МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» марта 2016 г.

СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ (ACL)

Методические указания
по выполнению лабораторной работы
для студентов, обучающихся по направлению подготовки
11.03.02 «Инфокоммуникационные технологии и системы связи»
по курсу «Методы и средства моделирования
телекоммуникационных систем и устройств», а также для
студентов других направлений подготовки в области
информационных технологий

Курск 2016

УДК 654:004.7 (075.8)

Составители: преподаватель кафедры И.Г. Бабанин
преподаватель кафедры Н.П. Павлюченков
младший научный сотрудник Т.М. Петрияненко

Рецензент
Кандидат технических наук, старший научный сотрудник,
профессор кафедры А.М. Потапенко

Списки управления доступом (ACL): методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: И.Г.Бабанин, Н.П. Павлюченков, Т.М. Петрияненко. Курск, 2016. 13 с.

Методические указания по выполнению лабораторной работы содержат краткие теоретические сведения о сетевой фильтрации, задания по выполнению работы, а также перечень вопросов для самопроверки изучаемого материала.

Полученные знания в результате выполнения работы дадут возможность сформировать целостную картину информационного взаимодействия в современных сетях, что является фундаментом для изучения остальных дисциплин профессионального цикла учебного плана, а также могут быть использованы в будущей профессиональной деятельности выпускника, связанной с сетевыми технологиями.

Предназначены для студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» по курсу «Методы и средства моделирования телекоммуникационных систем и устройств», а также для студентов других направлений подготовки в области информационных технологий в системе высшего образования.

Текст печатается в авторской редакции

Подписано печать . Формат 60x841/16.
Усл. печ. л.. Уч.-изд. л. 0,8 Тираж 100 экз. Заказ. 240 Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

1 Цель работы

- изучение работы со стандартными и расширенными списками доступа в эмуляторе Cisco Packet Tracer.

2 Краткие теоретические сведения

2.1 Стандартные списки доступа

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, **создаются командами access-list в режиме глобальной конфигурации**, каждый список определяется номером – числом в диапазоне 0 ÷ 99.

Каждая такая **команда добавляет новый критерий отбора в список:**

router(config)#access-list <номер_списка> <{deny|permit}> <IP-адрес> [маска_шаблона].

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона (wildcard) – это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми.

Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.1 0.0.0.254.

Комбинация «адрес – маска шаблона» вида 0.0.0.0 255.255.255.255 (то есть соответствующая всем возможным

адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобрать**) или отрицательное** (отбросить, отказать, игнорировать) **будет принято решение при срабатывании данного критерия отбора.** Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес – маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор allow отбирает трафик в эту категорию, а deny – нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) – он срабатывает, если ни одного соответствия обнаружено не было[1].

Для аннулирования списка доступа следует ввести команду:

router(config)#no access-list <номер_списка>.

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

router(config-if)#ip access-group <номер_списка><{in|out}>.

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно.

Входящими считаются пакеты, поступающие к интерфейсу из сети.

Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один – для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутри одного списка.

В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета [2].

2.2 Расширенные списки доступа

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество параметров и предлагающие более богатые возможности для формирования критериев отбора.

Расширенные списки доступа создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100–199. Пример синтаксиса **команды создания строки расширенного списка для контроля TCP-соединений [2]:**

router(config)#access-list<номер_списка><{deny| permit}> tcp <IP-адрес_источника><маска_шаблона> [оператор порт[порт]]<IP-адрес_получателя> <маска_шаблона> [оператор порт[порт]] [established]

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (меньше), gt (больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется.

Комбинация оператор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя. Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов.

Кроме того, ключевое слово established определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен параметр established, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном

направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

router(config)#access-list 101 permit tcp any 22.22.22.0 0.0.0.255 eq 23 established

router(config)#access-list 101 deny tcp any 22.22.22.0 0.0.0.255 eq 23

router(config)#access-list 101 permit ip any any

router(config)#interface FastEthernet 1/0

router(config-if)#ip access-group 101 in.

Указание ip вместо tcp в команде access-list означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается deny ip any any, поэтому в предыдущем примере мы указали permit ip any any для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Расширенный список с протоколом ip позволяет также производить отбор произвольных пакетов по адресу отправителя и по адресу получателя (в стандартных списках отбор производится только по адресу отравителя).

Критерии для отбора UDP-сообщений составляются аналогично TCP, при этом вместо tcp следует указать udp, а параметр established, конечно, не применим.

Контроль за ICMP-сообщениями может осуществляться с помощью критериев отбора типа:

router(config)#access-list <номер_списка> <{deny|permit}> icmp <IP-адрес_источника> <маска_шаблона> <IP-адрес_назначения> <маска_шаблона> [icmp-тип [icmp-код]].

Здесь icmp-тип и, если требуется уточнение, icmp-код определяют ICMP-сообщение.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора deny/permit надо указать название протокола (ahp, esp, eigrp, gre, icmp, igmp, igrp, ipinip, ospf, tcp, udp) или его номер, которым он кодируется в поле Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды access-list (расширенный) можно указать параметр log, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), **будут протоколироваться на консоль или как указано командой logging.** После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа (с указыванием числа срабатываний каждого критерия):

router#show access-lists.

Более подробную статистику работы списков доступа можно получить, включив режим ip accounting. Режим включается в контексте конфигурирования интерфейса. **Следующая команда включает режим учета случаев нарушения** (то есть, пакетов, которые не были пропущены списком доступа на данном интерфейсе):

router(config-if)#ip accounting access-violations.

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

router#show ip accounting access-violations.

При конфигурировании запрещающих фильтров (в конце которых подразумевается deny all) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе [1].

3 Перечень ресурсов, необходимых для выполнения работы

- персональный компьютер с конфигурацией не ниже Pentium IV, ОЗУ 256 Мб;
- сетевой эмулятор Cisco Packet Tracer.

4 Задание на лабораторную работу

1) Создать стандартный список доступа, разрешающий прохождения сетевых пакетов только для сетей 192.168.20.1/24 и 10.0.0.1/24. Для этого в глобальном контексте конфигурирования необходимо выполнить следующие команды:

router(config)#access-list 1 permit 192.168.20.1 0.0.0.255
router(config)#access-list 1 permit 10.0.0.1 0.0.0.255
router(config)#access-list 1 deny any any.

2) Применить созданный стандартный список доступа на вход одного из интерфейсов межсетевого экрана.

3) С помощью команды ping проверить доступность компьютеров из сетей 192.168.20.1/24 и 10.0.0.1/24.

4) Аннулировать созданный стандартный список доступа.

5) Создать расширенный список доступа, запрещающий установление соединений с помощью протокола HTTP со всеми узлами сети 192.168.20.0 netmask 255.255.255.0 со стороны всех узлов сети «Интернет», но разрешающий установление всех соединений в обратном направлении.

6) Применить созданный расширенный список доступа на вход одного из интерфейсов межсетевого экрана.

7) Проверить работоспособность созданного расширенного списка, подключив к межсетевому экрану две сети с Web-серверами и осуществив к ним поочередно запросы.

8) Просмотреть число срабатываний каждого критерия из созданного списка доступа.

9) Включить учет случаев нарушения списка доступа.

10) Выполнить несколько запросов к Web-серверам.

11) Просмотреть результаты работы команды ping.

12) Вывести на консоль накопленную статистику по учету случаев нарушений.

13) Аннулировать созданный расширенный список доступа.

Примечание: каждая итерация должна сопровождаться скриншотом (-ами).

5 Требования к оформлению отчёта по выполнению лабораторной работы

Отчёт должен быть оформлен с помощью редактора MS Word, версии 97 и выше (.doc, .rtf).

Параметры страницы:

- верхнее поле- 2 см;
- нижнее поле- 2 см;
- левое поле- 3 см;
- правое поле- 1 см;

- переплет- 0 см;
- размер бумаги А4;
- различать колонтитулы первой страницы.

Шрифт текста Times New Roman, 14 пунктов, через 1,5 интервала, выравнивание по ширине, первая строка с отступом 1,5 см. Номер страницы внизу, по центру, 14 пунктов.

Несложные формулы должны быть набраны с клавиатуры и с использованием команды «Вставка→Символ». Сложные формулы должны быть набраны в редакторе MathType 6.0 Equation.

Отчёт по лабораторной работе должен содержать:

- название предмета, номер и название лабораторной работы;
- фамилию и инициалы автора, номер группы;
- фамилию и инициалы преподавателя;
- цель работы;
- перечень используемого оборудования;
- последовательность действий проведения исследований;
- вывод о проделанной работе;
- ответы на вопросы п. 6;
- дату выполнения и личную подпись.

Результаты различных измерений необходимо представить в виде нескольких самостоятельных таблиц и графиков. Каждая таблица и каждый график должны иметь свой заголовок и исходные данные эксперимента.

При выполнении численных расчетов надо записать формулу определяемой величины, сделать соответственную численную подстановку и произвести вычисления.

Пример оформления отчёта представлен в приложении 1.

6 Примерный перечень вопросов для защиты лабораторной работы

1) Что представляют собой списки доступа (access lists)?
2) Какие существуют списки доступа и чем они отличаются друг от друга?
3) Какая команда добавляет новый критерий отбора в стандартный список доступа?
4) Какие операторы определяют положительное или отрицательное решение при срабатывании заданного критерия?

5) Какой командой производится аннулирование списка доступа?

6) Какие пакеты считаются входящими?

7) Какие действие будет производить команда log в конце access lists (расширенный)?

8) Какой командой осуществляется просмотр всех имеющихся списков доступа?

9) Какой командой осуществляется просмотр накопленной статистики?

7 Список использованных источников

1) Андрончик А.Н., Коллеров А.С., Синадский А.С., Щербаков М.Ю. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие; под общ. ред. Синадского Н.И.- Екатеринбург: изд-во Урал. ун-та, 2014. – 180 с.

2) Соболь Б.В., Манин А.А., Герасименко М.С. Сети и телекоммуникации : учеб. пособие. – Ростов н/Д : Феникс, 2015. – 191 с.

Приложение 1
Пример оформления отчёта по лабораторной работе

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра космического приборостроения и систем связи

Отчёт по выполнению лабораторной работы
по курсу «Радиопередающие и радиоприёмные устройства»
на тему «Изучение принципа работы супергетеродинного приёмника»

Выполнил: студент группы ИТ-11б
Иванов И.И.
_____ «___»_____2012
(подпись)

Проверил: д.т.н., профессор кафедры
Петров П.П.
_____ «___»_____2012
(подпись)

Курск 2016

1 Цель работы

Ознакомиться …

2 Структурная схема макета и перечень используемого оборудования

Структурная схема лабораторного макета для проведения исследований спектров сигналов представлена на рисунке 2.1.

Рисунок 2.1 – Структурная схема лабораторного макета

Перечень используемого оборудования:

- лабораторный стенд «Радиоприёмные устройства» (1 к-т);
- сменный блок «Изучение принципа работы супергетеродинного радиоприёмника АМ сигналов» (1 к-т);
- осциллограф типа С1-96 (1 к-т);
- милливольтметр переменного напряжения типа DT-820B (1 к-т).

3 Последовательность проведения и результаты лабораторных исследований

3.1 Снятие амплитудно-частотной характеристики входной цепи

Результаты снятия зависимости напряжения на выходе входной цепи от частоты генератора, при фиксированном напряжении на входе, представлены в таблице 1.

Таблица 1 – АЧХ входной цепи

Частота генератора, кГц				
Напряжение на выходе входной цепи $U_{ВЫХ}$, мВ при $U_{ВХ}$ = 500 мВ				

Продолжение таблицы 1

Нормированное напряжение на выходе входной цепи, $U_{ВЫХ}/ U_{ВЫХ.МАКС.}$				

4 Ответы на контрольные вопросы

Вопрос №1. Какие основные функции радиоприёмных устройств?

Ответ:

Вопрос №2. Перечислите основные электрические характеристики радиоприемников.

Ответ:

5 Вывод о проделанной работе

В ходе выполнения лабораторной работы ознакомился с …