Государственное образовательное учреждение высшего профессионального образования

«Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Факультет «Информатика и системы управления»

Кафедра «Информационные системы и телекоммуникации»

Методическое указание к лабораторной работе

«Списки контроля доступа»

по курсу

«Учебно-технологическая практика

по инфокоммуникационным системам и сетям»

Составила: Тихомирова Е.А.

Часы: 4 часа

Москва, 2013 г.

Оглавление

Цель работы

1. Изучить функциональные возможности списков контроля доступа;
2. Изучить настройку списков контроля доступа на маршрутизаторах на примере маршрутизаторов фирмы Cisco.

Теоретическая часть

Списки контроля доступа (Access Control List – ACL) позволяют классифицировать пакеты. При задании их на входе и выходе интерфейсов маршрутизатора осуществляется контроль доступа (безопасность) на основе фильтрации пакетов.

Списки контроля доступа представляют набор правил, которые обеспечивают контроль доступа над принимаемыми и отправляемыми пакетами на интерфейсах маршрутизаторов. Список контроля доступа не применяется к пакетам, созданным данным маршрутизатором, только – к проходящему трафику.

ACL работают в следующих режимах:

- Входящие списки контроля доступа;
- Исходящие списки контроля доступа.

Вне зависимости от деления, описанного выше, списки контроля доступа подразделяются на два типа:

- Стандартные;
- Расширенные.

Входящие списки контроля доступа

Входящие списки контроля доступа обрабатывают пакеты перед перенаправлением на исходящий интерфейс маршрутизатора. Достоинством данного подхода является уменьшение затрачиваемых ресурсов на поиск маршрутной информации в случае отклонения трафика в соответствии с правилами применяемого ACL.

Алгоритм работы входящего списка контроля доступа представлен на рис. 1.

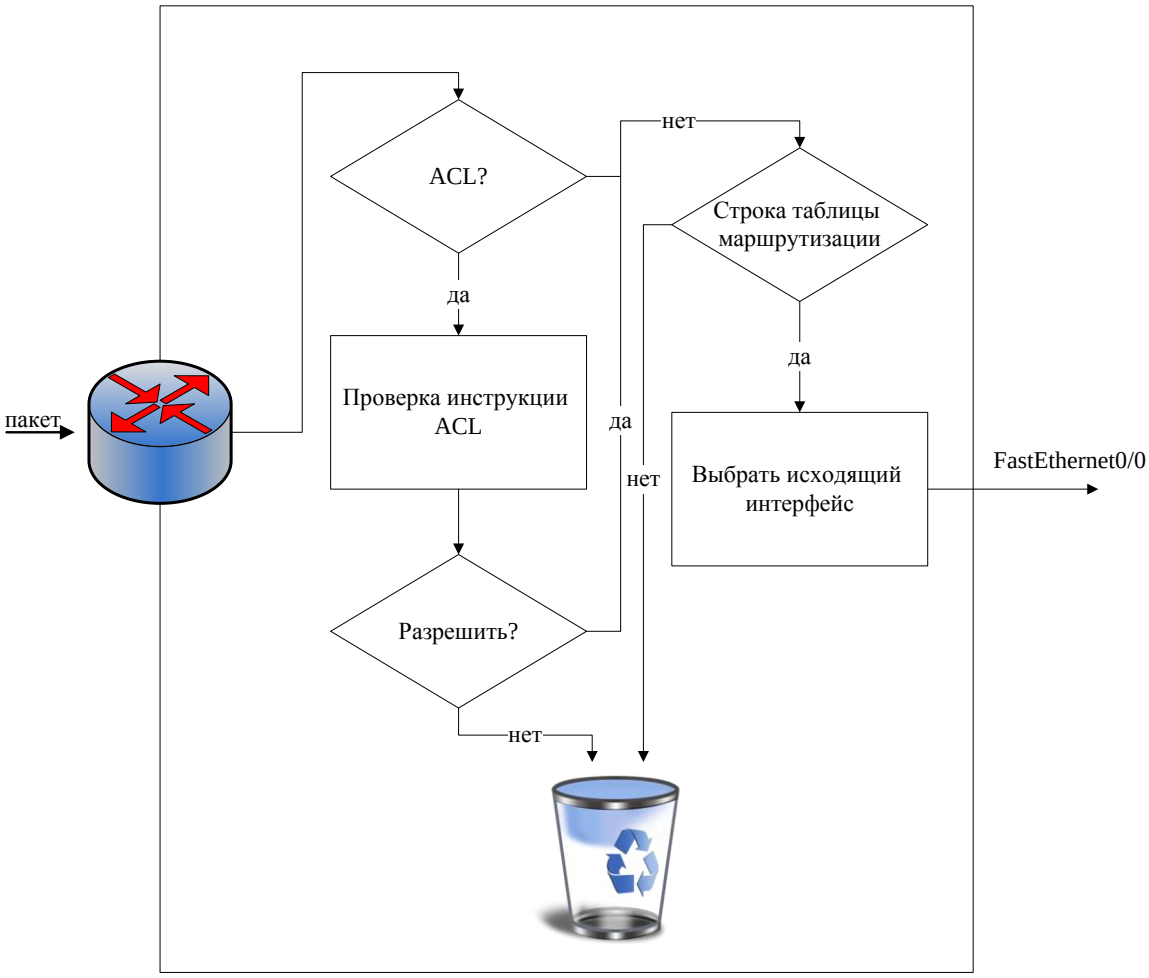

Рис. 1. Алгоритм работы входящего списка контроля доступа.

Исходящие списки контроля доступа

При использовании исходящих списков контроля доступа первоначально определяется исходящий интерфейс пакета в соответствии с маршрутной информацией, после чего пакет проверяется ACL.

Алгоритм работы исходящего списка контроля доступа представлен на рис. 2.

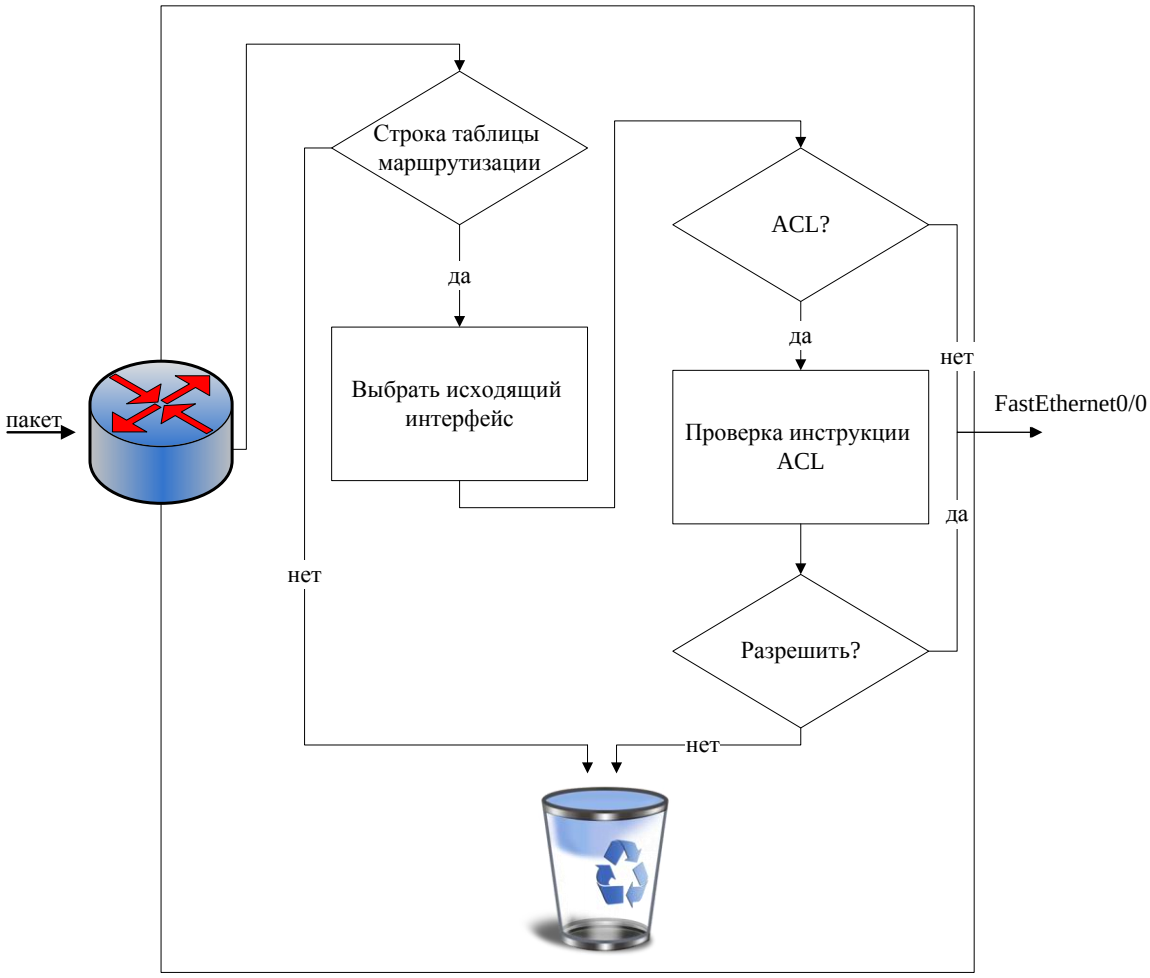

Рис. 2. Алгоритм работы исходящего списка контроля доступа.

Стандартные списки контроля доступа

Стандартные списки контроля доступа на основании IP адреса источника (сети-источника, подсети, хоста) принимают или отклоняют полный пакет протоколов.

Для идентификации стандартного списка контроля доступа списку присваивается номер из следующих диапазонов:

- 1 – 99;
- 1300 – 1999.

Пример стандартного списка контроля доступа:

access-list 1 permit 192.168.1.0 0.0.0.255 – пропускает все пакеты из сети 192.168.1.0, а все остальные запрещает.

Расширенные списки контроля доступа

Расширенные – проверяют адреса источника, назначения, протоколы, номера портов и другие параметры, предоставляя, таким образом, большую гибкость.

Для идентификации расширенного списка контроля доступа списку присваивается номер из следующих диапазонов:

- 100 – 199;
- 2000 – 2699.

Пример расширенного списка контроля доступа:

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 21
access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 20
```

Разрешает ftp-трафик из сети 192.168.1.0 в сеть 192.168.2.0, остальное запрещает.

Шаблонные маски списков контроля доступа

При указании в списке контроля доступа IP-адреса необходимо использовать шаблонную маску, которая укажет, какие именно биты указанного IP-адреса должны совпадать с битами IP-адреса в проверяемом пакете.

Шаблонная маска состоит из 32 бит, 4 октетов. Бит 0 в шаблонной маске означает, что значение соответствующих бит IP-адреса должно совпадать. Бит 1 – значение соответствующих бит IP-адреса не проверяется. Шаблонная маска списков контроля доступа записывается в десятичной системе счисления, по образцу масок IP-подсетей.

Практическая часть

Собрать и настроить топологию, заданную преподавателем. Настройку осуществить в соответствии с данными в табл. 2, 3. В качестве коммутатора использовать модель 2960, в качестве маршрутизатора – 2811.

В качестве среды моделирования использовать Cisco Packet Tracer.

Список необходимых команд приведен в табл. 1.

Конфигурирование списков контроля доступа осуществляется в следующем порядке:

1. создается список контроля доступа с правилами, удовлетворяющими требованиям сети;
2. созданный список контроля доступа устанавливается на входной или выходной интерфейс маршрутизатора.

Таблица 1.

Команды конфигурирования.

Команда	**Описание**
access-list *номер списка доступа* {permit|deny} *source* [*маска*]	Создает стандартный нумерованный список контроля доступа по протоколу IP.
access-list *номер списка контроля доступа* {permit|deny} *источник протокола шаблон источника* [*порт оператора*] *место*	Создает расширенный нумерованный список контроля доступа.

назначения шаблон места назначения [*порт оператора*]	
ip access-group *номер списка* доступа {in|out}	Включает список контроля доступа по протоколу IP на интерфейсе.
show ip access-list	Отображает содержимое всех списков контроля доступа по протоколу IP.

Таблица 2.

Справочные данные.

Параметр конфигурации	**Значение**
enable password	iu3
enable secret password	cisco
пароль линии vty	vty
пароль консольного порта	console

Таблица 3.

Условия заданий.

Адрес первой подсети	**Маска подсети**
192.168.x.0	255.255.255.0

Где x – номер варианта студента.

Контрольные вопросы

1. В чем заключается различие между стандартными и расширенными списками контроля доступа?
2. В чем заключается различие между входящими и исходящими списками контроля доступа?
3. Перечислите назначения списков контроля доступа.
4. Какое правило используется для описания последней инструкции по умолчанию в конце каждого списка контроля доступа?

Литература

1. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822// Издательство: «Вильямс», 2012 – 720 с.
2. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2// Издательство: «Вильямс», 2012 – 736 с.