IP, следующие из подсети 1.1.1.0/24 к любому получателю

Последняя запись в табл. 8.2 позволяет сделать важное заключение о том, как операционная система IOS обрабатывает расширенные списки ACL:

Ключевая тема **Важнейшая особенность логики расширенных списков ACL**

В команде `access-list` *расширенного списка ACL, чтобы пакет считался соответствующим команде, все параметры распознавания должны соответствовать полям пакета.*

Например, в последней строке табл. 8.2 команда проверяет наличие заголовка UDP, IP-адреса отправителя из подсети 10.1.1.0/24 и любого IP-адреса получателя. Если бы был исследован пакет с IP-адресом отправителя 10.1.1.1, то он прошел бы проверку IP-адреса отправителя, но если бы он имел заголовок TCP, а не UDP, то не соответствовал бы данной команде `access-list`. Соответствовать должны все параметры.

Проверка номеров портов TCP и UDP

Расширенные списки управления доступом позволяют также исследовать части заголовков TCP и UDP, в частности, поля номера порта получателя и отправителя. Номера портов идентифицируют приложение, которое посылает или получает данные.

Чаще всего проверяют порты, являющиеся стандартными портами, используемыми серверами. Например, веб-серверы используют по умолчанию стандартный порт 80. На рис. 8.4 представлено расположение номеров портов в заголовке TCP после заголовка IP.

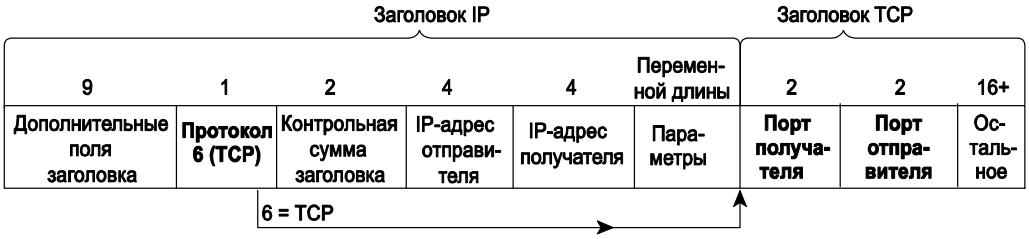

Рис. 8.4. Поля номеров портов в заголовке TCP, сопровождающем заголовок IP

Когда команда расширенного списка ACL включает ключевое слово `tcp` или `udp`, она может (необязательно) проверить порт отправителя и/или получателя. Для этого синтаксис использует для номеров портов ключевые слова равно (equal), не равно (not equal), меньше (less), больше (greater) и диапазон (range). Кроме того, команда может использовать литеральные или десятичные номера портов либо более удобные ключевые слова для некоторых общеизвестных портов приложений. Позиции полей портов отправителя и получателя в команде `access-list`, а также ключевых слов для номеров портов представлены на рис. 8.5.

В качестве примера рассмотрим простую сеть, показанную на рис. 8.6. Сервер FTP находится справа на рисунке, а клиент — слева. На рис. 8.6 показаны синтаксические конструкции списка управления доступом, применяемые для проверки соответствия перечисленных ниже типов пакетов критериям списка.

- Пакеты, которые включают заголовок TCP.
- Пакеты, отправленные из подсети клиента.
- Пакеты, отправленные в подсеть сервера.
- Пакеты с портом получателя TCP, равным 21 (порт управления сервера FTP).

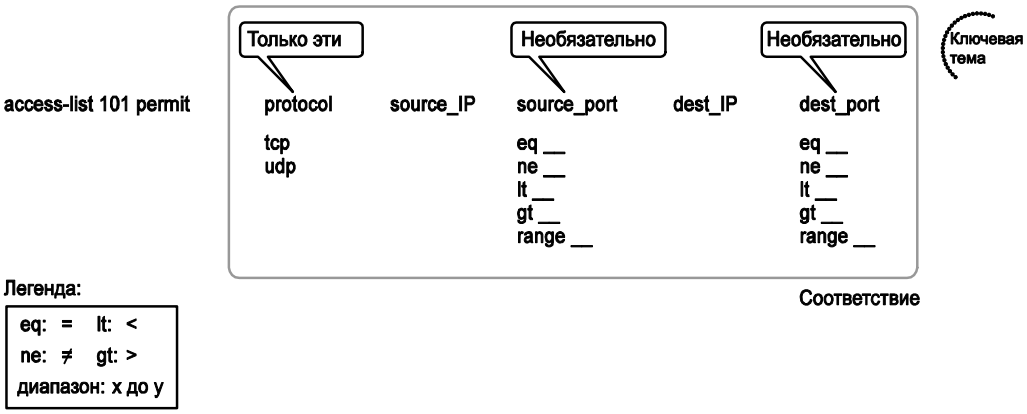

Рис. 8.5. Расширенный синтаксис команд ACL с номерами портов при использовании протокола TCP или UDP

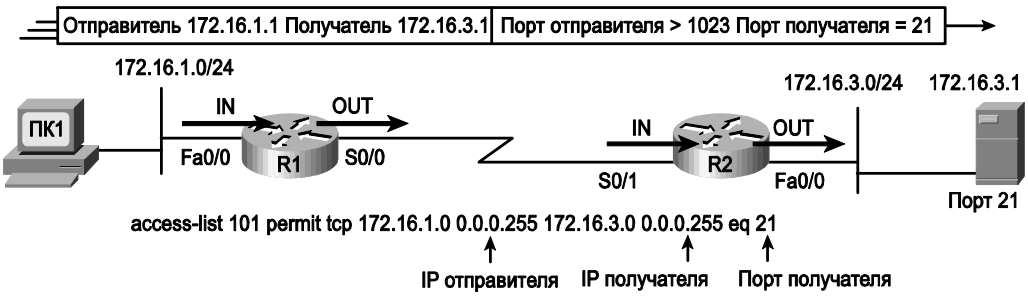

Рис. 8.6. Фильтрация пакетов на основе номера порта получателя

Чтобы полностью разобраться в том, как происходит проверка номера порта получателя на основе параметра `eq 21`, рассмотрим пакеты, движущиеся слева направо, от компьютера ПК1 к серверу. Предположим, на сервере используется зарезервированный порт 21 (порт управления протокола FTP), поэтому у пакета, отправленного компьютером ПК1, в своем заголовке TCP указан порт получателя 21. Синтаксическая конструкция команды в списке управления доступом включает параметр `eq 21` *после* IP-адреса получателя. Позиция после параметров адреса получателя важна: она свидетельствует о том, что параметр `eq 21` следует сравнивать с портом получателя пакета. В результате оператор списка управления доступом, показанный на рис. 8.6, будет успешно сопоставлен с пакетом (в том числе номер порта получателя 21), если он задан в любом из четырех вариантов, обозначенных четырьмя стрелками на этом рисунке.

С другой стороны, на рис. 8.7 показан обратный поток, в котором происходит передача ответного пакета от сервера компьютеру ПК1. В этом случае в заголовке TCP пакета указан порт отправителя 21, поэтому в списке управления доступом необходимо предусмотреть проверку значения номера порта отправителя, равного 21, а сам список управления доступом должен быть задан для других интерфейсов.

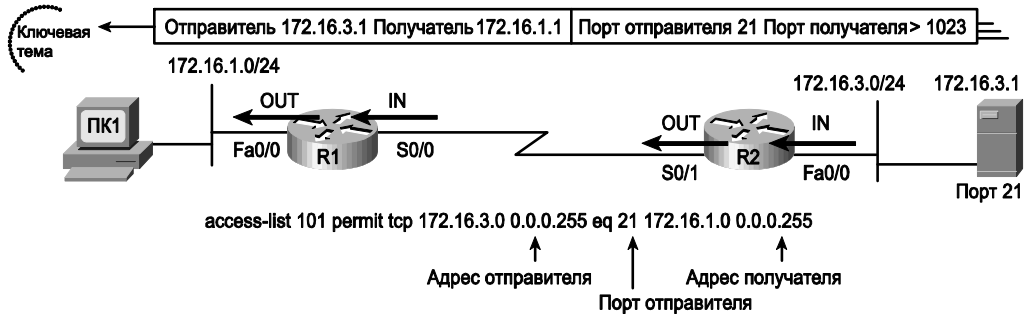

Рис. 8.7. Фильтрация пакетов по данным о номере порта отправителя

В экзаменационных вопросах по спискам ACL и распознаванию номеров портов сначала рассмотрите позицию параметра и направление, в котором будет применен список ACL. Направление определяет, передают ли пакет на сервер или с сервера. Теперь можно решить, требуется ли проверить в пакете порт отправителя или получателя, с учетом того, что проверяемая служба использует стандартный порт.

Для справки в табл. 8.3 перечислены наиболее известные номера портов, а также соответствующие им приложения и протоколы транспортного уровня. Следует учитывать, что синтаксис команд `access-list` допускает применение и номеров портов, и сокращенных вариантов имен приложений.

Таблица 8.3. Распространенные приложения и соответствующие им стандартные номера портов

Номер порта	Протокол	Приложение	Ключевое слово в команде `access-list`
20	TCP	FTP	`data ftp-data`
21	TCP	Управление сервером FTP	`ftp`
22	TCP	SSH	—
23	TCP	Telnet	`telnet`
25	TCP	SMTP	`Smtp`
53	UDP, TCP	DNS	`Domain`
67, 68	UDP	DHCP	`nameserver`
69	UDP	TFTP	`Tftp`
80	TCP	HTTP (WWW)	`www`
110	TCP	POP3	`pop3`
161	UDP	SNMP	`Snmp`
443	TCP	SSL	—
16 384–32 767	UDP	Передача голоса (VoIP) и видео на основе RTP	—

В табл. 8.4 приведено несколько примеров команд `access-list` с распознаванием на основании номера порта. Закройте правую сторону таблицы и попытайтесь охарактеризовать пакеты, соответствующие каждой команде. Затем проверьте свои ответы по правой стороне таблицы.

Таблица 8.4. Примеры команд расширенных списков ACL и объяснение логики

Оператор `access-list`	Чему соответствует
`access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23`	Пакеты с заголовком TCP, любым IP-адресом отправителя, с номером порта отправителя больше (`gt`) 1023, IP-адресом получателя 10.1.1.1 и номером порта получателя, равным (`eq`) 23
`access-list 101 deny tcp any host 10.1.1.1 eq 23`	То же, что и выше, но подходят любые порты отправителя, поскольку этот параметр в данном случае пропущен
`access-list 101 deny tcp any host 10.1.1.1 eq telnet`	То же, что и выше, но вместо указания порта 23 используется ключевое слово `telnet`
`access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any`	Пакет с отправителем в сети 1.0.0.0, использующий протокол UDP с портом отправителя, номер которого меньше (`lt`) 1023, и любым IP-адресом получателя

Конфигурирование расширенных списков управления доступом

Как уже было сказано, расширенные списки управления доступом позволяют проводить проверку многих полей из различных заголовков в пакете IP, поэтому синтаксис соответствующей команды вряд ли можно легко подытожить в виде одной универсальной команды.

Однако для подготовки к экзамену CCNA можно ориентироваться на две синтаксические конструкции, приведенные в табл. 8.5.

Таблица 8.5. Команды настройки конфигурации расширенных списков управления доступом IP

Команда	Режим настройки конфигурации и описание
`access-list` *номер* {deny | permit} *протокол адрес-отправителя шаблон_маски-отправителя адрес-получателя шаблон_маски-получателя* [log | log-input]	Глобальная команда для расширенных нумерованных списков управления доступом. Используются номера 100–199 или 2000–2699 включительно
`access-list` *номер* {deny | permit} {tcp | udp} *адрес-отправителя шаблон_маски-отправителя* [*оператор* [*порт*]] *адрес-получателя шаблон_маски-получателя* [*оператор* [*порт*]] [established] [log]	Версия команды `access-list` с параметрами, специфическими для протокола TCP или UDP

Процесс настройки конфигурации расширенных списков управления доступом в основных чертах совпадает с аналогичным процессом, используемым для стандартных списков управления доступом. В первую очередь необходимо выбрать положение и направление, чтобы можно было планировать применение параметров списка управления доступом с учетом информации в пакетах, проходящих в выбранном направлении. Настройка конфигурации списка управления доступом осуществляется с помощью команд `access-list`, а по завершении, чтобы задействовать список ACL, используется такая же команда `ip access-group`, применяемая для стандартных списков управления доступом. Все эти этапы отражают то, что происходит со стандартными списками управления доступом; однако при настройке помните о следующих различиях.

Ключевая тема **Советы и рекомендации по проверке портов TCP и UDP с использованием списков ACL**

- Располагайте расширенные списки управления доступом как можно ближе к отправителю пакетов, подлежащих фильтрации. Применение фильтрации ближе к источнику экономит полосу пропускания.
- Помните, что пакет считается соответствующим оператору `access-list`, только при полном совпадении всех параметров в одной из команд `access-list` с соответствующими полями пакета.
- Для расширенной команды `access-list` могут использоваться номера 100–199 или 2000–2699, причем ни один номер не рассматривается как более предпочтительный по отношению к другому.

Расширенные списки управления доступом. Пример 1

Назначение данного примера состоит в более глубоком изучении основного синтаксиса списков. В данном случае предполагается, что для компьютера Боб запрещен доступ ко всем серверам FTP в сети Ethernet маршрутизатора R1 и для компьютера Ларри запрещен доступ к веб-серверу Сервер 1. На рис. 8.8 еще раз показана топология сети, которая рассматривалась в предыдущем примере. В примере 8.1 показана конфигурация маршрутизатора R1.

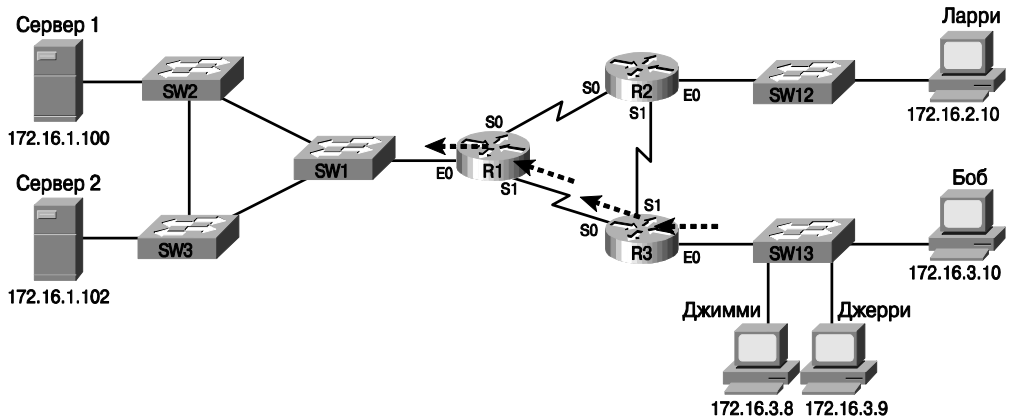

Рис. 8.8. Схема сети для примера 1 применения расширенного списка управления доступом

Пример 8.1. Расширенный список управления доступом маршрутизатора R1: пример 1

```
interface Serial0
   ip address 172.16.12.1 255.255.255.0
   ip access-group 101 in
!
interface Serial1
   ip address 172.16.13.1 255.255.255.0
   ip access-group 101 in
!
access-list 101 remark Stop Bob to FTP servers, and Larry to Server 1 web
access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
```

```
access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
```

Первый оператор списка управления доступом предотвращает для компьютера Боб доступ к серверам FTP в подсети 172.16.1.0. Второй оператор предотвращает для компьютера Ларри доступ к веб-службам на компьютере Сервер 1. Последний оператор разрешает весь прочий трафик.

Прежде всего рассмотрим синтаксис этих операторов, поскольку необходимо описать в нем несколько новых особенностей. Вначале напомним, что номера, применяемые в расширенных списках управления доступом, должны находиться в диапазоне 100–199 или 2000–2699. Вслед за указанием действия ключами `permit` или `deny` должен находиться параметр с обозначением протокола, который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками TCP или UDP. Если проверке подлежат номера портов TCP или UDP, то должен быть указан протокол TCP или UDP. (И FTP, и веб используют протокол TCP.)

В этом примере используется ключевое слово `eq`, означающее "равно", для проверки номеров портов получателей, относящихся к протоколу управления FTP (ключевое слово `ftp`), и трафика HTTP (ключевое слово `www`). Безусловно, можно использовать числовые значения, но для наиболее распространенных значений номеров портов более удобной является текстовая версия параметра. (В частности, в случае применения в команде оператора `eq 80` в конфигурации отображается `eq www`.)

Этот пример задействует список ACL в двух местах на маршрутизаторе R1: входящие на каждом последовательном интерфейсе. Эти расположения удовлетворяют задаче ACL. Как будет описано в конце данной главы, корпорацией Cisco даны некоторые конкретные рекомендации в отношении того, где должны находиться списки управления доступом. Поэтому в примере 8.2 достигается та же цель, что и в примере 8.1, т.е. предотвращается доступ для компьютера Боб к серверам FTP, находящимся в основном хосте, причем для решения этой задачи применяется список управления доступом, введенный в конфигурацию маршрутизатора R3.

Пример 8.2. Применение в маршрутизаторе R3 расширенного списка управления доступом для блокирования пакетов от компьютера Боб на сервер FTP, находящийся рядом с маршрутизатором R1

```
interface Ethernet0
   ip address 172.16.3.1 255.255.255.0
   ip access-group 103 in
access-list 103 remark deny Bob to FTP servers in subnet 172.16.1.0/24
access-list 103 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
access-list 103 permit ip any any
```

Новая конфигурация на маршрутизаторе R3 соответствует задаче фильтрации трафика компьютера Боб, а также общей задаче по расположению списков ACL ближе к отправителю пакетов. Список ACL 103 на маршрутизаторе R3 очень похож на список ACL 101 маршрутизатора R1 из примера 8.1, но на сей раз он не проверяет критерии, соответствующие трафику компьютера Ларри, поскольку он никогда не будет попадать на интерфейс Ethernet 0 маршрутизатора R3. Список ACL 103 фильтрует трафик FTP компьютера Боб в направлении к подсети 172.16.1.0/24 со всем другим трафиком, вводящим на интерфейс E0 маршрутизатора R3 и попадающим затем в общую сеть.

Расширенные списки управления доступом. Пример 2

В примере 8.3, в основе которого лежит сеть, показанная на рис. 8.9, демонстрируется еще один способ использования расширенных списков управления доступом IP. В данном примере используются следующие критерии.

- Компьютеру Сэм запрещен доступ к компьютеру Багс или Даффи.
- Для хостов в сети Ethernet маршрутизатора Seville запрещен доступ к хостам сети Ethernet маршрутизатора Yosemite.
- Обмен данными между всеми прочими хостами разрешен.

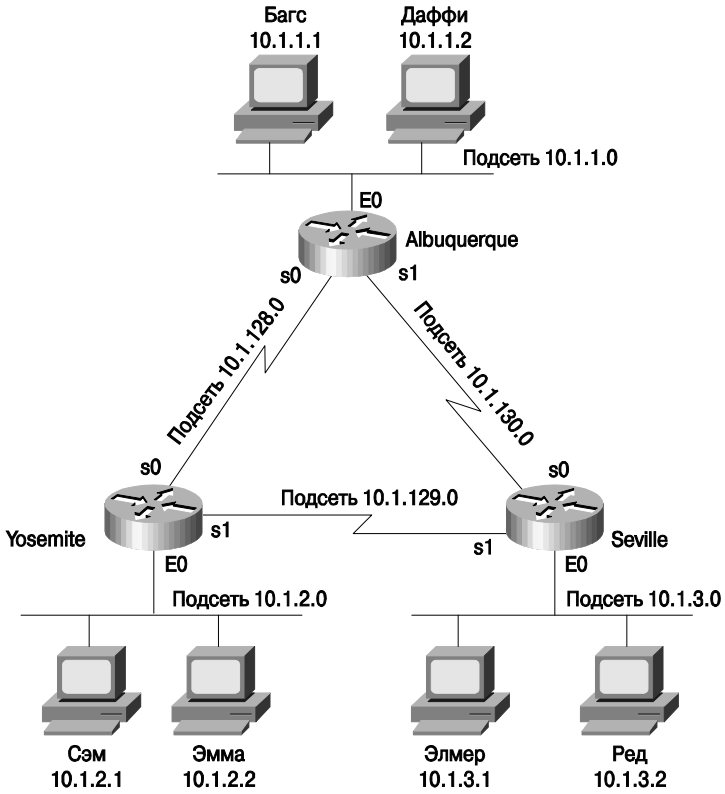

Рис. 8.9. Схема сети для примера 2 применения расширенного списка управления доступом

Пример 8.3. Конфигурация маршрутизатора Yosemite для примера 2 расширенного списка управления доступом

```
interface ethernet 0
   ip access-group 110 in
!
access-list 110 deny ip host 10.1.2.1 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.1.2.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 110 permit ip any any
```

Эта конфигурация позволяет решить поставленную задачу с помощью всего лишь нескольких операторов и вместе с тем соответствует рекомендациям по проектированию сетей от корпорации Cisco, поскольку предусматривает размещение расширенных списков управления доступом как можно ближе к отправителям трафика. Список управления доступом фильтрует пакеты, поступающие на интерфейс E0 маршрутизатора Yosemite, который является первым интерфейсом маршрутизатора, куда поступают пакеты, отправленные с компьютера Сэм. Если маршрут между маршрутизатором Yosemite и другими подсетями со временем изменится, список ACL все еще будет применим. Кроме того, требование по фильтрации, которое указано в качестве второго пункта задачи (согласно которому необходимо предотвратить для хостов локальной сети Seville доступ к маршрутизатору Yosemite), выполняется с помощью второго оператора `access-list`. Предотвращение возможности передачи пакетов из подсети локальной сети маршрутизатора Yosemite в подсеть локальной сети маршрутизатора Seville по существу исключает эффективный обмен данными между этими двумя подсетями. Еще один вариант состоит в том, что в конфигурации маршрутизатора Seville могут быть реализованы противоположные требования.

Практические задачи на создание команд списков управления доступом

В табл. 8.6 приведены практические задачи, способные помочь приобрести навыки в синтаксисе команды `access-list` расширенных списков ACL, особенно в выборе правильной логики распознавания. Задача заключается в создании однострочного расширенного списка ACL, который соответствует пакетам. Ответы находятся в разделе "Ответы на практические задачи главы". Обратите внимание на то, что если критерий упоминает определенный протокол прикладной программы, например "веб-клиент", то это означает соответствие именно этому протоколу.

Таблица 8.6. Создание однострочных расширенных списков ACL. Задачи

Задача	Критерий
1	От веб-клиента 10.1.1.1, следующие на веб-сервер в подсети 10.1.2.0/24
2	От клиента Telnet 172.16.4.3/25, следующие на сервер Telnet в подсети 172.16.3.0/25. Соответствие также всем хостам в подсети клиента
3	Сообщения ICMP из подсети 192.168.7.200/26 всем хостам в подсети 192.168.7.14/29
4	От веб-сервера в подсети 10.2.3.4/23/23 к клиентам в подсети 10.4.5.6/22
5	От подсети сервера Telnet 172.20.1.0/24 к клиентам в подсети 172.20.44.1/23
6	Пакеты от веб-клиента подсети 192.168.99.99/28, следующие на веб-сервер в подсети 192.168.176.0/28. Соответствие также всем хостам в подсети клиента
7	Сообщения ICMP из подсети 10.55.66.77/25 всем хостам в подсети 10.66.55.44/26
8	Любой и каждый пакет IPv4

Именованные списки ACL и их редактирование

На данный момент читатель должен полностью разобраться в основных понятиях списков управления доступом IP, применяемых в операционной системе IOS. В настоящем разделе рассматривается ряд усовершенствований списков управления дос-

тупом в системе IOS: именованные списки управления доступом и их редактирование с помощью порядковых номеров. Безусловно, обе указанные возможности являются важными и нужными, но не вносят какие-либо дополнительные функции по отношению к тем, с помощью которых маршрутизатор может фильтровать трафик. Вместо этого именованные списки управления доступом и порядковые номера списков управления доступом позволяют проще запоминать их имена и редактировать существующие списки управления доступом, если потребуется их изменить.

Именованные списки управления доступом

Именованные списки ACL IP имеют много сходств с нумерованными списками ACL IP. Они применяются для фильтрации пакетов, а также для многих других целей. Точно так же, подобно стандартным и расширенным нумерованным спискам ACL, которые отличаются возможностями распознавания пакетов, именованные списки ACL могут быть стандартными и расширенными.

Первоначально именованные списки ACL имели три существенных отличия от нумерованных списков ACL.

Ключевая тема **Различия между именованными и нумерованными списками ACL**

- Вместо номеров для идентификации списков ACL используются имена, облегчающие запоминание причин их применения.
- Для определения действий и параметров распознавания используются команды подсистемы ACL, а не глобальные команды.
- Лучшие инструменты редактирования списков ACL.

Изучить конфигурацию именованных списков ACL довольно легко, достаточно преобразовать нумерованный список ACL в именованный эквивалент. Такое преобразование простого стандартного списка ACL номер 1 из трех строк приведено на рис. 8.10. Чтобы создать три подкоманды `permit` для именованного списка ACL, достаточно скопировать части трех команд нумерованного списка ACL, начиная с ключевого слова `permit`.

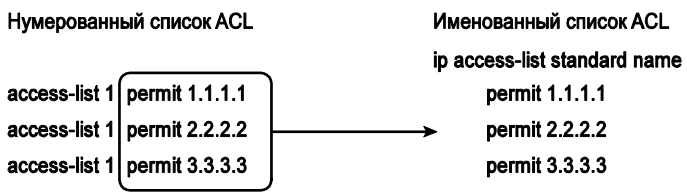

Рис. 8.10. Конфигурации нумерованного и именованного списков ACL

Единственная действительно новая часть конфигурации именованных списков ACL — это глобальная команда конфигурации `ip access-list`, которая определяет, является ли список ACL стандартным или расширенным, а также определяет имя. Она также переводит пользователя в режим конфигурации ACL, как видно в следующем примере 8.4. В режиме конфигурации ACL, настраиваются команды `permit`, `deny` и `remark`, которые отражают синтаксис команд `access-list` нуме-

рованных списков ACL. У стандартных именованных списков ACL эти команды соответствуют синтаксису стандартных нумерованных списков ACL, а у расширенных именованных списков ACL — синтаксису команд расширенных нумерованных списков ACL.

Именованные списки ACL, как уже упоминалось, преодолевают недостаток нумерованных списков ACL относительно редактирования или изменения. Именованные списки ACL изначально позволяют довольно просто удалить команду `permit` или `deny`, если использовать перед той же командой приставку `no`. Пример 8.4 демонстрирует конфигурацию именованного списка ACL, а затем удаление одной строки из него. Обратите особое внимание на приглашения, которые демонстрируют переход в режим конфигурации ACL.

Пример 8.4. Конфигурация именованного списка доступа

```
conf t
Enter configuration commands, one per line. End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#permit tcp host 10.1.1.2 eq www any
Router(config-ext-nacl)#deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
Router(config-ext-nacl)#deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
Router(config-ext-nacl)#deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#interface serial1
Router(config-if)#ip access-group barney out
Router(config-if)#^Z
Router#show running-config
Building configuration...

Current configuration:

.
! строки пропущены для краткости

interface serial 1
  ip access-group barney out
!
ip access-list extended barney
permit tcp host 10.1.1.2 eq www any
deny   udp host 10.1.1.1 10.1.2.0 0.0.0.255
deny   ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
deny   ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
permit ip any any
Router#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#no deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
Router(config-ext-nacl)#^Z
Router#show access-list

Extended IP access list barney
    10 permit tcp host 10.1.1.2 eq www any
    20 deny   udp host 10.1.1.1 10.1.2.0 0.0.0.255
    30 deny   ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
    50 permit ip any any
```

Пример 8.4 начинается с создания списка управления доступом, обозначенного именем “barney”. С помощью команды `ip access-list extended barney` создается список управления доступом, ему присваивается имя “barney”, после чего пользователь переходит в режим настройки конфигурации списка управления доступом. Эта команда содержит также сведения для системы IOS о том, что “barney” представляет собой расширенный список управления доступом. Затем следуют пять операторов с ключевыми словами `permit` и `deny`, которые определяют критерии проверки пакетов и указывают, какие действия должны быть выполнены в случае совпадения параметров пакета с правилом списка. Обратите внимание: команда `deny`, выделенная серым, удаляется далее в этом примере.

Команда `show running-config` выводит данные о конфигурации, определяемой именованным списком управления доступом, перед тем как удаляется отдельная запись из списка. Затем с помощью команды `no deny ip...` удаляется одна запись из списка управления доступом. Обратите внимание на то, что для иллюстрации используется еще одна команда, `show access-list`, в конце примера, которая выводит содержимое списка управления доступом, но на этот раз в выводе обнаруживаются четыре правила `permit` и `deny` вместо пяти.

Редактирование списков управления доступом с использованием порядковых номеров

Применение нумерованных списков управления доступом было предусмотрено в системе IOS с самых первых моделей маршрутизаторов Cisco. Со времени их создания и вплоть до версии 12.2 операционной системы Cisco IOS единственным способом редактирования существующих нумерованных списков управления доступом (например, лишь для того, чтобы просто удалить строку из списка управления доступом) было полное удаление списка управления доступом и повторный ввод в конфигурацию всех требуемых команд списка. В связи с этим инженеру приходилось сталкиваться с неудобствами; кроме того, использование такого процесса приводило к некоторым неблагоприятным побочным эффектам.

Предположим, например, что настроена команда `ip access-list 101 permit tcp any any eq 80`, и это третья строка списка ACL. Теперь решено попробовать удалить эту строку вводом той же команды с приставкой `no` вначале: `no ip access-list 101 permit tcp any any eq 80`. Но удален оказался весь список ACL 101! Удалить эту строку в списке ACL нет никакого способа.

При удалении любого списка управления доступом важно учитывать следующее требование: вначале необходимо отключить список управления доступом во всех интерфейсах, с которыми он связан, затем удалить его и повторно внести в конфигурацию и наконец — включить его на нужных интерфейсах. В противном случае в процессе перенастройки конфигурации, до того как будут введены в конфигурацию все операторы, список управления доступом не выполняет все требуемые проверки, что иногда приводит к возникновению проблем или сеть становится подверженной различным атакам.

Ныне операционная система IOS позволяет удалять и добавлять отдельные строки как в именованных, так и нумерованных списках ACL. Именованные списки ACL изначально были реализованы так, чтобы позволить удалять строки из списка ACL, но добавлять их только в конец списка. После появления версии IOS 12.3 корпорация

Cisco предусмотрела возможность применения некоторых дополнительных средств настройки конфигурации списков управления доступом, которые относятся и к именованным, и к нумерованным спискам управления доступом IP. В этих средствах настройки используются порядковые номера в списке управления доступом, которые добавляются к каждому оператору `permit` или `deny`, так что эти номера отражают последовательность операторов в списке. Благодаря введению порядковых номеров в списки управления доступом появились следующие возможности работы как с нумерованными, так и с именованными списками.

Средства, предоставляемые операционной системой IOS 12.3 порядковым номерам ACL

- **Новый стиль конфигурации для нумерованных списков**. Нумерованные списки ACL используют теперь стиль конфигурации, как у именованных, а также традиционный стиль для тех же списков ACL; для расширенного редактирования списков ACL необходим новый стиль.
- **Удаление отдельных строк**. С помощью команды `no` *`порядковый_номер`* можно удалять в списке управления доступом отдельные строки операторов `permit` или `deny`.
- **Вставка новых строк**. Добавляемые команды `permit` и `deny` можно задавать в конфигурации с указанием порядкового номера, определяя местонахождение оператора в списке управления доступом.
- **Автоматическая нумерация**. Операционная система IOS сама добавляет командам порядковые номера при настройке, даже если вы их не задаете сами.

Чтобы иметь возможность удалять и вставлять строки в списке управления доступом, и в нумерованных, и в именованных списках управления доступом необходимо использовать один общий стиль конфигурирования и вводить такие же команды, которые служат для работы с именованными списками управления доступом. Единственное различие в синтаксисе заключается в том, используется ли для обозначения списка имя или номер. В примере 8.5 показана конфигурация стандартного нумерованного списка управления доступом IP, демонстрирующая указанный альтернативный стиль настройки конфигурации. На основании этого примера можно судить, насколько широкие возможности для редактирования предоставляют порядковые номера списка управления доступом. В данном примере выполняются описанные ниже действия.

Этап 1 Создание нумерованного списка ACL 24, состоящего из трех команд `permit`, с использованием конфигурации в новом стиле

Этап 2 Вывод с помощью команды `show ip access-list` трех команд `permit` с порядковыми номерами 10, 20 и 30

Этап 3 Удаление инженером только второй команды `permit` с использованием подкоманды `no 20` для списка управления доступом, в которой указан порядковый номер 20

Этап 4 Проверка с помощью команды `show ip access-list` того, что список управления доступом содержит теперь только две строки (с порядковыми номерами 10 и 30)

Этап 5 Добавление инженером новой команды `permit` к началу списка управления доступом с использованием команды конфигурирования списка управления доступом `5 deny 10.1.1.1`

Этап 6 Повторная проверка с помощью команды `show ip access-list` правильности внесенных изменений, которая показывает, что на сей раз имеются три команды `permit` с порядковыми номерами 5, 10 и 30

ВНИМАНИЕ!

В отношении данного примера следует отметить, что пользователь не выходит из режима конфигурации устройства, а вместо этого использует команду `do` для передачи системе IOS указания, что команда режима EXEC `show ip access-list` должна быть выполнена без выхода из режима настройки конфигурации.

Пример 8.5. Редактирование списков управления доступом с использованием порядковых номеров

```
! Этап 1. В конфигурацию введен стандартный нумерованный список
! управления доступом IP, состоящий из трех строк.
R1#configure terminal
Enter configuration commands, one per line. End with Ctrl-Z.
R1(config)#ip access-list standard 24
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.2.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.3.0 0.0.0.255
! Этап 2. Отображение содержимого списка управления доступом без выхода
! из режима настройки конфигурации.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.1.2.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
! Этап 3. Удаление строки с порядковым номером 20 в условиях дальнейшего
! пребывания в режиме настройки конфигурации списка ACL 24.
R1(config-std-nacl)#no 20
! Этап 4. Повторное отображение содержимого списка управления доступом
! без выхода из режима настройки конфигурации.
! Обратите внимание на то, что теперь строка с номером 20 отсутствует в
! результатах вывода.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
! Этап 5. Вставка новой первой строки в список управления доступом.
R1(config-std-nacl)#5 deny 10.1.1.1
! Этап 6. Отображение содержимого списка управления доступом в последний
! раз, что позволяет видеть новый оператор (с порядковым
! номером 5), находящийся на первом месте в списке.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    5 deny 10.1.1.1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
```

Следует отметить, что настройку конфигурации нумерованных списков управления доступом можно выполнять с помощью команд настройки конфигурации в новом стиле, как показано в примере 8.5, или задавать конфигурацию в старом стиле с использованием глобальных команд конфигурации `access-list`, как показано

в нескольких первых примерах настоящей главы. Фактически предусмотрена возможность использовать оба стиля настройки конфигурации в каждом отдельном списке управления доступом. Но, независимо от используемого стиля конфигурации, в выводе команды `show running-config` по-прежнему отображаются команды конфигурации в старом стиле. В примере 8.6 демонстрируются указанные возможности, причем этот пример, в котором выполняются описанные ниже дополнительные этапы, является продолжением примера 8.5.

Этап 7 Вывод инженером результатов настройки конфигурации (с помощью команды `show running-config`), в которых отображаются команды конфигурации в старом стиле, даже несмотря на то, что сам список управления доступом был создан с помощью команд в новом стиле

Этап 8 Добавление инженером нового оператора в конце списка управления доступом с использованием глобальной команды конфигурации `access-list 24 permit 10.1.4.0 0.0.0.255` в старом стиле

Этап 9 Подтверждение с помощью команды `show ip access-list` того, что команда `access-list` в старом стиле, выполненная на предыдущем этапе, добавлена в соответствии с правилом, согласно которому она должна появиться только в конце списка управления доступом

Этап 10 Отображение инженером конфигурации для подтверждения того, что все части списка ACL, конфигурация которых была настроена и с помощью команд в новом стиле, и с помощью команд в старом стиле, присутствуют в выводе одного и того же списка управления доступом в старом стиле (с помощью команды `show running-config`)

Пример 8.6. Добавление к нумерованному списку управления доступом новых команд конфигурации и его отображение

```
! Этап 7. Фрагмент конфигурации, относящийся к списку ACL 24.
R1#show running-config
! Единственными отображаемыми строками являются строки из списка ACL 24
access-list 24 deny   10.1.1.1
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255

! Этап 8. Добавление новой глобальной команды access-list 24
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 24 permit 10.1.4.0 0.0.0.255
R1(config)#^Z
! Этап 9. Повторное отображение содержимого списка управления доступом с
! порядковыми номерами. Обратите внимание на то, что даже
! новому оператору был автоматически присвоен порядковый номер.
R1#show ip access-list 24
Standard IP access list 24
    5  deny   10.1.1.1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
    30 permit 10.1.3.0, wildcard bits 0.0.0.255
    40 permit 10.1.4.0, wildcard bits 0.0.0.255
!
! Этап 10. Конфигурация нумерованного списка управления доступом
! по-прежнему остается определенной с помощью команд конфигурации в
! старом стиле.
R1#show running-config
! Единственными отображаемыми строками являются строки из списка ACL 24
access-list 24 deny   10.1.1.1
```

```
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255
access-list 24 permit 10.1.4.0 0.0.0.255
```

Дополнительные темы, связанные со списками управления доступом

В этом разделе рассматривается целый ряд небольших тем, в частности, касающихся фильтрации трафика Telnet и SSH с помощью списков управления доступом, а также приводятся некоторые общие практические рекомендации.

Управление доступом по протоколам Telnet и SSH с помощью списков ACL

Операционная система IOS предоставляет непосредственный способ защиты доступа для входящего и исходящего трафика в портах каналов виртуального терминала (vty). Пользователи, работающие по протоколам Telnet и SSH, подключаются к маршрутизатору через соединения vty, поэтому для обеспечения безопасности доступа таких пользователей необходимо применить к ним список управления доступом IP. Можно применить список управления доступом для наложения ограничений на то, с каких хостов в сети IP можно подключаться по протоколу удаленного доступа (допустим, telnet) к маршрутизатору, а также наложить ограничение на сами хосты, с помощью которых можно определить круг пользователей, имеющих право доступа к маршрутизатору.

Предположим, например, что предусмотрено предоставление возможности подключаться по протоколу удаленного доступа к любому из маршрутизаторов Cisco в сети только хостам из подсети 10.1.1.0/24. В таком случае в каждом маршрутизаторе можно использовать конфигурацию, показанную в примере 8.7, чтобы исключить возможность доступа для хостов с IP-адресами, не находящимися в указанной подсети.

Пример 8.7. Управление доступом через соединения vty с использованием команды `access-class`

```
line vty 0 4
  login
  password cisco
  access-class 3 in
!
! Следующая команда является глобальной
  access-list 3 permit 10.1.1.0 0.0.0.255
```

В команде `access-class` применяется ссылка на средства проверки, заданные с помощью команды `access-list 3`. Ключевое слово `in` указывает, что речь идет о входящих запросах на создание соединений Telnet с маршрутизатором, иными словами, о подключении к маршрутизатору с помощью этого протокола удаленного соединения. В том виде, в каком он задан в конфигурации, список ACL 3 проверяет IP-адрес отправителя в пакетах, относящихся к запросам на создание соединений Telnet.

Чтобы использовать ключевое слово `out` в этой команде в режиме vty, например `access-class 3 out`, следует помнить два, возможно удивительных, факта. Во-первых, эта команда относится к пользователю, который уже имеет на маршрутизаторе соединения telnet или SSH с логикой ACL, примененной к дальнейшим попыт-

кам вывода telnet или SSH на маршрутизаторе где-то еще. Таким образом, при применении на маршрутизаторе R1, при попытке установить сеанс telnet сначала к маршрутизатору R1, а затем к R2, маршрутизатор R1 применил бы логику ACL к попытке установить сеанс telnet к маршрутизатору R2. Во-вторых, при использовании ключевого слова `out` команда `access-class 3 out` является одним из тех редких случаев, в которых стандартный список ACL IP фактически проверяет IP-адрес получателя, а не отправителя.

Принципы использования списков управления доступом

В реальных сетях IP работы, связанные с созданием, диагностированием и обновлением списков управления доступом, могут потребовать много времени и усилий. На экзамене ICND2 не так уж много вопросов посвящено нюансам, которые необходимо учитывать при реализации списков управления доступом IP в действующих сетях; больше внимания уделяется некоторым основным принципам, которые обсуждаются в настоящем разделе.

Корпорация Cisco дает приведенные ниже общие рекомендации для курсов, на которых основаны экзамены CCNA.

Рекомендации по реализации списков ACL

Ключевая тема

- Создавайте списки управления доступом с помощью текстового редактора вне маршрутизатора, а затем вносите готовые команды конфигурации в маршрутизатор с использованием копирования и вставки. (Даже несмотря на то, что теперь имеется возможность удалять и вставлять строки в списке управления доступом, подготовка команд в текстовом редакторе все еще, по-видимому, остается наиболее простым методом.)
- Размещайте расширенные списки управления доступом как можно ближе к отправителю пакета, чтобы сразу же отбрасывать определенные типы пакетов.
- Размещайте стандартные списки управления доступом как можно ближе к получателю пакетов, поскольку они часто уничтожают пакеты, которые не должны быть уничтожены, если находятся ближе к отправителю.
- Размещайте более специфичные (т.е. узкие) правила проверки ближе к началу списка управления доступом.
- Прежде чем вносить изменения в список управления доступом, удалите список управления доступом на том интерфейсе, в котором он задан (с помощью команды `no ip access-group`).

Согласно первой рекомендации список управления доступом должен создаваться вне маршрутизатора с помощью текстового редактора. Таким образом, если при вводе команды будут допущены опечатки, их можно исправить в редакторе. Безусловно, значимость этой рекомендации не столь велика, как по отношению к версиям, предшествующим IOS 12.3, поскольку в этой версии была введена поддержка номеров строк списка управления доступом, а также предусмотрена возможность удаления и вставки отдельных строк в списке управления доступом, как было описано в одном из предыдущих разделов.

ВНИМАНИЕ!

Если все применяемые списки управления доступом создаются в текстовом редакторе, то может оказаться удобным начинать каждый файл с команды `no access-list number`, за которой следуют команды конфигурации в списке управления доступом. В таком случае после каждого редактирования текстового файла для внесения изменений в список управления доступом достаточно просто скопировать и вставить содержимое всего файла, причем с помощью первой строки будет выполнено удаление всего существующего списка управления доступом, а остальные операторы воссоздадут новый список управления доступом.

Вторая и третья из приведенных выше рекомендаций касаются места расположения списков управления доступом. Если цель состоит в фильтрации пакетов, то применение критериев, допускающих прохождение только определенных пакетов ближе к их отправителю, означает, что ненужные пакеты с самого начала не будут расходовать пропускную способность сети, что, по-видимому, должно способствовать повышению производительности сети (и действительно способствует). Поэтому корпорация Cisco рекомендует располагать расширенные списки управления доступом настолько близко к отправителю, насколько это возможно.

Но, с другой стороны, корпорация Cisco рекомендует также, по крайней мере на курсах, посвященных подготовке к экзаменам CCNA, располагать стандартные списки управления доступом ближе к получателю. Почему бы такие списки не размещать ближе к отправителю пакетов? Дело в том, что стандартные списки управления доступом обеспечивают только проверку IP-адреса отправителя, поэтому, как правило, будучи размещенными ближе к отправителю, они фильтруют больший объем трафика, чем предполагалось. Предположим, например, что компьютеры Фред и Барни разделены четырьмя маршрутизаторами. Если фильтрация трафика компьютера Барни, направляемого на компьютер Фред, будет осуществляться на первом маршрутизаторе, то пакеты от компьютера Барни не смогут достичь каких-либо хостов, связанных со всеми прочими тремя маршрутизаторами. В связи с этим на курсах ICND2 корпорации Cisco применяется общая рекомендация, согласно которой стандартные списки управления доступом должны находиться как можно ближе к получателю, чтобы была предотвращена фильтрация того трафика, для которого не предназначен данный фильтр.

Кроме того, важно, чтобы более конкретные критерии сопоставления были заданы ближе к началу каждого списка, поскольку при этом уменьшается вероятность появления ошибок в списке управления доступом. Предположим, например, что имеются оператор, разрешающий прохождение всего трафика от хоста 10.1.1.1 к хосту 10.2.2.2 для порта 80 (веб-трафик), и оператор, запрещающий прохождение всех прочих пакетов, отправители которых находятся в подсети 10.1.1.0/24. Оба эти оператора обеспечивают сопоставление с пакетами, отправленными с хоста 10.1.1.1 на веб-сервер, находящийся по адресу 10.2.2.2, но было бы более оправданным проведение сопоставления в первую очередь с помощью более специфичного оператора (`permit`). Вообще говоря, размещение на первых местах более конкретных операторов гарантирует также то, что в списке не будет пропущен какой-либо необходимый критерий.

Наконец, корпорация Cisco рекомендует удалять списки управления доступом в интерфейсах и только после этого приступать к внесению изменений в операторе этого списка. К счастью, если какой-либо список управления доступом IP включен в интерфейсе с помощью команды `ip access-group`, после чего удален весь список

управления доступом, то система IOS прекращает фильтрацию каких-либо пакетов. (В более ранних версиях IOS так было не всегда!) При этом сразу после добавления команд в список управления доступом начинается фильтрация пакетов системой IOS. Предположим, что разрешено применение списка ACL 101 на интерфейсе S0 для исходящих пакетов. Затем происходит удаление списка 101, чтобы было разрешено прохождение всех пакетов. После этого вводится одна команда `access-list 101`. Сразу после нажатия клавиши <Enter> создается список и маршрутизатор начинает фильтровать все пакеты, исходящие из интерфейса S0, на основе этого однострочного списка. Таким образом, даже если должен был введен в действие длинный список управления доступом, может оказаться, что в течение какого-то времени происходит фильтрация пакетов, которые не должны были быть отфильтрованными! Поэтому наилучший путь — запретить применение списка на интерфейсе, внести в него изменения, а затем снова разрешить его применение на интерфейсе.

Рефлексивные списки управления доступом

Рефлексивные списки управления доступом, называемые также средствами фильтрации сеансов IP, позволяют предотвращать атаки определенного класса, направленные на бреши в системе безопасности, поскольку позволяют отдельно пропускать через устройство каждый разрешенный сеанс TCP или UDP. Для этого предусмотрено, чтобы маршрутизатор реагировал определенным образом, обнаруживая первый пакет в новом сеансе обмена данными между двумя хостами. Реагируя на появление пакета, маршрутизатор добавляет в список управления доступом оператор `permit`, в результате чего разрешается прохождение в сеансе трафика, характеризующегося применением определенных IP-адресов отправителя и получателя, а также конкретного порта TCP или UDP.

На рис. 8.11 показан классический случай, в котором при использовании традиционных списков управления доступом создается брешь в защите, а рефлексивные списки управления доступом позволяют закрыть эту брешь. На большинстве предприятий для пользователей допускается возможность подключаться к веб-серверам в Интернете с помощью веб-браузеров. Традиционные расширенные списки управления доступом позволяют разрешить передачу трафика, обеспечив возможность пересылки пакетов в прямом и обратном направлениях между любыми двумя IP-адресами, но с учетом выполнения дополнительной проверки порта TCP, используемого в протоколе HTTP (порт 80). На рис. 8.11 в этом случае показан список управления доступом, с помощью которого проверяется порт 80 отправителя применительно к пакетам, поступающим на предприятие, после чего делается вывод, что пакеты поступили от веб-сервера.

Список управления доступом, используемый в маршрутизаторе R2, фильтрует весь входящий трафик, за исключением трафика от веб-серверов. Это позволяет веб-серверам, находящимся в Интернете и показанным в левой части рисунка, передавать пакеты пользователю на предприятии, показанному справа. Но это также позволяет передавать пакеты и потенциальному взломщику, для чего ему достаточно указать порт отправителя 80, а маршрутизатор будет беспрепятственно пропускать эти пакеты. При этом подобные пакеты могут даже не относиться к существующему соединению TCP, но с их помощью можно предпринять несколько известных атак, начиная от простой атаки по принципу DoS (отказ в обслуживании), при которой осуществляется отправка нескончаемого потока пакетов на предприятие, и заканчивая использованием известных ошибок в операционной системе.

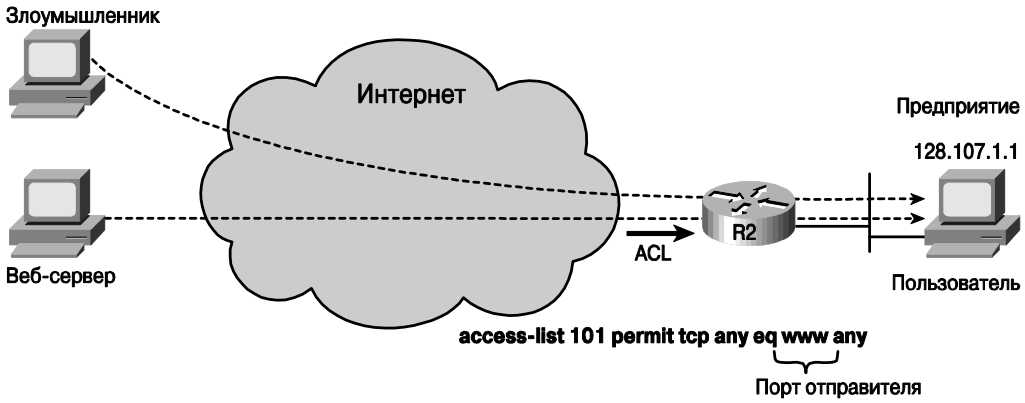

Рис. 8.11. Иллюстрация к ситуации, в которой необходимо применять рефлексивные списки управления доступом

Рефлексивные списки управления доступом в полной мере позволяют законным пользователям передавать и принимать пакеты через маршрутизатор, но отбрасывать все пакеты, поступающие от других хостов, наподобие пакетов, отправленных взломщиком, как показано на рис. 8.11. Если применяются рефлексивные списки управления доступом, то сразу после создания нового сеанса пользователем на предприятии маршрутизатор обнаруживает этот новый сеанс и регистрирует IP-адреса отправителя и получателя, а также порты, используемые в этом сеансе. Рефлексивный список управления доступом, применяемый в маршрутизаторе R2, не допускает прохождение всего трафика с номером порта 80. Вместо этого с помощью данного списка разрешается передача только тех пакетов, в которых адреса и порты совпадают с данными оригинального пакета. Например, если бы на персональном компьютере, показанном справа, был инициирован сеанс обмена данными с разрешенным к применению веб-сервером, для чего был бы определен порт отправителя 1030, то маршрутизатор R2 обеспечил бы доступ для входящих пакетов из Интернета, при условии, что они имеют следующие характеристики: IP-адрес отправителя — 64.100.2.2, IP-адрес получателя — 128.107.1.1, порт отправителя — 80, порт получателя — 1030. В результате этого разрешается передача через маршрутизатор только пакетов, относящихся к этому разрешенному сеансу, а пакеты, отправленные злоумышленником, отбрасываются.

Для применения рефлексивных списков управления доступом требуется некоторая дополнительная настройка конфигурации, а также использование в конфигурации именованного расширенного списка управления доступом.

Динамические списки управления доступом

Динамические списки управления доступом позволяют решать различные проблемы, которые также требуют больших усилий при попытке решить их с помощью традиционных списков управления доступом. Предположим, необходимо обеспечить для небольшого коллектива пользователей доступ к ряду серверов. Списки управления доступом позволяют сопоставлять с критериями IP-адреса хостов, применяемых пользователями. Но если пользователь садится за другой персональный компьютер, или на время получает новый адрес с помощью протокола DHCP, или

относит свой ноутбук домой и так далее, то, оставаясь санкционированным пользователем, он приобретает другой IP-адрес. В связи с этим традиционный список управления доступом должен быть отредактирован для поддержки каждого нового IP-адреса. Со временем сопровождение списка управления доступом, предусматривающее проверку всех подобных IP-адресов, становится все более трудоемким. Кроме того, применение традиционного списка управления доступом становится предпосылкой для появления брешей в защите, поскольку в каждый конкретный момент применяются не все заданные IP-адреса, поэтому некоторые из неиспользуемых IP-адресов могут вводить в действие пользователи других хостов.

Динамические списки управления доступом, называемые также средством обеспечения безопасности по принципу замка и ключа, позволяют решить эту проблему, связывая применение списка управления доступом с процессом аутентификации пользователя. Но в этом случае пользователей необходимо проинструктировать, чтобы они начинали свою работу не с попытки подключения к серверу, а с установления сеанса связи по протоколу Telnet с маршрутизатором. Маршрутизатор передает приглашение к вводу комбинации имени пользователя и пароля. Если подлинность пользователя подтверждается, маршрутизатор динамически изменяет свой список управления доступом, разрешая прохождение трафика от хоста с IP-адресом, с помощью которого были только что отправлены пакеты аутентификации. А по истечении определенного времени простоя маршрутизатор удаляет динамическую запись из списка управления доступом, закрывая потенциальную брешь в защите. Реализация этой идеи демонстрируется на рис. 8.12.

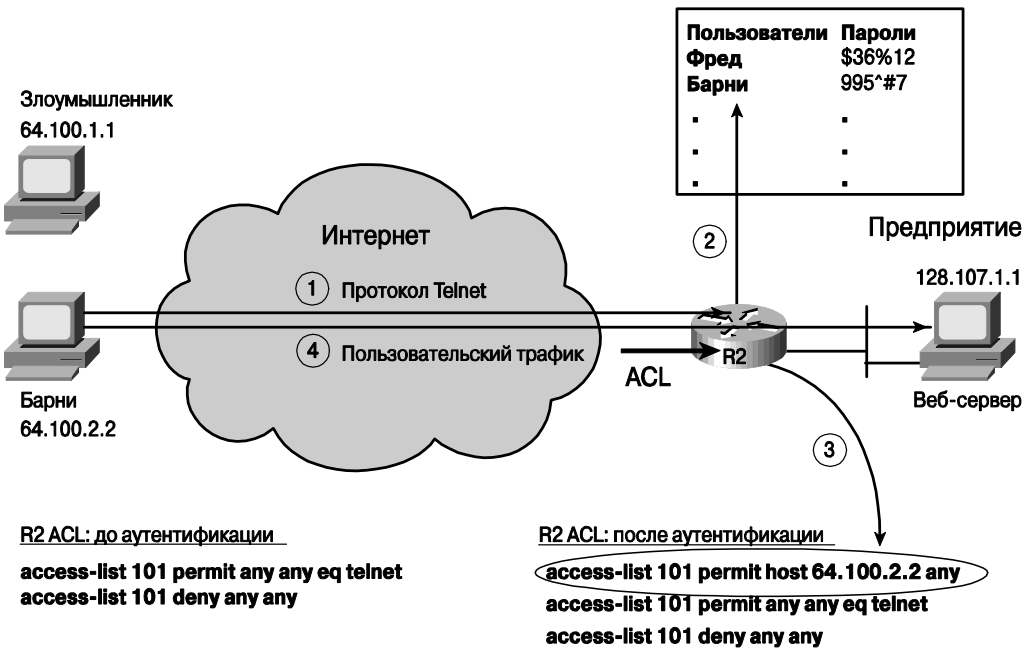

Рис. 8.12. Применение динамических списков управления доступом

Процесс, показанный на рис. 8.12, начинается с того, что маршрутизатор запрещает весь трафик, кроме поступающего по протоколу Telnet. (Безусловно, на рис. 8.12 показан список управления доступом, который позволяет подключение по этому протоколу к любому IP-адресу, но на практике необходимо разрешить прохождение трафика Telnet только по IP-адресу маршрутизатора.) Для активизации этого процесса необходимо выполнить описанные ниже действия.

Этап 1 Пользователь подключается к маршрутизатору с помощью протокола Telnet

Этап 2 Пользователь указывает имя пользователя и пароль, после чего маршрутизатор сравнивает эти значения со списком, подтверждая подлинность пользователя

Этап 3 После аутентификации маршрутизатор динамически добавляет запись в начало списка управления доступом, разрешая прохождение трафика, отправителем которого является хост, прошедший проверку подлинности

Этап 4 Пакеты, передаваемые с хоста, получившего разрешение, проходят через маршрутизатор на сервер.

Списки управления доступом, контролируемые по времени

Под списками управления доступом, контролируемыми по времени, подразумеваются обычные списки управления доступом IP (и нумерованные, и именованные), которые имеют одну особенность: они позволяют добавлять ограничения по времени в команды конфигурации. В некоторых случаях может потребоваться проверка пакетов с учетом критериев в списке управления доступом, но только в определенное время дня или даже в определенные дни недели. В списках управления доступом, контролируемых по времени, предусмотрена возможность добавлять временные ограничения, в связи с чем система IOS вводит или удаляет оператор из списка управления доступом после того, как наступает установленное время.

Подготовка к экзамену

Повторите все ключевые темы

Повторите все ключевые темы данной главы, отмеченные пиктограммой "Ключевая тема". Ключевые темы и соответствующие им страницы перечислены в табл. 8.7.

Таблица 8.7. Ключевые темы главы 8

Элемент	Описание	Страница
Рис. 8.3	Синтаксис расширенных списков ACL с необходимыми полями	319
Параграф	Важнейшая особенность логики расширенных списков ACL	320
Рис. 8.5	Расширенный синтаксис команд ACL с номерами портов при использовании протокола TCP или UDP	321
Рис. 8.7	Фильтрация пакетов по данным о номере порта отправителя	322
Список	Советы и рекомендации по проверке портов TCP и UDP с использованием списков ACL	324
Список	Различия между именованными и нумерованными списками ACL	328
Список	Средства, предоставляемые операционной системой IOS 12.3 порядковым номерам ACL	331
Список	Рекомендации по реализации списков ACL	335

Дополнительные сценарии на компакт-диске

В приложении на компакт-диске содержатся пять подробных сценариев, которые позволяют не только проанализировать различные проекты, проблемы и вывод команд, но и ознакомиться с тем, как связаны понятия, рассматриваемые в нескольких главах. Сценарий 3 посвящен спискам управления доступом и содержит практические задания по выбору шаблонов масок.

Ключевые термины

Дайте определения перечисленным ниже терминам и проверьте правильность их написания в словаре терминов:

расширенный список управления доступом (extended access list), именованный список управления доступом (named access list), динамический список управления доступом (dynamic ACL), рефлексивный список управления доступом (reflexive ACL)

Ключевые команды

Хотя информацию в табл. 8.8 и 8.9 не обязательно запоминать на память, в них приведен краткий список конфигурационных команд и команд EXEC, рассматривавшихся в данной главе.

Таблица 8.8. Конфигурационные команды главы 8

Команда	Описание
`access-list` *номер* {deny | permit} *протокол отправитель шаблон_маски-отправителя получатель шаблон_маски-получателя* [log]	Глобальная команда для расширенных нумерованных списков управления доступом. Используются номера 100–199 или 2000–2699 включительно
`access-list` *номер* {deny | permit} tcp *отправитель шаблон_маски-отправителя* [*оператор* [*порт*]] *получатель шаблон_маски-получателя* [*оператор* [*порт*]] [log]	Версия команды `access-list` с параметрами, относящимися к протоколу TCP
`access-list` *номер* remark *текст*	Позволяет задать комментарий, который помогает запомнить, для чего предназначен список управления доступом
`ip access-group` {*номер* | *имя* [in | out]}	Команда режима конфигурирования интерфейса, привязывающая к нему список управления доступом
`access-class` *номер* | *имя* [in | out]	Команда режима конфигурирования линий, позволяющая включить стандартные или расширенные списки управления доступом для них
`ip access-list` {standard | extended} *имя*	Глобальная команда, предназначенная для настройки конфигурации именованного стандартного или расширенного списка управления доступом с переходом в режим настройки конфигурации списка управления доступом
{deny | permit} *отправитель* [*шаблон_маски-отправителя*] [log]	Команда режима настройки списка управления доступом, предназначенная для ввода в конфигурацию сведений о правилах проверки и действиях, относящихся к стандартному именованному списку управления доступом
{deny | permit} *протокол отправитель шаблон_маски-отправителя получатель шаблон_маски-получателя* [log]	Команда режима настройки списка управления доступом, предназначенная для ввода в конфигурацию сведений о правилах проверки и действиях, относящихся к расширенному именованному списку управления доступом
{deny | permit} tcp *отправитель шаблон_маски-отправителя* [*оператор* [*порт*]] *получатель шаблон_маски-получателя* [*оператор* [*порт*]] [log]	Команда режима настройки списка управления доступом, предназначенная для ввода в конфигурацию сведений о критериях сопоставления и действиях, относящихся к именованному списку управления доступом, который сопоставляется с сегментами TCP
`remark` *текст*	Команда режима настройки списка управления доступом, предназначенная для ввода в конфигурацию описания именованного списка управления доступом

Таблица 8.9. Команды EXEC главы 8

Команда	Описание
`show ip interface [`*`тип номер`*`]`	Выводит информацию о списках управления доступом, примененных на интерфейсе
`show access-lists [`*`номер-списка	название-списка`*`]`	Показывает сведения о введенных в конфигурацию списках управления доступом для всех протоколов
`show ip access-list [`*`номер-списка	название-списка`*`]`	Показывает сведения о списках управления доступом IP

Ответы на практические задачи главы

В табл. 8.10 содержатся ответы на практические задачи, приведенные в табл. 8.6. Обратите внимание на то, что для любого вопроса, упоминающего клиент, можно выбирать соответствие порту, номер которого больше 1023. Ответы в данной таблице, по большей части, игнорируют эту возможность, но только для демонстрации одного из примеров, в ответе на первую задачу приведен вариант со ссылкой на порт клиента с номером больше 1023 и вариант без нее. Остальные ответы просто опускают эту часть логики.

Таблица 8.10. Создание однострочных расширенных списков ACL. Ответы

	Критерий
1	`access-list 101 permit tcp host 10.1.1.1 10.1.2.0 0.0.0.255 eq www`
	`access-list 101 permit tcp host 10.1.1.1 gt 1023 10.1.2.0 0.0.0.255 eq www`
2	`access-list 102 permit tcp 172.16.4.0 0.0.0.127 172.16.3.0 0.0.0.127 eq telnet`
3	`access-list 103 permit icmp 192.168.7.192 0.0.0.63 192.168.7.8 0.0.0.7`
4	`access-list 104 permit tcp 10.2.2.0 0.0.1.255 eq www 10.4.4.0 0.0.3.255`
5	`access-list 105 permit tcp 172.20.1.0 0.0.0.255 eq 23 172.20.44.0 0.0.1.255`
6	`access-list 106 permit tcp 192.168.99.96 0.0.0.15 192.168.176.0 0.0.0.15 eq www`
7	`access-list 107 permit icmp 10.55.66.0 0.0.0.127 10.66.55.0 0.0.0.63`
8	`access-list 108 permit ip any any`