Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Оренбургский государственный университет»

Кафедра управления и информатики в технических системах

А.Л. Коннов

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ И КОМПЛЕКСЫ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 27.03.04 Управление в технических системах

Оренбург
2018

УДК 004.7(07)
ББК 32.973.202я7
К 64

Рецензент – доцент, кандидат технических наук Ю.А. Ушаков

Коннов, А. Л.
К64 Вычислительные сети и комплексы: методические указания / А. Л. Коннов; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2018. – 35 с.

Методические указания содержат теоретический материал, задание и пример выполнения курсовой работы по дисциплине «Вычислительные сети и комплексы».

Предназначены для студентов, обучающихся по направлению подготовки 27.03.04 Управление в технических системах, при изучении дисциплины «Вычислительные сети и комплексы».

УДК 004.7(07)
ББК 32.973.202я7

Содержание

Введение

В соответствии с рабочей программой, целью освоения дисциплины «Вычислительные сети и комплексы» является изучение студентами основных принципов функционирования и методов построения вычислительных сетей и комплексов.

Задачами для освоения дисциплины являются:

– освоение студентами теоретических и практических основ функционирования вычислительных сетей;

– изучение способов проектирования вычислительных сетей и комплексов;

– приобретение студентами навыков проектирования вычислительных сетей;

– приобретение студентами навыков администрирования вычислительных сетей.

Одной из главных задач при проектировании и администрировании вычислительных сетей и комплексов является настройка их безопасного функционирования. Данную задачу невозможно решить без настройки параметров безопасности маршрутизатора и разработки списков контроля доступа для соответствующей вычислительной сети.

Поэтому темой курсовой работы является – «Разработка списков контроля доступа».

Для достижения цели работы необходимо выполнить следующие задачи:

– настроить базовые параметры безопасности маршрутизатора: пароль на доступ к привилегированному режиму, пароль на консольный и удаленный доступ, шифрование паролей в конфигурационном файле;

– разработать и настроить стандартные списки доступа;

– разработать и настроить расширенные списки доступа;

– разработать и настроить именованные списки доступа.

Выполнение данной курсовой работы направлено на формирование следующих компетенций для направления подготовки 27.03.04 Управление в технических системах:

– ОПК-6 способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий;

– ПК-2 способность проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления.

Пояснительная записка к курсовой работе должна быть оформлена в соответствии с требованиями СТО 02069024. 101 – 2015 Работы студенческие (общие требования и правила оформления) и содержать следующие структурные элементы:

– титульный лист;

– задание;

– аннотацию;

– содержание;

– введение;

– основную часть;

– список использованных источников;

– приложения (при необходимости).

1 Задача 1. Настройка базовых параметров безопасности маршрутизатора

Цель – настроить базовые параметры безопасности маршрутизатора такие, как пароль на доступ к привилегированному режиму, пароль на консольный и удаленный доступ, шифрование паролей в конфигурационном файле.

1.1 Основные теоретические положения

В процессе организации межсетевого взаимодействия важное место занимает маршрутизация сообщений между отдельными подсетями [1]. При этом под маршрутизацией понимается процесс доставки сообщения из одной подсети в другую. Данная задача может решаться различными способами. При этом, чем сложнее рассматриваемая система, чем больше подсетей ее образуют, тем более нетривиальным является решение задачи доставки сообщений. Сетевой компонент, выполняющий маршрутизацию пакетов, называется маршрутизатором (router). Маршрутизатор может быть реализован на базе компьютера с несколькими сетевыми интерфейсами, на котором установлено специальное программное обеспечение. В этом случае говорят о программном маршрутизаторе. В другом случае маршрутизатор может быть выполнен в виде отдельного сетевого устройства. Разумеется, наиболее эффективным решением является использование специальных аппаратных маршрутизаторов. В настоящее время лидером на рынке корпоративных маршрутизаторов является компания Cisco, предлагающая высокопроизводительные и надежные устройства. В небольших сетях (таких как сеть небольшого офиса или домашняя сеть) использование аппаратного маршрутизатора может быть экономически невыгодно.

Различают два режима работы маршрутизатора: непривилегированный и привилегированный. Первый режим предназначен только для просмотра настроек маршрутизатора, изменить которые в данном режиме работы нельзя. Во втором

режиме администратор получает возможность использовать и настраивать все возможные протоколы и технологии, которыми обладает конкретный маршрутизатор. Для доступа к этому режиму обязательно должен быть установлен пароль, иначе возможен несанкционированный доступ к маршрутизатору.

Возможны следующие виды подключений к маршрутизатору:

– консольное, используя специальный консольный порт;

– удаленное, используется после предварительной настройки маршрутизатора.

Данные подключения тоже должны быть защищены паролями от несанкционированного доступа.

Также в целях безопасности имеется возможность зашифровать все пароли в конфигурационном файле маршрутизатора.

В качестве основных параметров безопасности маршрутизатора выступают защищенный доступ к привилегированному режиму работы маршрутизатора, защищенный доступ на маршрутизатор через консольный порт, защищиенный удаленный доступ на маршрутизатор.

1.2 Задание и пример выполнения

Для настройки базовых параметров безопасности маршрутизатора необходимо использовать программу Cisco Packet Tracer. Эта программа становится доступной для скачивания после регистрации на сайте netacad.com в разделе «Вводный курс по Packet Tracer» по ссылке https://www.netacad.com/documents/301287/657402203/Packet+Tracer+7.2+for+Windows+64+bit.zip/f1b42d6e-1c30-4134-986c-e40111634152?version=1.0. Сеть для настройки представлена на рисунке 1.1. На этом рисунке PC0-PC-3 выполняют функции персональных компьютеров, Switch0-Switch3 выполняют функции коммутаторов, а Router0-Router3 выполняют функции маршрутизаторов.

Необходимо перейти в настройки центрального маршрутизатора Router0 на вкладку CLI и осуществить настройку защищенного доступа для маршрутизатора, введя следующие команды (таблица 1).

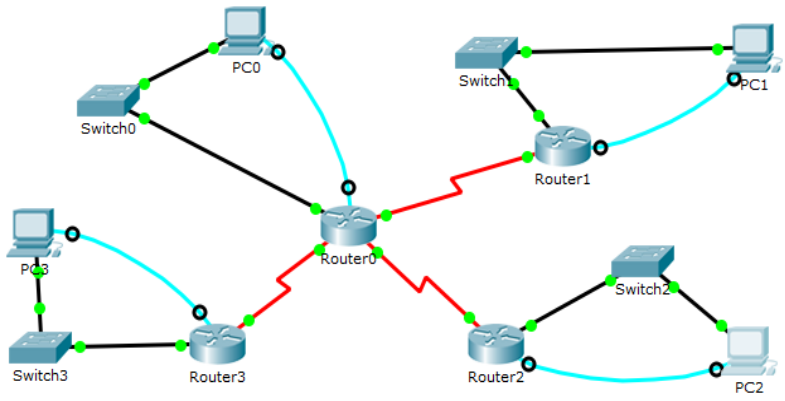

Рисунок 1.1 – Схема сети

Таблица 1 – Команды настройки защищенного доступа на маршрутизатор

Команда	Назначение
enable	Переход в привилегированный режим работы маршрутизатора
conf term	Переход в режим настроек или режим глобального конфига
enable password cisco	Установка пароля «cisco» для доступа к привилегированному режиму маршрутизатора
enable secret class	Установка пароля «class» для для доступа к привилегированному режиму маршрутизатора
lincon 0	Переход в режим настройки консольного доступа на маршрутизатор
password console	Установка пароля «console» консольного доступа на маршрутизатор
login	Инициализация запроса пароля для доступа на маршрутизатор через консоль
lin vty 0 15	Переход в режим настройки удаленного доступа на маршрутизатор
password class	Установка пароля «class» для удаленного доступа на маршрутизатор
login	Инициализация запроса пароля для удаленного доступа на маршрутизатор
service password-encryption	Шифрование паролей в конфигурационном файле
wr mem	Сохранение настроек

Проверка работоспособности осуществляется через окно PC – Desktop– Comand Promt (рисунок 1.2).

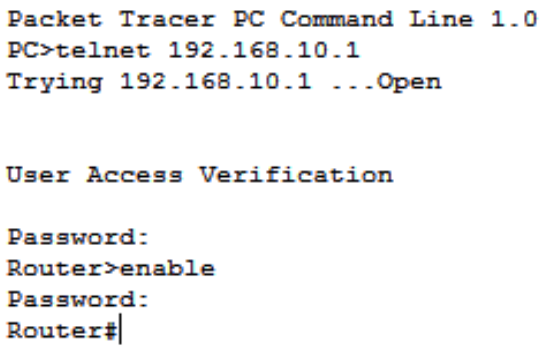

Рисунок 1.2 – Проверка работоспособности

Остальные маршрутизаторы Router1, Router2 и Router3 настраиваются аналогично. В качестве пароля на доступ к привилегированному режиму использовать номер зачетной книжки. Пароль на доступ к консоли и удаленный доступ должен содержать номер зачетной книжки в обратном порядке.

1.3 Контрольные вопросы

1. Дайте понятие маршрутизации в сетях передачи данных.
2. Какое устройство выполняет функции маршрутизации в сетях передачи данных ?
3. Дайте понятие программного и аппаратного маршрутизатора.
4. Какие режимы работы маршрутизатора используются ?
5. Какая команда используется для доступа к привилегированному режиму работы маршрутизатора ?
6. Какая команда используется для перехода к режиму настроек ?
7. Какая команда используется для установки пароля доступа к привилегированному режиму работы маршрутизатора ?
8. Какая команда используется для установки пароля доступа к маршрутизатору через консольное подключение ?

9. Какая команда используется для установки пароля доступа к маршрутизатору через удаленное подключение ?

10. Какая команда используется для шифрования паролей в конфигурационном файле ?

2 Задача 2. Разработка и настройка стандартных списков контроля доступа

Цель – изучить теоретические положения, связанные со стандартными списками контроля доступа, разработать и настроить стандартные списки контроля доступа.

2.1 Основные теоретические положения

Списки контроля доступа (Access Control List, ACL) – предназначены для фильтрации трафика в сетях передачи данных. Различают стандартные и расширенные списки контроля доступа.

Стандартные списки контроля доступа имеют следующий формат:

Access-list <Номер> <Условие> <IP адрес и маска подсети источника трафика>. Стандартные списки нумеруются от одного до 99. В качестве условия могут быть разрешение (permit), запрет (deny) или комментарий (remark).

Особенностью стандартных списков является то, что в них указывается только источник и не указывается приемник трафика, поэтому данный тип списков необходимо размещать как можно ближе к назначению или приемнику трафика. После разработки списка необходимо применить его для фильтрации трафика на выбранном интерфейсе маршрутизатора в необходимом направлении. Для этого используется команда ip access-group <Номер списка> <направление>. В поле номер указывается номер списка, а в поле направление указывается входящее (in) или исходящее направление (out).

2.2 Задание и пример выполнения

На маршрутизаторе R2 необходимо разработать стандартный список контроля доступа, который бы запрещал доступ к сети 192.168.20.0/24 от сети 192.168.11.0/24.

Данный список будет иметь следующий вид: access-list 1 deny 192.168.11.0 0.0.0.255.

На маршрутизаторе R3 необходимо разработать стандартный список контроля доступа, который устанавливает запрет доступа к сети 192.168.30.0/24 от сети 192.168.10.0/24.

Данный список будет иметь следующий вид: access-list 1 deny 192.168.10.0 0.0.0.255.

Настройка списков осуществляется для сети, представленной на рисунке 2.1.

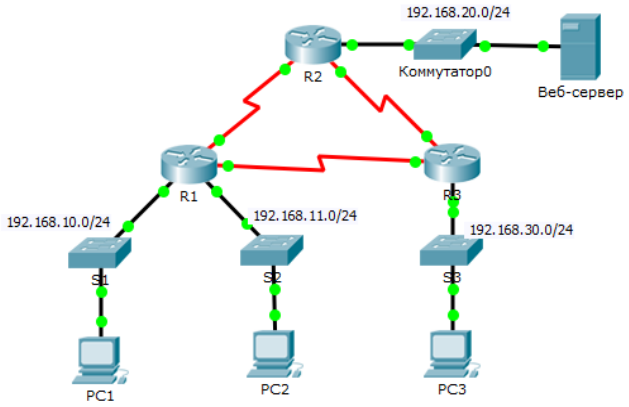

Рисунок 2.1 – Настраиваемая сеть

На этом рисунке PC1-PC-3 выполняют функции персональных компьютеров, S1-S3 и Коммутатор0 выполняют функции коммутаторов, R1-R3 выполняют функции маршрутизаторов, а Веб-сервер выполняет функцию веб-сервера.

Перед применением ACL-списков проверяем наличие полного подключения. Для этого отправляем эхо-запросы с ПК на другие устройства. Они были успешны. Пример эхо-запроса показан на рисунке 2.2.

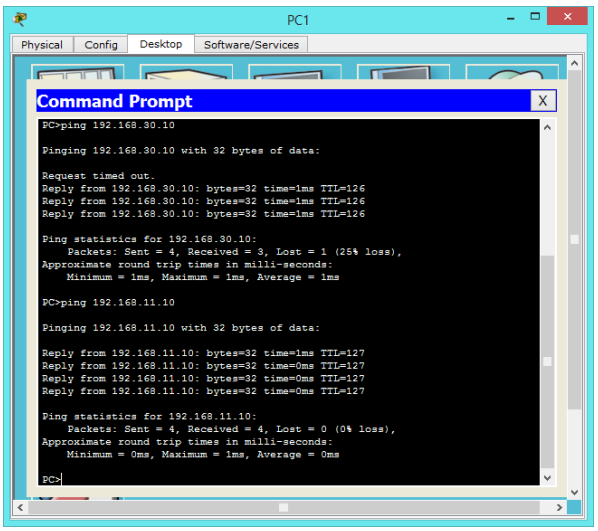

Рисунок 2.2 – Пример эхо-запроса

Далее настраиваем и применяем нумерованный стандартный ACL-список на маршрутизаторе R2. Для этого вводим команды, представленные в таблице 2.1.

Таблица 2.1 – Настройка и размещение стандартного списка на маршрутизаторе R2

Команда	Назначение
enable	Переход в привилегированный режим
conf term	Переход в режим настроек
access-list 1 deny 192.168.11.0 0.0.0.255	Устанавливает запрет доступа к сети 192.168.20.0/24 от сети 192.168.11.0/24
access-list 1 permit any	Разрешает остальной трафик
Interface GigabitEthernet 0/0	Переход в режим настройки интерфейса
Ip access-group 1 out	Размещение списка для фильтрации исходящего трафика

Далее настраиваем и применяем нумерованный стандартный ACL-список на маршрутизаторе R3. Для этого вводим следующие команды, представленные в таблице 2.2.

Таблица 2.2 – Настройка стандартного списка на маршрутизаторе R3

Команда	Назначение
enable	Переход в привилегированный режим работы маршрутизатора
conf term	Переход в режим настроек или режим глобального конфига
access-list 1 deny 192.168.10.0 0.0.0.255	Устанавливает запрет доступа к сети 192.168.30.0/24 от сети 192.168.10.0/24
access-list 1 permit any	Разрешает остальной трафик
Interface GigabitEthernet 0/0	Переход в режим настройки инфтерфейса GigabitEthernet 0/0
Ip access-group 1 out	Размещение списка для фильтрации исходящего трафика

Проверка конфигураций ACL-списков осуществляется командой show access-lists. Результат представлен на рисунке 2.3.

```
R2(config)#do sh access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any
R3(config)#do sh access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

Рисунок 2.3 – Проверка конфигурации списков

Для проверки реализаций ACL-списков были отправлены эхо-запросы. Эхо-запрос от 192.168.10.10 к 192.168.11.10 прошёл успешно (рисунок 2.4), эхо-запрос от 192.168.10.10 к 192.168.20.254 прошёл успешно (рисунок 2.4), сбой эхо-запроса от 192.168.11.10 к 192.168.20.254 (рисунок 2.5), сбой эхо-запроса от 192.168.10.10 к 192.168.30.10 (рисунок 2.5), эхо-запрос от 192.168.11.10 к 192.168.30.10 прошёл успешно (рисунок 2.6), эхо-запрос от 192.168.30.10 к 192.168.20.254 прошёл успешно (рисунок 2.6).

```
PC>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=0ms TTL=127
Reply from 192.168.11.10: bytes=32 time=0ms TTL=127
Reply from 192.168.11.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Рисунок 2.4 – Эхо-запрос от 192.168.10.10

```
PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 2.5 – Сбои эхо-запросов

```
PC>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Рисунок 2.6 – Успешные эхо-запросы

Варианты заданий отличаются номерами сетей Коммутатора0 и коммутаторов S1-S3 на рисунке 2.1. Адрес сети Коммутатора0 должен быть выбран в виде 192.168.XX.0/24, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора S1 больше адреса сети Коммутатора0 на 10. Адрес сети коммутатора S2 больше адреса сети Коммутатора0 на 15. Адрес сети коммутатора S3 больше адреса сети Коммутатора0 на 20.

2.3 Контрольные вопросы

1. Дайте понятие списка контроля доступа.
2. Какие типы списков контроля доступа существуют ?
3. Опишите формат стандартного списка контроля доступа.
4. Какие особенности имеют стандартные списки контроля доступа ?
5. Где размещаются стандартные списки контроля доступа ?
6. Какая команда используется для размещения стандартного списка на выбранном интерфейсе маршрутизатора в нужном направлении ?

7. Какая команда используется для перехода в режим настройки выбранного интерфейса маршрутизатора ?

8. Какая команда используется для создания стандартного списка контроля доступа, запрещающего сети 192.168.10.0/24 доступ к сети 192.168.20.0/24 ?

9. Какая команда используется для создания стандартного списка контроля доступа, разрешающего сети 192.168.10.0/24 доступ к сети 192.168.20.0/24 ?

10. Какая команда используется для разрешения всего остального трафика в стандартном списке контроля доступа ?

3 Задача 3. Разработка и настройка расширенных списков контроля доступа

Цель – изучить теоретические положения, связанные с расширенными списками контроля доступа, разработать и настроить расширенные списки контроля доступа.

3.1 Основные теоретические положения

Расширенные списки контроля доступа имеют следующий формат: Access-list <Номер> <Условие> <Протокол> <IP адрес и маска подсети источника трафика> < IP адрес и маска подсети приемника трафика > <условие выбора порта> <номер порта или имя приложения>.

Расширенные списки нумеруются от 100 до 199. В качестве условия могут быть разрешение (permit), запрет (deny) или комментарий (remark). В поле <протокол> указывается протокол, по которому нужно фильтровать трафик (ip, tcp, udp и др). В полях <IP адрес и маска подсети источника трафика> и < IP адрес и маска подсети приемника трафика> указываются соответственно IP адрес и маска подсети источника и приемника трафика. В поле <условие выбора порта> указывается условие выбора порта (eq, neg, gt ,lt, range). В поле <номер порта или

имя приложения> указывается соответственно номер порта или имя приложения, трафик которого будет фильтроваться данным списком.

Особенностью расширенных списков является то, что в них указывается как источник, так и приемник трафика, поэтому данный тип списков необходимо размещать как можно ближе к источнику трафика, чтобы ненужный трафик не ходил по сети.

После разработки списка необходимо применить его для фильтрации трафика на выбранном интерфейсе маршрутизатора в необходимом направлении. Для этого используется команда ip access-group <Номер списка> <направление>. В поле номер указывается номер списка, а в поле направление указывается входящее (in) или исходящее направление (out).

3.2 Задание и пример выполнения

Работнику предприятия требуется доступ к службам, предоставляемым сервером. Компьютеру PC1 требуется доступ только по протоколу FTP. Компьютер PC1 может отправлять эхо-запросы серверу, но не компьютеру PC2. Схема сети представлена на рисунке 3.1. На этом рисунке S1-S3 выполняют функции коммутаторов, R1 выполняет функции маршрутизатора.

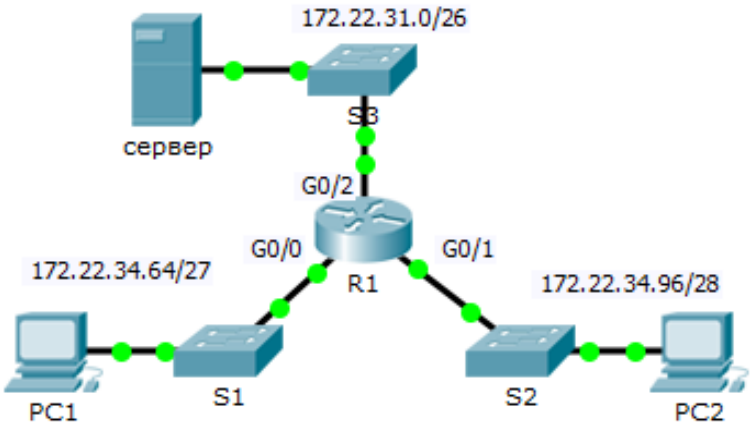

Рисунок 3.1 – Схема сети

3.2.1 Разработка, настройка и проверка расширенного нумерованного ACL-списка №1

Для настройки ACL-списка на разрешение FTP используем следующую команду: access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp. Данная команда задает правило в списке доступа, разрешающее передачу трафика FTP от сети 172.22.34.64/27 на сервер Server.

Для настройки ACL-списка на разрешение ICMP используем следующую команду: access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62. Данная команда задает правило в списке доступа, разрешающее передачу трафика ICMP от сети 172.22.34.64/27 на сервер Server. Остальной трафик запрещён по умолчанию.

Для размещения списка с номером 101 на интерфейсе gigabitEthernet 0/0 во входящем направлении используем команды interface gigabitEthernet 0/0 и ip access-group 100 in.

Для проверки работы примененного списка отправляем эхо-запрос от PC1 на сервер Server (рисунок 3.2). Далее выполняется FTP-подключение от PC1 к серверу Server (рисунок 3.3). Затем отправляется эхо-запрос от PC1 на PC2. Узел назначения должен быть недоступен, поскольку отсутствует явное разрешение трафика (рисунок 3.2).

```
PC>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.2 – Эхо-запросы от PC1 к Serveri PC2

```
PC>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
```

Рисунок 3.3 – FTP-подключение от PC1 к серверу Server

Варианты заданий отличаются адресами сетей коммутаторов S1-S3 на рисунке 3.1. Адрес сети коммутатора S1 должен быть выбран в виде 172.22.XX.64/27, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора S2 должен быть выбран в виде 172.22.XX.96/28, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора S3 должен быть выбран в виде 172.22.XX-1.0/26, где XX две последние цифры номера зачетной книжки.

3.2.2 Разработка, настройка и проверка расширенного нумерованного ACL-списка №2

Устройствам в одной сети разрешается удалённый доступ к устройствам другой сети через протокол Telnet. За исключением ICMP, весь трафик от других сетей запрещён. Схема сети представлена на рисунке 3.4. На этом рисунке PCA и PCB выполняют функции персональных компьютеров, SWA, SWB и SWC выполняют функции коммутаторов, а RTA выполняет функции маршрутизатора.

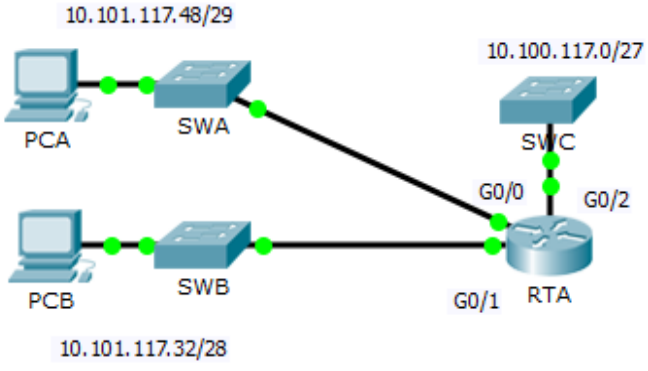

Рисунок 3.4 – Схема сети

Настраиваем расширенный нумерованный ACL-список при помощи следующей команды: access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq telnet. Данная команда разрешает трафик по протоколу Telnet от сети 10.101.117.32/28 до сети 10.100.117.0/27.

Далее выполняем следующую команду: access-list 199 permit icmp any any. Данная команда разрешает трафик по протоколу ICMP от любого устройства и в любом направлении. Остальной трафик будет запрещён по умолчанию.

Для размещения списка с номером 199 на интерфейсе gigabitEthernet 0/2 в исходящем направлении используем команды interface gigabitEthernet 0/2 и ip access-group 199 out.

Для проверки работы расширенного списка сначала необходимо отправить эхо-запросы от компьютера PCB на все остальные IP-адреса в сети (рисунок 3.5). Далее отправляются эхо-запросы от компьютера PCA на все остальные IP-адреса в сети (рисунок 3.6).

```
PC>ping 10.101.117.51

Pinging 10.101.117.51 with 32 bytes of data:

Reply from 10.101.117.51: bytes=32 time=0ms TTL=127
Reply from 10.101.117.51: bytes=32 time=0ms TTL=127
Reply from 10.101.117.51: bytes=32 time=0ms TTL=127
Reply from 10.101.117.51: bytes=32 time=0ms TTL=127

Ping statistics for 10.101.117.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.5 – Эхо-запрос от PCB

Варианты заданий отличаются адресами сетей коммутаторов SWA, SWB и SWC на рисунке 3.4. Адрес сети коммутатора SWA должен быть выбран в виде 10.101.XX.48/29, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора SWB должен быть выбран в виде 10.101.XX.32/28, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора SWC должен

быть выбран в виде 10.100.XX.0/27, где XX две последние цифры номера зачетной книжки.

```
PC>ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time=0ms TTL=127
Reply from 10.101.117.35: bytes=32 time=0ms TTL=127
Reply from 10.101.117.35: bytes=32 time=0ms TTL=127
Reply from 10.101.117.35: bytes=32 time=0ms TTL=127

Ping statistics for 10.101.117.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.6 – Эхо-запрос от PCA

3.3 Контрольные вопросы

1. Опишите формат расширенного списка контроля доступа.

2. Какие особенности имеют расширенные списки контроля доступа ?

3. Где размещаются расширенные списки контроля доступа ?

4. Какая команда используется для размещения расширенного списка на выбранном интерфейсе маршрутизатора в нужном направлении ?

5. Какая команда используется для перехода в режим настройки выбранного интерфейса маршрутизатора?

6. Какая команда используется для создания расширенного списка контроля доступа, разрешающего сети 172.22.34.64/27 доступ к узлу 172.22.34.62 по протоколу ftp ?

7. Какая команда используется для создания расширенного списка контроля доступа, запрещающего узлу 172.22.34.62 доступ к сети 172.22.34.64/27 по протоколу http ?

8. Какая команда используется для разрешения всего остального трафика в расширенном списке контроля доступа ?

9. Какая команда используется для создания расширенного списка контроля доступа, запрещающего любым узлам и сетям доступ к сети 172.22.34.64/27 по протоколу http ?

10. Какая команда используется для создания расширенного списка контроля доступа, разрешающего сети 172.22.34.64/27 доступ к любым узлам и сетям по протоколу telnet ?

4 Задача 4. Разработка и настройка именованных списков контроля доступа

Цель – изучить теоретические положения, связанные с именованными списками контроля доступа, разработать и настроить стандартные и расширенные именованные списки контроля доступа.

4.1 Основные теоретические положения

Именованные списки контроля доступа бывают как стандартными, так и расширенными. Стандартные именованные списки имеют следующий формат: ip access-list standard <Имя>.

В качестве имени может быть использована последовательность символов, несущая смысловую нагрузку. Далее идут правила списка в следующем формате: <условие> <IP адрес и маска источника трафика>.

В поле условие могут быть разрешение (permit), запрет (deny) или комментарий (remark). Далее указывается IP адрес и маска источника трафика, которым может быть как узел, так и целая сеть узлов.

После разработки списка необходимо применить его для фильтрации трафика на выбранном интерфейсе маршрутизатора в необходимом направлении. Для этого используется команда ip access-group <Имя списка> <направление>. В поле номер

указывается имя списка, а в поле направление указывается входящее (in) или исходящее направление (out).

Расширенные списки контроля доступа имеют следующий формат: ip access-list extended <Имя>.

В качестве имени может быть использована последовательность символов, несущая смысловую нагрузку. Далее идут правила списка в следующем формате: <Условие> <Протокол> <IP адрес и маска источника трафика> < IP адрес и маска приемника трафика > <условие выбора порта> <номер порта или имя приложения>.

В качестве условия могут быть разрешение (permit), запрет (deny) или комментарий (remark). В поле <протокол> указывается протокол, по которому нужно фильтровать трафик (ip, tcp, udp). В полях <IP адрес и маска источника трафика> и < IP адрес и маска приемника трафика> указываются соответственно IP адрес и маска источника и приемника трафика. В поле <условие выбора порта> указывается условие выбора порта (eq, neg, gt, lt, range). В поле <номер порта или имя приложения> указывается соответственно номер порта или имя приложения, трафик которого будет фильтроваться данным списком.

После разработки списка необходимо применить его для фильтрации трафика на выбранном интерфейсе маршрутизатора в необходимом направлении. Для этого используется команда ip access-group <Имя списка> <направление>. В поле имя указывается имя списка, а в поле направление указывается входящее (in) или исходящее направление (out).

4.2 Задание и пример выполнения

4.2.1 Разработка, настройка и проверка стандартного именованного ACL-списка

Разработка, настройка и проверка стандартного именованного ACL-списка осуществляется в сети, представленной на рисунке 4.1.

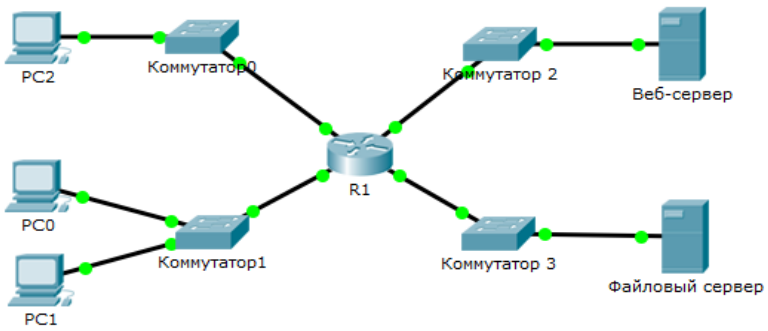

Рисунок 4.1 – Схема настраиваемой сети

На этом рисунке PC0-PC2 выполняют функции персональных компьютеров, Коммутатор0-Коммутатороз выполняют функции коммутаторов, R1 выполняет функции маршрутизатора, а Веб-сервер и Файловый сервер выполняют соответствующие одноименные функции.

Необходимо разработать стандартный именованный ACL-список для предотвращения доступа к файловому серверу. Доступ должен быть запрещён всем клиентам одной сети и конкретной рабочей станции другой сети.

Перед настройкой и применением ACL-списка необходимо проверить подключение. Для этого со всех рабочих станций отправляют эхо-запросы к веб-серверу и файловому серверу. Они должны быть успешны. Пример запросов от второй рабочей станции – на рисунке 4.2.

```
PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=7ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms
```

Рисунок 4.2 – Проверка подключения

Для создания и применения стандартного именованного ACL-списка вводим следующую команду: ip access-list standard File_Server_Restrictions. Данная команда создает стандартный именованный список контроля доступа с именем File_Server_Restrictions.

Для разрешения узлу 192.168.20.4 передавать данные вводим команду permit host 192.168.20.4 и deny any.

Для применения разработанного списка доступа на интерфейсе fastethernet0/1 вводим команды interface fastethernet0/1 и ip access-group File_Server_Restrictions out.

Для проверки конфигурации ACL-списка используется команда show access-lists (рисунок 4.3).

```
R1(config)#do sh access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4
    20 deny any
```

Рисунок 4.3 – Проверка конфигурации

Для проверки правильности работы ACL-списка отправляются эхо-запросы. Все три рабочие станции должны иметь возможность отправлять эхо-запросы на Веб-сервер, но только компьютеру PC1 должно быть разрешено отправлять эхо-запросы на файловому серверу. Соответствующие запросы представлены на рисунках 4.4 – 4.6.

Варианты заданий отличаются номерами сетей коммутаторов на рисунке 4.1. Адрес сети Коммутатора0 должен быть выбран в виде 192.168.XX.0/24, где XX две последние цифры номера зачетной книжки. Адрес сети коммутатора Коммутатор1 больше адреса сети Коммутатора0 на 10. Адрес сети Коммутатора2 больше адреса сети Коммутатора0 на 15. Адрес сети Коммутатора3 больше адреса сети Коммутатора0 на 20.

```
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=14ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 4.4 – Эхо-запросы от PC0

```
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=7ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127
Reply from 192.168.200.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 4.5 – Эхо-запросы от PC1

```
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127
Reply from 192.168.100.100: bytes=32 time=2ms TTL=127
Reply from 192.168.100.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

PC>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 4.6 – Эхо-запросы от PC2

4.2.2 Разработка, настройка и проверка расширенного именованного ACL-списка №1

Работнику предприятия требуется доступ к службам, предоставляемым сервером. Компьютеру PC2 нужен только веб-доступ. PC1 и PC2 могут отправлять эхо-запросы серверу, но не друг другу. Схема сети представлена на рисунке 3.1.

Необходимо разработать расширенный именованный ACL-список для того чтобы узлы сети 172.22.34.96/28 могли отправлять запросы по протоколам HTTP и ICMP на сервер, но не по протоколу FTP.

При помощи команды ip access-list extended HTTP_ONLY создаем расширенный список доступа.

Далее необходимо прописать правила фильтрации трафика при помощи следующей команды: permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www. По данному правилу будет разрешен трафик www от сети 172.22.34.96/28 к узлу 172.22.34.62.

Далее вводим команду permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62. По данному правилу будет разрешена передача данных по протоколу ICMP от компьютера PC2 на сервер. Остальной трафик запрещён по умолчанию.

Далее необходимо применить разработанный список на интерфейсе gigabitEthernet 0/1 во входящем направлении при помощи команды interface gigabitEthernet 0/1 и ip access-group in.

Для проверки работы примененного списка отправляем эхо-запрос от PC2 на сервер Server (рисунок 4.7). Далее выполняется неуспешное FTP-подключение от PC2 к серверу Server (рисунок 4.7). Затем необходимо открыть веб-браузер на PC2 и введите IP-адрес сервера Server в виде URL-адреса. Подключение должно быть успешным (рисунок 4.8).

```
PC>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
```

Рисунок 4.7 – Эхо-запрос и FTP-подключение к серверу от PC2

Рисунок 4.8 – Подключение к серверу через веб-браузер

Варианты заданий выбираются по аналогии с пунктом 3.2.1

4.2.3 Разработка, настройка и проверка расширенного именованного ACL-списка №2

В этом задании конкретным устройствам сети LAN разрешается доступ к нескольким службам серверов, размещённых в сети Интернет. Используемая сеть представлена на рисунке 4.9.

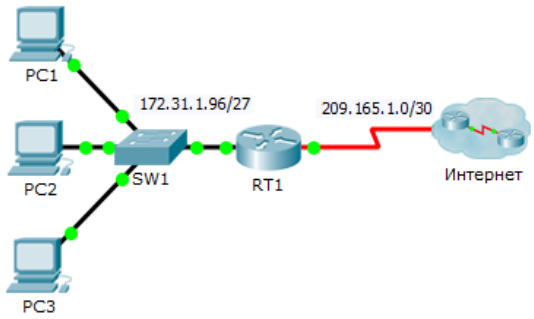

Рисунок 4.9 – Схема сети

На рисунке 4.9 PC1-PC3 выполняют функции персональных компьютеров, SW1 выполняет функции коммутатора, RT1 выполняет функции маршрутизатора, который подключен к сети Интернет.

Необходимо разработать один именованный ACL-список для реализации следующих правил:

– запретить доступ через протоколы HTTP и HTTPS с PC1 на серверы Server1 и Server2, которые находятся внутри облака, известны только их IP-адреса;

– заблокировать FTP-доступ с PC2 к серверам Server1 и Server2;

– заблокировать ICMP-доступ с PC3 к серверам Server1 и Server.

Для создания расширенного именованного ACL-списка необходимо выполнить команду ip access-list extended ACL.

Далее создаем правило, запрещающее доступ с PC1 к серверу Server1, только для HTTP при помощи команды deny tcp host 172.31.1.101 host 64.101.255.254 eq www.

Правило, запрещающее доступ с PC1 к серверу Server1, только для HTTPS создаем при помощи команды deny tcp host 172.31.1.101 host 64.101.255.254 eq 443.

Правила, запрещающие доступ с PC1 к серверу Server2, только для HTTP и HTTPS создаем при помощи команды deny tcp host 172.31.1.101 host 64.103.255.254 eq www и deny tcp host 172.31.1.101 host 64.103.255.254 eq 443.

Правило, запрещающее доступ с PC2 к серверу Server1, только для FTP создаем при помощи команды deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp.

Правило, запрещающее доступ с PC2 к серверу Server2, только для FTP создаем при помощи команды deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp.

Для создания правила, запрещающего ICMP-доступ с PC3 к серверу Server1 используем команду deny icmp host 172.31.1.103 host 64.101.255.254.

При помощи команды deny icmp host 172.31.1.103 host 64.103.255.254 и permit ip any any создаем правило запрещающее ICMP-доступ с PC3 к серверу Server2.

Для применения ACL-списка на соответствующем интерфейсе и направлении выполним команду interface gigabitEthernet 0/0 и ip access-group ACL in.

Проверка расширенного ACL-списка заключается в следующем: проверяется доступ к веб-сайтам на серверах Server1 и Server2, используя веб-браузер PC1, а также протоколы HTTP и HTTPS (рисунок 4.10), проверяется FTP-доступ к серверам Server1 и Server2 с компьютера PC1 (рисунок 4.11),выполняются эхо-запросы на серверы Server1 и Server2 от PC1 (рисунок 4.12). Аналогично поверяются PC2 и PC3. Удачный доступ к веб-сайтам на серверах от PC2 и PC3 – на рисунке 4.13. Неудачный FTP-доступ к серверам от PC2 – на рисунке 4.14. Неудачные эхо-запросы от PC3 к серверам представлены на рисунке 4.15.

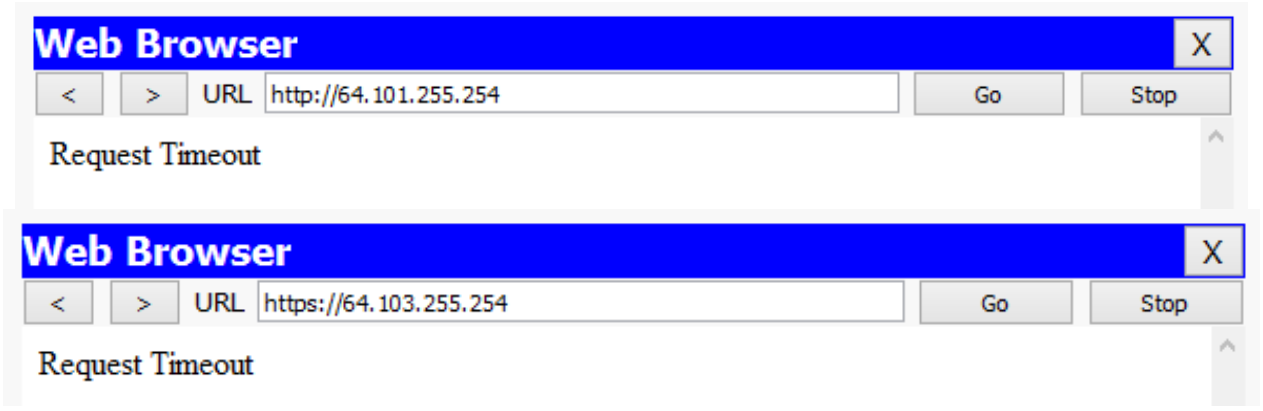

Рисунок 4.10 – Проверка доступа через HTTP и HTTPS

```
PC>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
```

Рисунок 4.11 – FTP-доступ к серверам Server1 и Server2 с PC1

```
PC>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Рисунок 4.12 – Эхо-запросы на серверы Server1 и Server2 от PC1

Рисунок 4.13 – Удачный доступ к веб-сайтам на серверах от PC2 и PC3

```
PC>ftp 64.101.255.254
Trying to connect...64.101.255.254

%Error opening ftp://64.101.255.254/ (Timed out)
PC>ftp 64.103.255.254
Trying to connect...64.103.255.254

%Error opening ftp://64.103.255.254/ (Timed out)
```

Рисунок 4.14 – Неудачный FTP-доступ к серверам от PC2

```
PC>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 4.15 – Неудачные эхо-запросы от PC3 к серверам

Варианты заданий отличаются адресами сети коммутатора SW1 и серверов Server1 и Server2. Адрес сети коммутатора SW1 выбирается в виде 172.31.XX.96/27, где XX две последние цифры номера зачетной книжки. Адрес сервера S1 выбирается в виде 64.101.255.X/15, где X последняя цифра номера зачетной книжки. Адрес сервера S2 выбирается в виде 64.103.255.X/15, где X последняя цифра номера зачетной книжки.

4.3 Контрольные вопросы

1. Опишите формат стандартного именованного списка контроля доступа.

2. Опишите формат расширенного именованного списка контроля доступа.

3. Какая команда используется для размещения списка контроля доступа на выбранном интерфейсе маршрутизатора в нужном направлении ?

4. Какая команда используется для перехода в режим настройки выбранного интерфейса маршрутизатора ?

5. Какие команды используются для создания расширенного именованного ACL-списка для того, чтобы узлы сети 172.22.34.96/28 могли отправлять запросы по протоколам HTTP и ICMP на сервер с адресом 172.22.34.62, но не по протоколу FTP?

6. Какая команда используется для создания расширенного именованного списка контроля доступа, запрещающего узлу 172.22.34.62 доступ к сети 172.22.34.64/27 по протоколу http ?

7. Какая команда используется для разрешения всего остального трафика в расширенном именованном списке контроля доступа ?

8. Какая команда используется для создания расширенного именованного списка контроля доступа, запрещающего любым узлам и сетям доступ к сети 172.22.34.64/27 по протоколу ftp ?

9. Какая команда используется для создания расширенного именованного списка контроля доступа, разрешающего сети 172.22.34.64/27 доступ к любым узлам и сетям по протоколу telnet ?

10. Какое правило устанавливает команда deny tcp host 172.31.1.101 host 64.101.255.254 eq www ?

Список использованных источников

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника» и по специальности «Вычислительные машины, комплексы, системы и сети», «Автоматизированные машины, комплексы, системы и сети», «Программное обеспечение вычислительной техники и автоматизированных систем» / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – Санкт-Петербург : Питер, 2013. – 944 с. : ил. – (Учебник для вузов. Стандарт третьего поколения). – Библиогр.: с. 917. – Алф. указ.: с. 918-943. – ISBN 978-5-496-00004-8.

2. Шевченко, В. П. Вычислительные системы, сети и телекоммуникации: учеб. для вузов / В. П. Шевченко; Моск. авиац. ин-т (Нац. исслед. ун-т). – М. :КноРус, 2012. – 288 с. : ил. – Библиогр.: с. 287-288. – ISBN 978-5406-00521-7.

3. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации : учеб. пособие для вузов / В. Л. Бройдо, О. П. Ильина. – 4-е изд. – СПб. : Питер, 2011. – 555 с. – (Учебник для вузов). – Библиогр.: с. 545-548. – Алф. указ.: с. 549-554. – ISBN 978-5-49807-875-5.

4. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации: учеб. для вузов / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. – 4-е изд., перераб. и доп. – М. : Финансы и статистика, 2008. – 736 с. – Библиогр.: с. 718-721. – Предм. указ.: с. 727-734. – ISBN 978-5-279-03285-3. – ISBN 978-5-16-003418-8.

5. Максимов, Н. В. Компьютерные сети : учеб. пособие / Н. В. Максимов, И. И. Попов. – 3-е изд., перераб. и доп. – М. : Форум, 2008. – 447 с. : ил. – (Проф. образование). – Библиогр.: с. 403-405. – Глоссарий: с. 406-429. – Прил.: с. 430-439. – ISBN 978-5-91134-235-7.

6. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. – 124 с. – Режим доступа: http://znanium.com/bookread2.php?book=463062.

7. Гагарина, Л. Г. Введение в инфокоммуникационные технологии: учебное пособие / Л. Г. Гагарина, А. М. Баин; Под ред. д-ра техн. наук., проф. Л. Г. Гагариной. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 336 с.: 60x90 1/16. – (Высшее образование). – ISBN 978-5-8199-0551-7. Режим доступа: http://znanium.com/bookread2.php?book=408650.

8. СТО 02069024.101–2015 РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления.