

Д.С. Кулябов, А.В. Королькова

АДМИНИСТРИРОВАНИЕ ЛОКАЛЬНЫХ СИСТЕМ

Лабораторные работы



Москва

Российский университет дружбы народов
2017

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Д. С. Кулябов, А. В. Королькова

Администрирование локальных систем

Лабораторные работы

Учебное пособие

Москва

Российский университета дружбы народов

2017

УДК 004.051 (075.8)
ББК 32.973.202
К 90

Утверждено
РИС Учёного совета
Российского университета
дружбы народов

Рецензенты:
доктор технических наук, профессор, начальник отдела УИТО и СТС
РУДН К. Е. Самуйлов
кандидат физико-математических наук, доцент, с.н.с. ЛИТ ОИЯИ
О. И. Стрельцова

Кулябов, Д. С.
К90 Администрирование локальных систем: лабораторные работы :
учебное пособие / Д. С. Кулябов, А. В. Королькова. — Москва :
РУДН, 2017. — 119 с. : ил.

Пособие рекомендуется для проведения лабораторных работ по курсу «Администрирование локальных сетей» для направлений 02.03.02 «Фундаментальная информатика и информационные технологии», 02.03.01 «Математика и компьютерные науки», 09.03.03 «Прикладная информатика».

УДК 004.451(075.8)
ББК 32.973.202

ISBN
978-5-209-08397-9

© Кулябов Д. С., Королькова А. В., 2017
© Российский университет дружбы народов, 2017

Оглавление

Введение.	7
Лабораторная работа № 1. Знакомство с Cisco Packet Tracer	8
1.1. Цель работы	8
1.2. Задание.	8
1.3. Последовательность выполнения работы	8
1.4. Содержание отчёта	12
1.5. Контрольные вопросы	13
Лабораторная работа № 2. Предварительная настройка оборудования Cisco	14
2.1. Цель работы	14
2.2. Задание.	14
2.3. Предварительные сведения	14
2.4. Последовательность выполнения работы	16
2.5. Содержание отчёта	18
2.6. Контрольные вопросы	18
Лабораторная работа № 3. Планирование локальной сети организации	19
3.1. Цель работы	19
3.2. Постановка задачи	19
3.3. Схемы сети	20
3.4. Задание.	24
3.5. Содержание отчёта	24
3.6. Контрольные вопросы	24
Лабораторная работа № 4. Первоначальное конфигурирование сети	26
4.1. Цель работы	26
4.2. Задание.	26
4.3. Последовательность выполнения работы	26
4.4. Содержание отчёта	27
4.5. Контрольные вопросы	27
Лабораторная работа № 5. Конфигурирование VLAN	29
5.1. Цель работы	29
5.2. Задание.	29
5.3. Последовательность выполнения работы	29
5.4. Содержание отчёта	30
5.5. Контрольные вопросы	30
Лабораторная работа № 6. Статическая маршрутизация VLAN	32
6.1. Цель работы	32
6.2. Задание.	32
6.3. Последовательность выполнения работы	32
6.4. Содержание отчёта	33
6.5. Контрольные вопросы	34

Лабораторная работа № 7. Учёт физических параметров сети	35
7.1. Цель работы	35
7.2. Задание	35
7.3. Последовательность выполнения работы	35
7.4. Содержание отчёта	41
7.5. Контрольные вопросы	41
Лабораторная работа № 8. Настройка сетевых сервисов. DHCP	42
8.1. Цель работы	42
8.2. Задание	42
8.3. Последовательность выполнения работы	42
8.4. Содержание отчёта	44
8.5. Контрольные вопросы	45
Лабораторная работа № 9. Использование протокола STP. Агрегирование каналов	46
9.1. Цель работы	46
9.2. Предварительные сведения	46
9.3. Задание	48
9.4. Последовательность выполнения работы	48
9.5. Содержание отчёта	51
9.6. Контрольные вопросы	51
Лабораторная работа № 10. Настройка списков управления доступом (ACL)	52
10.1. Цель работы	52
10.2. Задание	52
10.3. Последовательность выполнения работы	52
10.4. Самостоятельная работа	56
10.5. Содержание отчёта	56
10.6. Контрольные вопросы	56
Лабораторная работа № 11. Настройка NAT. Планирование	57
11.1. Цель работы	57
11.2. Предварительные сведения	57
11.3. Задание	58
11.4. Последовательность выполнения работы	59
11.5. Содержание отчёта	62
11.6. Контрольные вопросы	62
Лабораторная работа № 12. Настройка NAT	63
12.1. Цель работы	63
12.2. Постановка задачи	63
12.3. Задание	64
12.4. Последовательность выполнения работы	64
12.5. Содержание отчёта	68
12.6. Контрольные вопросы	68

Лабораторная работа № 13. Статическая маршрутизация в Интернете. Планирование	70
13.1. Цель работы.	70
13.2. Модельные предположения.	70
13.3. Задание	70
13.4. Последовательность выполнения работы	74
13.5. Содержание отчёта	80
13.6. Контрольные вопросы	80
Лабораторная работа № 14. Статическая маршрутизация в Интернете. Настройка	81
14.1. Цель работы.	81
14.2. Задание	81
14.3. Последовательность выполнения работы	81
14.4. Содержание отчёта	86
14.5. Контрольные вопросы	87
Лабораторная работа № 15. Динамическая маршрутизация	88
15.1. Цель работы.	88
15.2. Предварительные сведения.	88
15.3. Задание	89
15.4. Последовательность выполнения работы	89
15.5. Содержание отчёта	91
15.6. Контрольные вопросы	92
Лабораторная работа № 16. Настройка VPN	93
16.1. Цель работы.	93
16.2. Задание	93
16.3. Предварительные сведения.	94
16.4. Модельные предположения.	94
16.5. Последовательность выполнения работы	95
16.6. Содержание отчёта	97
16.7. Контрольные вопросы	97
Рекомендуемая литература.	98
Глоссарий	98

Учебно-методический комплекс	101
Программа дисциплины	103
1. Цели и задачи дисциплины	103
2. Место дисциплины в структуре ОП ВО	103
3. Требования к результатам освоения дисциплины.	105
4. Объем дисциплины и виды учебной работы	106
5. Содержание дисциплины	106
6. Лабораторный практикум	107
7. Практические занятия (семинары)	107
8. Материально-техническое обеспечение дисциплины	108
9. Информационное обеспечение дисциплины	108
10. Учебно-методическое обеспечение дисциплины	108
11. Методические указания для обучающихся по освоению дисциплины.	108

Паспорт фонда оценочных средств	110
Фонд оценочных средств	112
Балльно-рейтинговая система оценки уровня знаний	112
Критерии оценки по дисциплине	114
Примерный перечень оценочных средств	116
Комплект заданий для итогового контроля знаний	117
Комплект разноуровневых задач (заданий)	118
Сведения об авторах	119

Введение

Пособие рекомендуется для проведения лабораторных работ по курсу «Администрирование локальных сетей» для направлений 02.03.02 «Фундаментальная информатика и информационные технологии», 02.03.01 «Математика и компьютерные науки», 09.03.03 «Прикладная информатика».

Дисциплина «Администрирование локальных сетей» является продолжением цикла дисциплин, посвящённых сетевым технологиям [2], в которых рассматривались теоретические и практические аспекты сетевых протоколов и организации IP-сетей. Данное пособие носит практический характер и призвано дать первоначальные знания и умения по построению и конфигурированию локальных сетей.

Практикум проводится с использованием свободно-распространяемого средства имитационного моделирования локальных сетей Cisco Packet Tracer [1]. Данное программное средство накладывает ограничения на содержание лабораторных работ практикума. Основой идеи курса послужил проект «Сети для самых маленьких» [3], рассматривающего основы построения сетевого оборудования компании Cisco, в частности вопросы коммутации, маршрутизации, настройки протоколов NAT, STP, VPN.

В пособии моделируется локальная сеть учебной организации. Вначале строится коммутируемая сеть одного из территориальных подразделений организации. Затем, по мере усложнения структуры организации, осуществляется переход к задачам статической и динамической маршрутизации как внутри подразделения, так и между другими её территориями. Завершается пособие решением задачи подключения удалённых площадок с помощью протоколов 2-го и 3-го уровней модели ISO/OSI.

Каждая лабораторная работа практикума содержит формулировку конкретной практической задачи, пошаговое описание выполнения задания, а также вопросы для самоконтроля понимания рассматриваемой темы. Часть работ содержит задания для самостоятельного выполнения. В конце практикума дан учебно-методический комплекс, содержащий программу курса и фонд оценочных средств по дисциплине.

Литература по теме

1. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014.
2. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
3. Цикл статей «Сети для самых маленьких». — URL: <http://linkmeup.ru/blog/11.html>.

Лабораторная работа № 1. Знакомство с Cisco Packet Tracer

1.1. Цель работы

Установка инструмента моделирования конфигурации сети Cisco Packet Tracer [1], знакомство с его интерфейсом.

1.2. Задание

1. Зарегистрироваться на сайте сетевой академии Cisco (<https://www.netacad.com>).
2. Пройти часовой онлайн курс, знакомящий с интерфейсом Packet Tracer (<https://www.netacad.com/campaign/ptdt-2>).
3. Установить на домашнем устройстве Cisco Packet Tracer.

1.3. Последовательность выполнения работы

1.3.1. Регистрация на сайте академии Cisco

1. Перейдите на страницу <https://www.netacad.com/campaign/ptdt-2>.
2. Заполните поля блока Enroll Now, указав имя (First Name), фамилию (Last Name) и e-mail. Введите текст для верификации, отображённый на картинке и нажмите Submit.
3. После получения на Ваш e-mail письма от сетевой академии Cisco Вам потребуется подтвердить Ваш e-mail. На открывшейся странице необходимо будет указать страну (Russia), регион (Moscow), дату рождения и прописать пароль. После этого Вы можете использовать для обучения Packet Tracer (установленный в дисплейных классах или на домашнем устройстве).

1.3.2. Знакомство с интерфейсом Packet Tracer

1. Перейдите на страницу курса Packet Tracer 101 0817g.
2. Изучите содержание курса (курс представлен на английском языке):
 - опишите в отчёте основные элементы пользовательского интерфейса Packet Tracer;
 - опишите в отчёте, за что отвечают основные элементы меню Packet Tracer;
 - укажите в отчёте, для чего нужна логическая рабочая область (Logical) (рис. 1.1), когда и для чего используется физическая рабочая область (Physical) (рис. 1.2);
 - опишите основные элементы навигационной панели физической рабочей области (см. рис. 1.2).
3. Выполните следующие действия по построению небольшой сети, состоящей из маршрутизатора, двух коммутаторов и двух компьютеров пользователя:

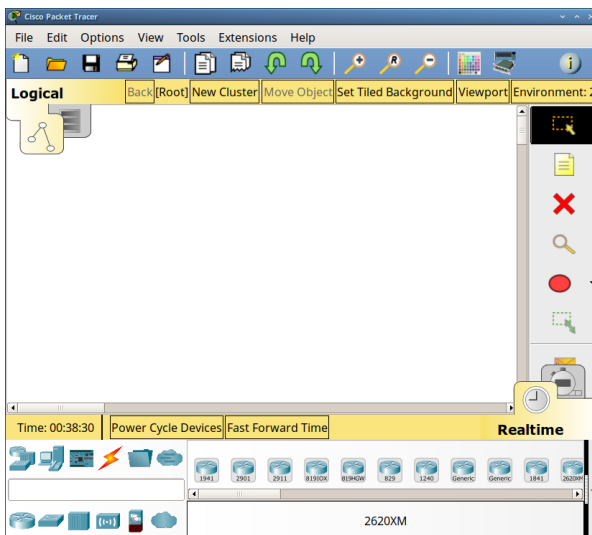


Рис. 1.1. Логическая рабочая область Packet Tracer

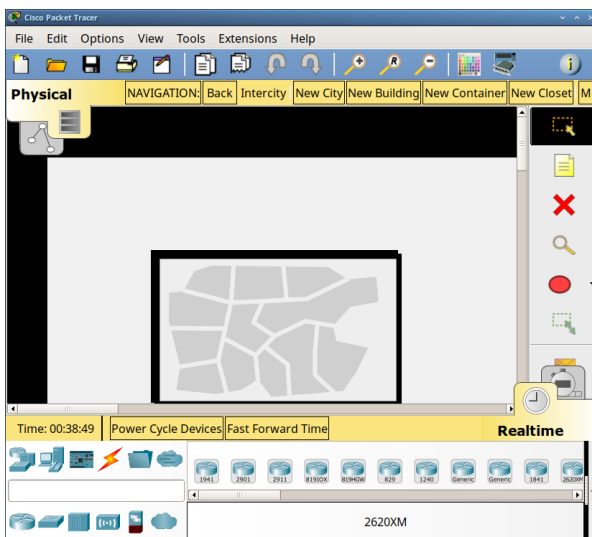


Рис. 1.2. Физическая рабочая область Packet Tracer

- в логической рабочей области разместите маршрутизатор типа Router 2901, два коммутатора типа Switch 2960, два оконечных устройства (End Devices) типа PC-PT Generic (рис. 1.3);

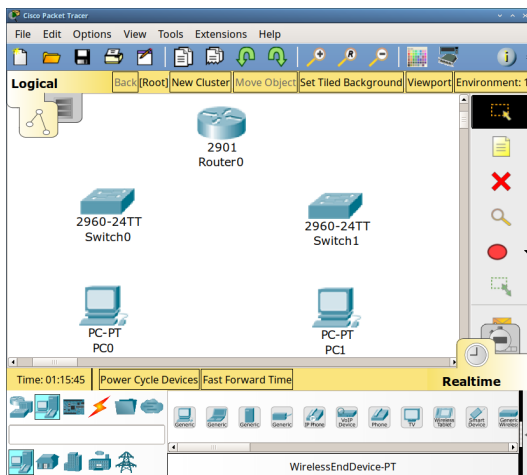


Рис. 1.3. Размещение элементов сети в логической рабочей области Packet Tracer

- задайте имена коммутаторам сети, используя как возможности графического интерфейса (рис. 1.4) для первого коммутатора, так и возможности командной строки (рис. 1.5) для второго коммутатора, введя последовательно команды: `enable`, `configure terminal`, `hostname S02`;
- для оконечного устройства PC01 через графический интерфейс задайте gateway-адрес 192.168.1.1, ip-адрес 192.168.1.2 с маской сети 255.255.255.0, а для для оконечного устройства PC02 — gateway-адрес 192.168.2.1, ip-адрес 192.168.2.2 с маской сети 255.255.255.0;
- соедините элементы сети, используя соответствующие коннекторы;
- на маршрутизаторе с помощью командной строки задайте его имя и адреса на интерфейсах G0/0 и G0/1:

```
enable
configure terminal
hostname R01
interface g0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface g0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
write memory
```

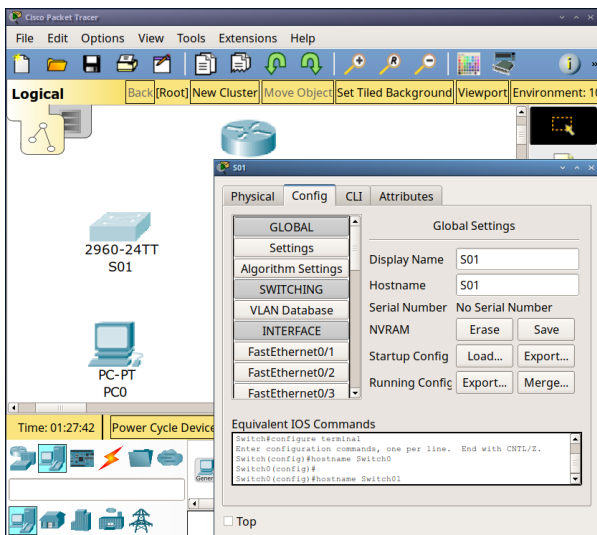


Рис. 1.4. Графический интерфейс настроек коммутатора S01

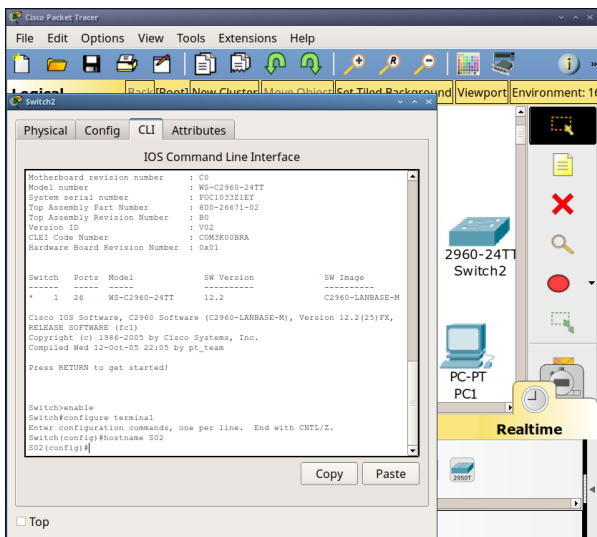


Рис. 1.5. Интерфейс командной строки настроек коммутатора S02

- используя командную строку (Command Prompt) на PC01, проверьте доступность узла PC02, применив команду `ping 192.168.2.1`.

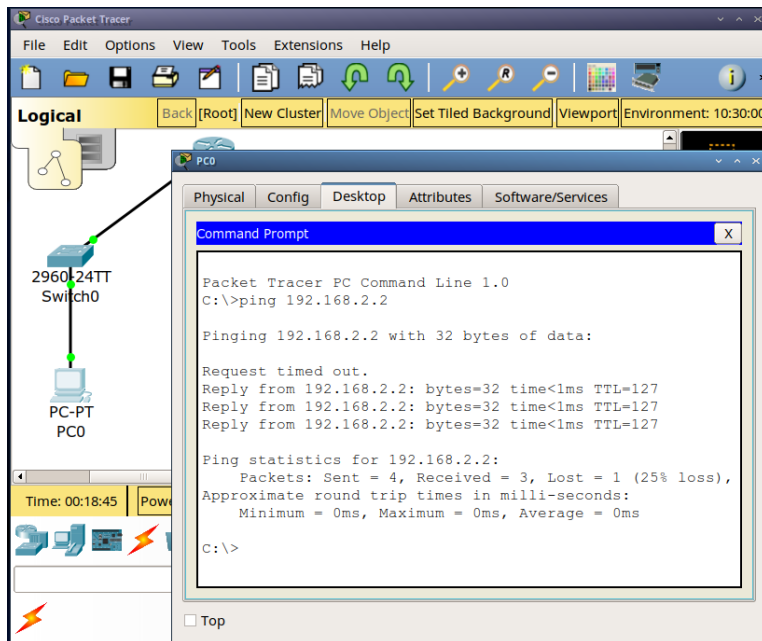


Рис. 1.6. Использование командной строки оконечного устройства PC01 для проверки узла PC02 с помощью команды `ping`

1.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - резюме содержания часового курса академии Cisco;
 - описание основных панелей и меню интерфейса Packet Tracer.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

1.5. Контрольные вопросы

1. Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования?
2. Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcast-адрес.
3. Что такое сетевой интерфейс? Приведите примеры.
4. Приведите основные последовательности команд для задания на маршрутизаторе имени, ip-адреса интерфейса.
5. Как можно проверить доступность узла сети?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1–9].

Литература по теме

1. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014.
2. Cotton M., Vegoda L. Special Use IPv4 Addresses : RFC / RFC Editor. — 01/2010. — P. 1–11. — No. 5735. — DOI: 10.17487/rfc5735.
3. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series).
4. Королькова А. В., Кулябов Д. С. Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014.
5. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
6. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
7. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
8. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
9. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 2. Предварительная настройка оборудования Cisco

2.1. Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.















2.2. Задание

1. Сделать предварительную настройку маршрутизатора:
 - задать имя в виде «город-территория-тип_оборудования-номер»: `msk-donskaya-gw-1`;
 - задать интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднять интерфейс;
 - задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);
 - настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена `donskaya.rudn.edu`);
 - сохранить и экспортировать конфигурацию в отдельный файл.
2. Сделать предварительную настройку коммутатора:
 - задать имя в виде «город-территория-тип_оборудования-номер»: `msk-donskaya-sw-1`;
 - задать интерфейсу vlan 2 ip-адрес 192.168.2.1 и маску 255.255.255.0, затем поднять интерфейс;
 - привязать интерфейс Fast Ethernet с номером 1 к vlan 2;
 - задать в качестве адреса шлюза по умолчанию адрес 192.168.2.254;
 - задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);
 - настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена `donskaya.rudn.edu`);
 - для пользователя `admin` задать доступ 1-го уровня по паролю;
 - сохранить и экспортировать конфигурацию в отдельный файл.

2.3. Предварительные сведения

Некоторые особенности при работе с cisco IOS Command Line Interface (CLI):

- вводимые в консоли команды воспринимаются как в полном, так и в сокращённом виде (например, для вывода содержания файла конфигурации оборудования можно использовать как `show running-config`, так и её сокращённую запись `sh run`);
- для дописывания сокращённой команды до полной формы используйте клавишу `Tab`;
- для вывода списка возможных к исполнению команд и краткой информации по ним используйте знак вопроса;
- горячие клавиши:
 - `Ctrl`+`a` — переместить курсор в начало строки;

-  +  — переместить курсор в конец строки;
-  ,  — отвечают за навигацию по истории команд;
-  +  — удалить слово, расположенное до курсора;
-  +  — удалить строку;
-  +  — выйти из режима конфигурирования;
-  +  — применить текущую команду и выйти из режима конфигурирования;
- доступные режимы CLI (вместо слова **Router** в консоли выдаётся имя устройства):
 - *пользовательский режим (user mode)* предназначен для просмотра статистики и выполнения ограниченного числа операций, не влияющих на функционирование устройства:
Router>
 - *привилегированный режим (privileged mode)* предназначен для выполнения операций по настройке оборудования:
Router#
 - *режим глобальной конфигурации (global configuration mode)* позволяет вносить изменения в настройки устройства:
Router(config)#
 - *режим специфической конфигурации:*
Router(config-*)#
вместо звёздочки отображается название подрежима (например, **Router(config-if)#** указывает на переход в режим настройки интерфейса маршрутизатора);
- для перехода в привилегированный режим из пользовательского режима используется команда **enable**, возможно с введением пароля;
- для перехода в режим глобальной конфигурации из привилегированного режима используется команда **configure terminal** или её сокращённый аналог **conf t**;
- переход в режим специфической конфигурации всегда осуществляется из режима глобальной конфигурации после ввода соответствующей команды (например, для перехода в режим настройки интерфейса Fast Ethernet с номером 0 потребуется ввести в режиме глобальной конфигурации команду **interface FastEthernet 0/0**);
- некоторые часто используемые команды:
 - **exit** — возвращение в привилегированный режим (аналог комбинации клавиш  + );
 - **show running-configuration** (или **sh ru**) — отображение текущей конфигурации устройства;
 - **show startup config** — отображает содержание конфигурации оборудования, загружаемое после включения оборудования;
 - **write memory** — запись изменений;
 - **copy running-configuration startup-configuration** — сохранение текущих изменений в настройках в энергонезависимую память;
 - **(no) service password-encryption** — указание на отображение в конфигурационном файле введённых ранее паролей в (открытом — при использовании **no** в начале) зашифрованном виде;
 - **show interface** — отображение состояния сетевого интерфейса;

- (no) shutdown — (включение) выключение сетевого интерфейса (по умолчанию интерфейсы находятся в выключенном состоянии);
- show vlan — отображение имеющихся vlan с привязкой к ним физических интерфейсов (Virtual Local Area Network, VLAN — группа узлов сети, возможно подключённых к разным сетевым устройствам (коммутаторам), но при этом взаимодействующих между собой через протокол канального уровня, как если бы они были подключены к широковещательному домену);
- no vlan n — отключить vlan с номером n;
- show ip route — выводит таблицу маршрутизации роутера.

2.4. Последовательность выполнения работы

1. В логической рабочей области Packet Tracer разместите коммутатор, маршрутизатор и 2 конечных устройства типа PC, соедините один PC с маршрутизатором, другой PC — с коммутатором (рис. 2.1).

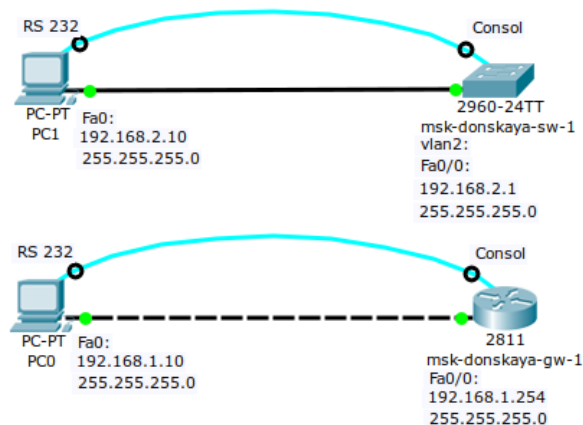


Рис. 2.1. Схема подключения оборудования для проведения его предварительной настройки

2. Проведите настройку маршрутизатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации маршрутизатора (см. раздел 2.4.1).
3. Проведите настройку коммутатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации коммутатора (см. раздел 2.4.2).
4. Проверьте работоспособность соединений с помощью команды ping.
5. Попробуйте подключиться к коммутатору и маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

2.4.1. Конфигурация маршрутизатора

```
Router>enable
Router#configure terminal

Router(config)#hostname msk-donskaya-gw-1

msk-donskaya-gw-1(config)#interface f0/0
msk-donskaya-gw-1(config-if)#no shutdown
msk-donskaya-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0

msk-donskaya-gw-1(config)#line vty 0 4
msk-donskaya-gw-1(config-line)#password cisco
msk-donskaya-gw-1(config-line)#login

msk-donskaya-gw-1(config)#line console 0
msk-donskaya-gw-1(config-line)#password cisco
msk-donskaya-gw-1(config-line)#login

msk-donskaya-gw-1(config)#enable secret cisco
msk-donskaya-gw-1(config)#service password-encryption

msk-donskaya-gw-1(config)#username admin privilege 1 secret cisco

msk-donskaya-gw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-gw-1(config)#crypto key generate rsa
msk-donskaya-gw-1(config)#line vty 0 4
msk-donskaya-gw-1(config-line)#transport input ssh
```

2.4.2. Конфигурация коммутатора

```
Switch>enable
Switch#configure terminal

Switch(config)#hostname msk-donskaya-sw-1

msk-donskaya-sw-1(config)#interface vlan2
msk-donskaya-sw-1(config-if)#no shutdown
msk-donskaya-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0

msk-donskaya-sw-1(config)#interface f0/1
msk-donskaya-sw-1(config-if)#switchport mode access
msk-donskaya-sw-1(config-if)#switchport access vlan 2

msk-donskaya-sw-1(config)#ip default-gateway 192.168.2.254

msk-donskaya-sw-1(config)#line vty 0 4
msk-donskaya-sw-1(config-line)#password cisco
msk-donskaya-sw-1(config-line)#login

msk-donskaya-sw-1(config)#line console 0
msk-donskaya-sw-1(config-line)#password cisco
msk-donskaya-sw-1(config-line)#login

msk-donskaya-sw-1(config)#enable secret cisco
msk-donskaya-sw-1(config)#service password-encryption
msk-donskaya-sw-1(config)#username admin privilege 1 secret cisco

msk-donskaya-sw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-sw-1(config)#crypto key generate rsa
msk-donskaya-sw-1(config)#line vty 0 4
msk-donskaya-sw-1(config-line)#transport input ssh
```

2.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

2.6. Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.
2. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему?
3. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему?
4. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему?
5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.
6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—5].

Литература по теме

1. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014.
2. *Королькова А. В., Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014.
3. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
4. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
5. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 3. Планирование локальной сети организации

3.1. Цель работы

Познакомится с принципами планирования локальной сети организации.

3.2. Постановка задачи

Предположим, что в некоторой учебной организации требуется спланировать сетевую инфраструктуру.

Особенности организации с точки зрения планирования локальной сети:

- организация располагается в одном городе (предположим — в Москве), но на двух территориях (назовём их «Донская» и «Павловская»);
- группы пользователей организации:
 - администрация (А);
 - преподавательский состав кафедр (К);
 - пользователи дисплейных классов общего пользования (ДК);
 - другие пользователи (Д);
- предполагается, что на территории «Донская» будут располагаться:
 - устройства управления сетью;
 - серверная инфраструктура;
 - оборудование всех групп пользователей;
- предполагается, что на территории «Павловская» будет располагаться оборудование групп пользователей «ДК» и «Д».

Сеть организации должна соответствовать так называемой «иерархической модели сети», т.е. оборудование сетевой инфраструктуры при планировании должно быть распределено по трём уровням:

- 1) уровень ядра (Core Layer) — высокопроизводительные сетевые устройства (коммутаторы, маршрутизаторы), обеспечивающие скоростную передачу трафика между сегментами уровня распределения;
- 2) уровень распределения (Distribution Layer) — устройства (коммутаторы, маршрутизаторы), обеспечивающие применение политик безопасности и качества обслуживания (QoS), агрегацию и маршрутизацию трафика посредством VLAN, определение широковебательных доменов;
- 3) уровень доступа (Access Layer) — устройства для подключения серверов и оконечного оборудования пользователей к сети организации.

Далее при проектировании сети необходимо:

- разработать схемы сети, соответствующие физическому, каналному и сетевому уровням эталонной модели взаимодействия открытых систем (OSI);
- составить план IP-адресация сети;
- составить план VLAN сети;
- составить план подключения интерфейсов оборудования;
- зафиксировать перечень устройств, используемых в сети организации, с указанием модели, версии операционной системы, объема RAM/NVRAM, списка интерфейсов;
- обеспечить маркировку всех задействованных как сетевых и других типов кабелей (откуда и куда идёт), так и устройств сети;
- разработать и внедрить единый регламент эксплуатации сети.

3.3. Схемы сети

Примерная схема планируемой сети с указанием типов и номеров портов подключения устройств, соответствующая физическому уровню модели OSI (L1), будет иметь вид, изображённый на рис. 3.1.

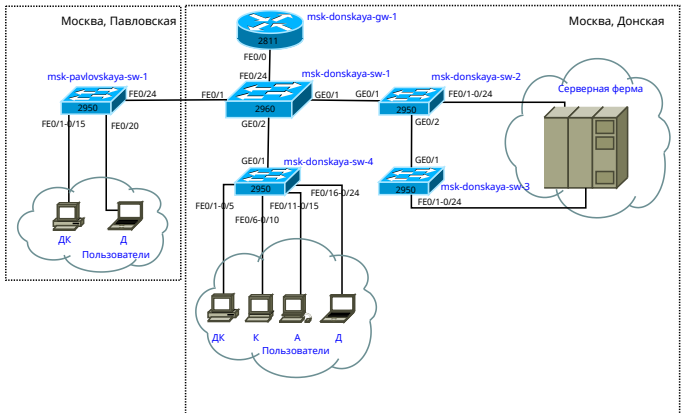


Рис. 3.1. Физические устройства сети с номерами портов (Layer 1)

В качестве оборудования уровня ядра будем использовать маршрутизатор Cisco 2811, на уровне распределения — коммутаторы Cisco 2960 с возможностью настройки VLAN, а на уровне доступа — коммутаторы Cisco 2950.

Далее следует спланировать распределение VLAN. Рекомендуется выделять в отдельные подсети (VLAN) устройства управления сетью, а также различные группы пользователей (см. табл. 3.1).

Таблица 3.1

Таблица VLAN

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4-100		Зарезервировано
101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей

Примерная схема сети с указанием номеров VLAN, соответствующая канальному уровню модели OSI (L2), будет иметь вид, изображённый на рис. 3.2

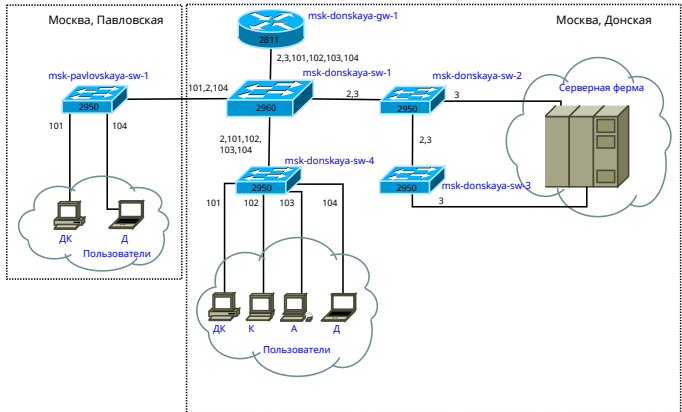


Рис. 3.2. Схема VLAN сети (Layer 2)

Далее необходимо определить адресное пространство, ассоциированное с выделенными VLAN. Примерная схема сети, соответствующая сетевому уровню модели OSI (L3), будет иметь вид, изображённый на рис. 3.3.

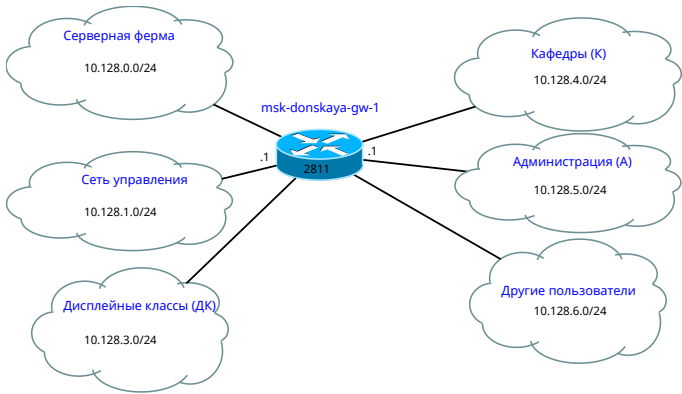


Рис. 3.3. Схема маршрутизации сети (Layer 3)

Более детальное распределение IP-адресов [2] в сети представлено в табл. 3.2.

При планировании IP-адресация (разбиении адресного пространства сети на подсети) следует учитывать потенциальное количество устройств подсети, а также возможность увеличения их числа.

В табл. 3.3 приведён план подключения оборудования сети по портам.

Таблица 3.2

Таблица IP

IP-адреса	Примечание	VLAN
10.128.0.0/16	Вся сеть	
10.128.0.0/24	Серверная ферма	3
10.128.0.1	Шлюз	
10.128.0.2	Web	
10.128.0.3	File	
10.128.0.4	Mail	
10.128.0.5	Dns	
10.128.0.6-10.128.0.254	Зарезервировано	
10.128.1.0/24	Управление	2
10.128.1.1	Шлюз	
10.128.1.2	msk-donskaya-sw-1	
10.128.1.3	msk-donskaya-sw-2	
10.128.1.4	msk-donskaya-sw-3	
10.128.1.5	msk-donskaya-sw-4	
10.128.1.6	msk-pavlovskaya-sw-1	
10.128.1.6-10.128.1.254	Зарезервировано	
10.128.2.0/24	Сеть Point-to-Point	
10.128.2.1	Шлюз	
10.128.2.2-10.128.2.254	Зарезервировано	
10.128.3.0/24	Дисплейные классы (ДК)	101
10.128.3.1	Шлюз	
10.128.3.2-10.128.3.254	Пул для пользователей	
10.128.4.0/24	Кафедры (К)	102
10.128.4.1	Шлюз	
10.128.4.2-10.128.4.254	Пул для пользователей	
10.128.5.0/24	Администрация (А)	103
10.128.5.1	Шлюз	
10.128.5.2-10.128.5.254	Пул для пользователей	
10.128.6.0/24	Другие пользователи (Д)	104
10.128.6.1	Шлюз	
10.128.6.2-10.128.6.254	Пул для пользователей	

Таблица 3.3

Таблица портов

Устройство	Порт	Примечание	Access VLAN	Trunk VLAN
msk-donskaya-gw-1	f0/1 f0/0	UpLink msk-donskaya-sw-1		2, 3, 101, 102, 103, 104
msk-donskaya-sw-1	g1/1 g1/2 f0/1 f0/2	msk-donskaya-gw-1 msk-donskaya-sw-2 msk-donskaya-sw-4 msk-pavlovskaya-sw-1		2, 3 2, 101, 102, 103, 104 2, 101, 104
msk-donskaya-sw-2	g1/1 g1/2 f0/1 f0/2	msk-donskaya-sw-1 msk-donskaya-sw-3 Web-server File-server	3 3	2, 3 2, 3
msk-donskaya-sw-3	g1/1	msk-donskaya-sw-2		2, 3
	f0/1 f0/2	Mail-server Dns-server	3 3	
msk-donskaya-sw-4	f0/24 f0/1–f0/5 f0/6–f0/10 f0/11–f0/15 f0/16–f0/24	msk-donskaya-sw-1 dk departments adm other	101 102 103 104	2, 101, 102, 103, 104
msk-pavlovskaya-sw-1	f0/24 f0/1–f0/15 f0/20	msk-donskaya-sw-1 dk other	101 104	2, 101, 104

Регламент выделения ip-адресов дан в табл. 3.4.

Таблица 3.4

Регламент выделения ip-адресов (для сети класса C)

IP-адреса	Примечание
1	Шлюз
2–19	Сетевое оборудование
20–29	Серверы
30–199	Компьютеры, DHCP
200–219	Компьютеры, Static
220–229	Принтеры
230–254	Резерв

3.4. Задание

1. Используя графический редактор (например, Dia), требуется повторить схемы L1, L2, L3, а также сопутствующие им таблицы VLAN, IP-адресов и портов подключения оборудования планируемой сети.
2. Рассмотренный выше пример планирования адресного пространства сети базируется на разбиении сети 10.128.0.0/16 на соответствующие подсети. Требуется сделать аналогичный план адресного пространства для сетей 172.16.0.0/12 и 192.168.0.0/16 с соответствующими схемами сети и сопутствующими таблицами VLAN, IP-адресов и портов подключения оборудования.

3.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания: схемы L1, L2, L3, таблицы VLAN, IP-адресов и портов подключения оборудования для трёх сетей: 10.128.0.0/16, 172.16.0.0/12 и 192.168.0.0/16 с комментариями.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

3.6. Контрольные вопросы

1. Что такое модель взаимодействия открытых систем (OSI)? Какие уровни в ней есть? Какие функции закреплены за каждым уровнем модели OSI?
2. Какие функции выполняет коммутатор?
3. Какие функции выполняет маршрутизатор?
4. В чём отличие коммутаторов третьего уровня от коммутаторов второго уровня?

5. Что такое сетевой интерфейс?
6. Что такое сетевой порт?
7. Кратко охарактеризуйте технологии Ethernet, Fast Ethernet, Gigabit Ethernet.
8. Что такое IP-адрес (IPv4-адрес)? Определите понятия сеть, подсеть, маска подсети. Охарактеризуйте служебные IP-адреса. Приведите пример с пояснениями разбиения сети на две или более подсетей с указанием числа узлов в каждой подсети.
9. Дайте определение понятию VLAN. Для чего применяется VLAN в сети организации? Какие преимущества даёт применение VLAN в сети организации? Приведите примеры разных ситуаций.
10. В чём отличие Trunk Port от Access Port?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—7].

Литература по теме

1. 802.1Q - Virtual LANs. — URL: <http://www.ieee802.org/1/pages/802.1q.html>.
2. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01/2010. — P. 1–11. — No. 5735. — DOI: 10.17487/rfc5735.
3. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: <http://www.ietf.org/rfc/rfc3069.txt>.
4. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: <http://protect.gost.ru/v.aspx?control=7&id=132355>.
5. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
6. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
7. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 4. Первоначальное конфигурирование сети

4.1. Цель работы

Провести подготовительную работу по первоначальной настройке коммутаторов сети.

4.2. Задание

Требуется сделать первоначальную настройку коммутаторов сети, представленной на схеме L1 (см. рис. 3.1 из раздела 3.3). Под первоначальной настройкой понимается указание имени устройства, его IP-адреса, настройка доступа по паролю к виртуальным терминалам и консоли, настройка удалённого доступа к устройству по ssh.

4.3. Последовательность выполнения работы

1. В логической рабочей области Packet Tracer разместите коммутаторы и оконечные устройства согласно схеме сети L1 (см. рис. 3.1 из раздела 3.3) и соедините их через соответствующие интерфейсы (рис. 4.1).

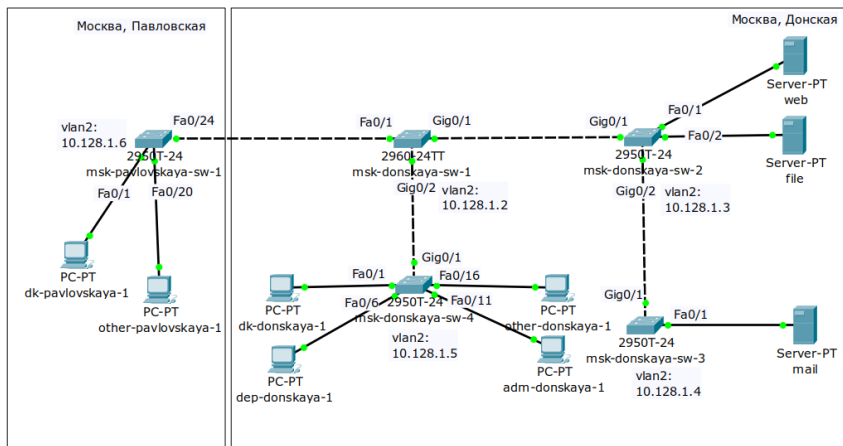


Рис. 4.1. Размещение коммутаторов и оконечных устройств согласно схеме сети L1

2. Используя типовую конфигурацию коммутатора (см. пример 4.1), настройте все коммутаторы, изменяя название устройства и его IP-адрес согласно плану IP (см. табл. 3.2 из раздела 3.3).

Пример 4.1. Последовательность команд по первоначальной настройке коммутатора `msk-donskaya-sw-1`.

```
Switch>enable
Switch#configure terminal

Switch(config)#hostname msk-donskaya-sw-1

msk-donskaya-sw-1(config)#interface vlan2
msk-donskaya-sw-1(config-if)#no shutdown
msk-donskaya-sw-1(config-if)#ip address 10.128.1.2 255.255.255.0
msk-donskaya-sw-1(config-if)#exit

msk-donskaya-sw-1(config)#ip default-gateway 10.128.1.1

msk-donskaya-sw-1(config)#line vty 0 4
msk-donskaya-sw-1(config-line)#password cisco
msk-donskaya-sw-1(config-line)#login
msk-donskaya-sw-1(config-line)#exit

msk-donskaya-sw-1(config)#line console 0
msk-donskaya-sw-1(config-line)#password cisco
msk-donskaya-sw-1(config-line)#login
msk-donskaya-sw-1(config-line)#exit

msk-donskaya-sw-1(config)#enable secret cisco
msk-donskaya-sw-1(config)#service password-encryption
msk-donskaya-sw-1(config)#username admin privilege 1 secret cisco

msk-donskaya-sw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-sw-1(config)#crypto key generate rsa

msk-donskaya-sw-1(config)#line vty 0 4
msk-donskaya-sw-1(config-line)#transport input ssh

msk-donskaya-sw-1(config-line)#exit
msk-donskaya-sw-1(config)#exit
msk-donskaya-sw-1#write memory
```

4.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана) с пояснениями, фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

4.5. Контрольные вопросы

1. При помощи каких команд можно посмотреть конфигурацию сетевого оборудования?

2. При помощи каких команд можно посмотреть стартовый конфигурационный файл оборудования?
3. При помощи каких команд можно экспортировать конфигурационный файл оборудования?
4. При помощи каких команд можно импортировать конфигурационный файл оборудования?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—4].

Литература по теме

1. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014.
2. *Королькова А. В., Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014.
3. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
4. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

Лабораторная работа № 5. Конфигурирование VLAN

5.1. Цель работы

Получить основные навыки по настройке VLAN на коммутаторах сети.

5.2. Задание

1. На коммутаторах сети настроить Trunk-порты на соответствующих интерфейсах (см. табл. 3.2 из раздела 3.3), связывающих коммутаторы между собой.
2. Коммутатор `msk-donskaya-sw-1` настроить как VTP-сервер и прописать на нём номера и названия VLAN согласно табл. 3.1 из раздела 3.3.
3. Коммутаторы `msk-donskaya-sw-2` — `msk-donskaya-sw-4`, `msk-pavlovskaya-sw-1` настроить как VTP-клиенты, на интерфейсах указать принадлежность к соответствующему VLAN (см. табл. 3.3 из раздела 3.3).
4. На серверах прописать IP-адреса, как указано в табл. 3.2 из раздела 3.3.
5. На оконечных устройствах указать соответствующий адрес шлюза и прописать статические IP-адреса из диапазона соответствующей сети, следуя регламенту выделения IP-адресов (см. табл. 3.4 из раздела 3.3).
6. Проверить доступность устройств, принадлежащих одному VLAN, и недоступность устройств, принадлежащих разным VLAN.

5.3. Последовательность выполнения работы

1. Используя приведённую ниже последовательность команд из примера по конфигурации Trunk-порта на интерфейсе `g0/1` коммутатора `msk-donskaya-sw-1`, настройте Trunk-порты на соответствующих интерфейсах всех коммутаторов.
2. Используя приведённую ниже последовательность команд по конфигурации VTP, настройте коммутатор `msk-donskaya-sw-1` как VTP-сервер и пропишите на нём номера и названия VLAN (см. табл. 3.1 из раздела 3.3).
3. Используя приведённую ниже последовательность команд по конфигурации диапазонов портов, настройте коммутаторы `msk-donskaya-sw-2` — `msk-donskaya-sw-4`, `msk-pavlovskaya-sw-1` как VTP-клиенты и на интерфейсах укажите принадлежность к VLAN (см. табл. 3.3 из раздела 3.3).
4. После указания статических IP-адресов на оконечных устройствах проверьте с помощью команды `ping` доступность устройств, принадлежащих одному VLAN, и недоступность устройств, принадлежащих разным VLAN.
5. Используя режим симуляции в Packet Tracer, изучите процесс передвижения пакета ICMP по сети. Изучите содержимое передаваемого пакета и заголовки задействованных протоколов.

5.3.1. Конфигурация Trunk-порта

```
msk-donskaya-sw-1>enable
msk-donskaya-sw-1#configure terminal
msk-donskaya-sw-1(config)#interface g0/1
msk-donskaya-sw-1(config-if)#switchport mode trunk
```

5.3.2. Конфигурация VTP

```
msk-donskaya-sw-1>enable
msk-donskaya-sw-1#configure terminal
msk-donskaya-sw-1(config)#vtp mode server
msk-donskaya-sw-1(config)#vtp domain donsкаya
msk-donskaya-sw-1(config)#vtp password cisco
msk-donskaya-sw-1(config-vlan)#vlan 2
msk-donskaya-sw-1(config-vlan)#name management
msk-donskaya-sw-1(config-vlan)#vlan 3
msk-donskaya-sw-1(config-vlan)#name servers
msk-donskaya-sw-1(config-vlan)#vlan 101
msk-donskaya-sw-1(config-vlan)#name dk
msk-donskaya-sw-1(config-vlan)#vlan 102
msk-donskaya-sw-1(config-vlan)#name departaments
msk-donskaya-sw-1(config-vlan)#vlan 103
msk-donskaya-sw-1(config-vlan)#name adm
msk-donskaya-sw-1(config-vlan)#vlan 104
msk-donskaya-sw-1(config-vlan)#name other
```

5.3.3. Конфигурация диапазона портов

```
msk-donskaya-sw-4#conf terminal
msk-donskaya-sw-4(config)#vtp mode client
msk-donskaya-sw-4(config)#interface range f0/1 - 5
msk-donskaya-sw-4(config-if-range)#switchport mode access
msk-donskaya-sw-4(config-if-range)#switchport access vlan 101
```

5.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

5.5. Контрольные вопросы

1. Какая команда используется для просмотра списка VLAN на сетевом устройстве?
2. Охарактеризуйте VLAN Trunking Protocol (VTP). Приведите перечень команд с пояснениями для настройки и просмотра информации о VLAN.
3. Охарактеризуйте Internet Control Message Protocol (ICMP). Опишите формат пакета ICMP.
4. Охарактеризуйте Address Resolution Protocol (ARP). Опишите формат пакета ARP.
5. Что такое MAC-адрес? Какова его структура?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—8].

Литература по теме

1. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014.
2. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series).
3. Королькова А. В., Кулябов Д. С. Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014.
4. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
5. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
7. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 6. Статическая маршрутизация VLAN

6.1. Цель работы

Настроить статическую маршрутизацию VLAN в сети.

6.2. Задание

1. Добавить в локальную сеть маршрутизатор, провести его первоначальную настройку.
2. Настроить статическую маршрутизацию VLAN.

6.3. Последовательность выполнения работы

1. В логической области проекта разместить маршрутизатор Cisco 2811, подключить его к порту 24 коммутатора `msk-donskaya-sw-1` в соответствии с таблицей портов (см. табл. 3.3 из раздела 3.3).
2. Используя приведённую ниже последовательность команд по первоначальной настройке маршрутизатора, сконфигурируйте маршрутизатор, задав на нём имя, пароль для доступа к консоли, настройте удалённое подключение к нему по ssh.
3. Настройте порт 24 коммутатора `msk-donskaya-sw-1` как trunk-порт.
4. На интерфейсе `f0/0` маршрутизатора `msk-donskaya-gw-1` настройте виртуальные интерфейсы, соответствующие номерам VLAN. Согласно таблице IP-адресов (см. табл. 3.2 из раздела 3.3) задайте соответствующие IP-адреса на виртуальных интерфейсах. Для этого используйте приведённую ниже последовательность команд по конфигурации VLAN-интерфейсов маршрутизатора.
5. Проверьте доступность конечных устройств из разных VLAN.
6. Используя режим симуляции в Packet Tracer, изучите процесс передвижения пакета ICMP по сети. Изучите содержимое передаваемого пакета и заголовки задействованных протоколов.

6.3.1. Первичная конфигурация маршрутизатора

```
Router>enable
Router#configure terminal

Router(config)#hostname msk-donskaya-gw-1

msk-donskaya-gw-1(config)#line vty 0 4
msk-donskaya-gw-1(config-line)#password cisco
msk-donskaya-gw-1(config-line)#login

msk-donskaya-gw-1(config)#line console 0
msk-donskaya-gw-1(config-line)#password cisco
msk-donskaya-gw-1(config-line)#login

msk-donskaya-gw-1(config)#enable secret cisco
msk-donskaya-gw-1(config)#service password-encryption
```

```
msk-donskaya-gw-1(config)#username admin privilege 1 secret cisco

msk-donskaya-gw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-gw-1(config)#crypto key generate rsa
msk-donskaya-gw-1(config)#line vty 0 4
msk-donskaya-gw-1(config-line)#transport input ssh
```

6.3.2. Конфигурация VLAN-интерфейсов маршрутизатора

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface f0/0
msk-donskaya-gw-1(config-if)#no shutdown

msk-donskaya-gw-1(config)#interface f0/0.2
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 2
msk-donskaya-gw-1(config-subif)#ip address 10.128.1.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description management

msk-donskaya-gw-1(config)#interface f0/0.3
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 3
msk-donskaya-gw-1(config-subif)#ip address 10.128.0.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description servers

msk-donskaya-gw-1(config-subif)#interface f0/0.101
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 101
msk-donskaya-gw-1(config-subif)#ip address 10.128.3.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description dk

msk-donskaya-gw-1(config-subif)#interface f0/0.102
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 102
msk-donskaya-gw-1(config-subif)#ip address 10.128.4.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description departments

msk-donskaya-gw-1(config-subif)#interface f0/0.103
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 103
msk-donskaya-gw-1(config-subif)#ip address 10.128.5.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description adm

msk-donskaya-gw-1(config-subif)#interface f0/0.104
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 104
msk-donskaya-gw-1(config-subif)#ip address 10.128.6.1 255.255.255.0
msk-donskaya-gw-1(config-subif)#description other
```

6.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

6.5. Контрольные вопросы

1. Охарактеризуйте стандарт IEEE 802.1Q.
2. Опишите формат кадра IEEE 802.1Q.

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1; 2].

Литература по теме

1. 802.1Q - Virtual LANs. — URL: <http://www.ieee802.org/1/pages/802.1Q.html>.
2. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: <http://www.ietf.org/rfc/rfc3069.txt>.

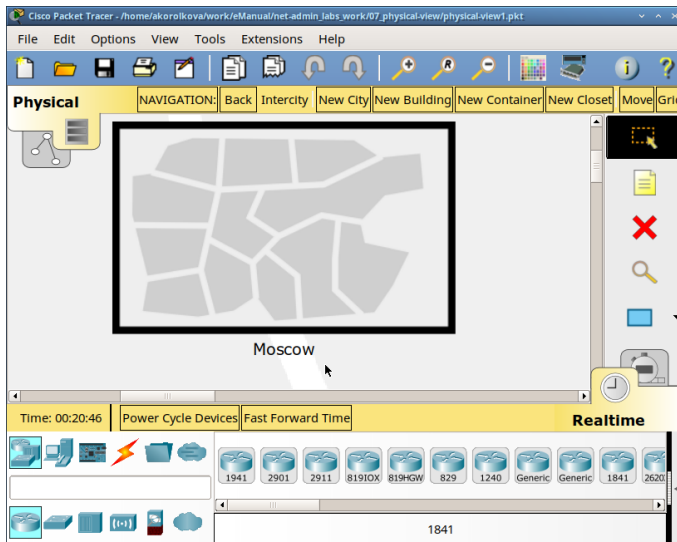


Рис. 7.2. Физическая рабочая область Packet Tracer

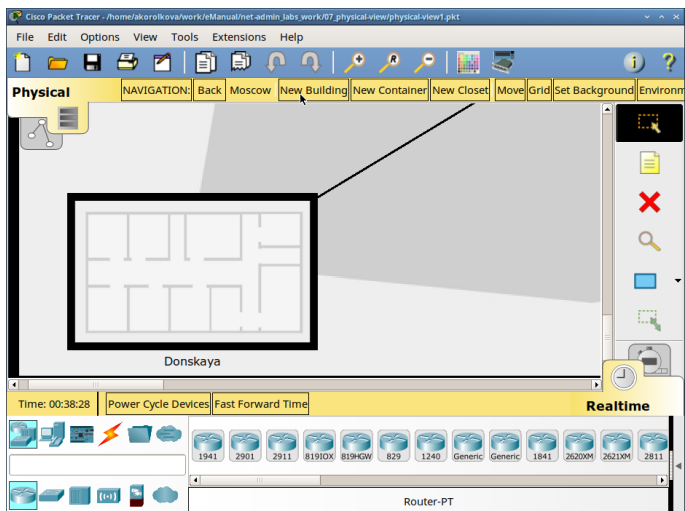


Рис. 7.3. Изображение здания в физической рабочей области Packet Tracer (сеть территории «Донская»)

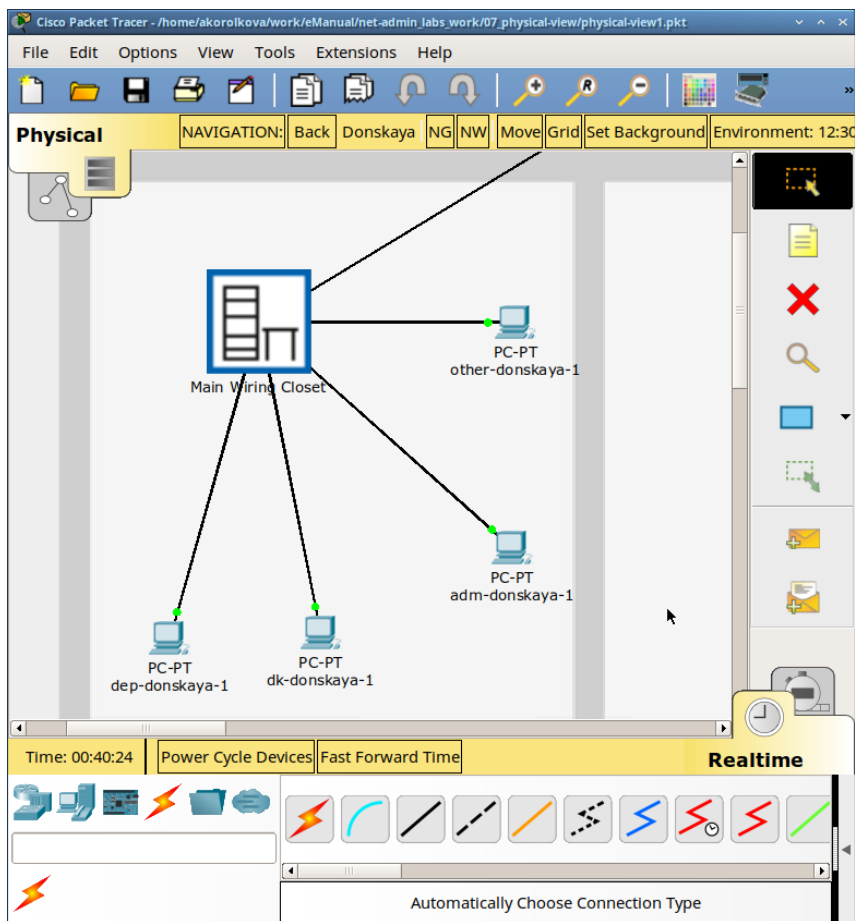


Рис. 7.4. Пример размещения в физической рабочей области Packet Tracer серверной с подключением оконечных устройств (сеть территории «Донская»)

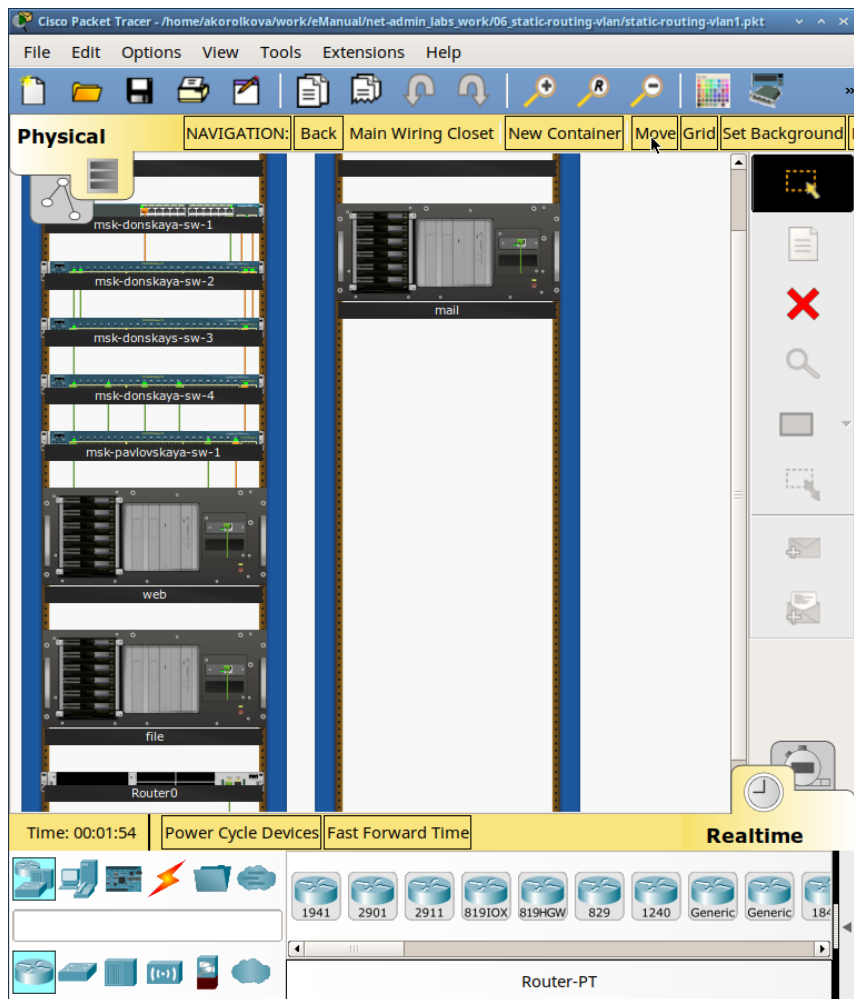


Рис. 7.5. Отображение серверных стоек в Packet Tracer

6. Переместите коммутатор `msk-pavlovskaya-sw-1` и два оконечных устройства `dk-pavlovskaya-1` и `other-pavlovskaya-1` на территорию Pavlovskaya, используя меню **Move** физической рабочей области Packet Tracer.
7. Вернувшись в логическую рабочую область Packet Tracer, пропингуйте с коммутатора `msk-donskaya-sw-1` коммутатор `msk-pavlovskaya-sw-1`. Убедитесь в работоспособности соединения.
8. В меню **Options**, **Preferences** во вкладке **Interface** активируйте разрешение на учёт физических характеристик среды передачи (Enable Cable Length Effects).
9. В физической рабочей области Packet Tracer разместите две территории на расстоянии более 100 м друг от друга (рекомендуемое расстояние — около 1000 м или более).
10. Вернувшись в логическую рабочую область Packet Tracer, пропингуйте с коммутатора `msk-donskaya-sw-1` коммутатор `msk-pavlovskaya-sw-1`. Убедитесь в неработоспособности соединения.
11. Удалите соединение между `msk-donskaya-sw-1` и `msk-pavlovskaya-sw-1`. Добавьте в логическую рабочую область два повторителя (Repeater-PT). Присвойте им соответствующие названия `msk-donskaya-mc-1` и `msk-pavlovskaya-mc-1`. Замените имеющиеся модули на PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE для подключения оптоволокну и витой пары по технологии Fast Ethernet (рис. 7.6).

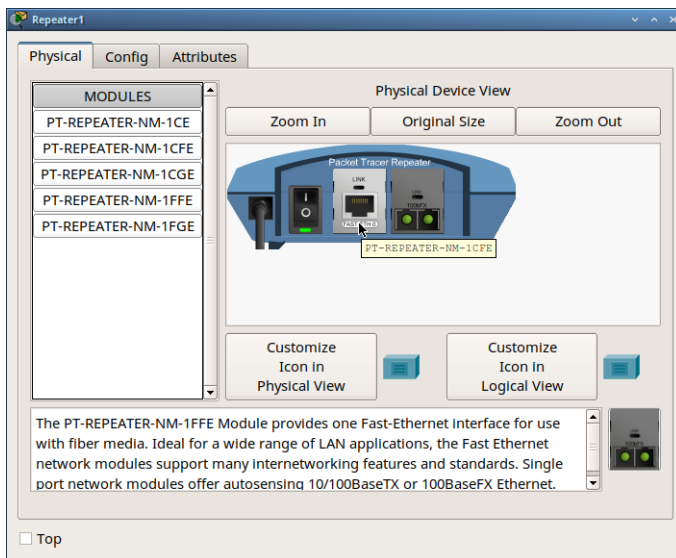


Рис. 7.6. Повторитель с портами PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE для подключения оптоволокну и витой пары по технологии Fast Ethernet

12. Переместите msk-pavlovskaya-мс-1 на территорию Pavlovskaya (в физической рабочей области Packet Tracer).
13. Подключите коммутатор msk-donskaya-sw-1 к msk-donskaya-мс-1 по витой паре, msk-donskaya-мс-1 и msk-pavlovskaya-мс-1 — по оптоволокну, msk-pavlovskaya-sw-1 к msk-pavlovskaya-мс-1 — по витой паре (рис. 7.7, рис. 7.8).

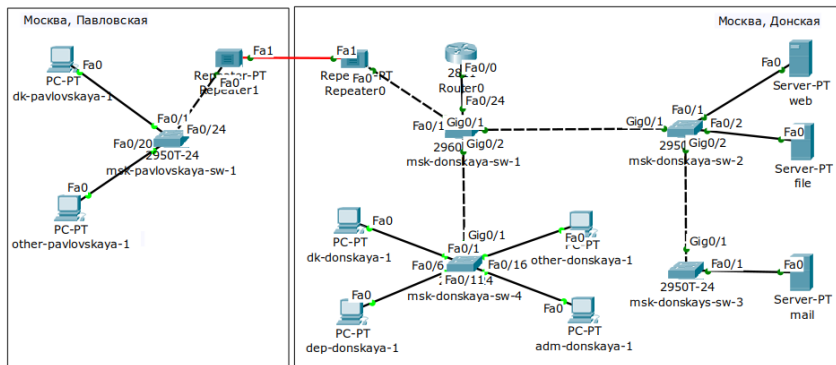


Рис. 7.7. Схема сети с учётом физических параметров сети в логической рабочей области Packet Tracer

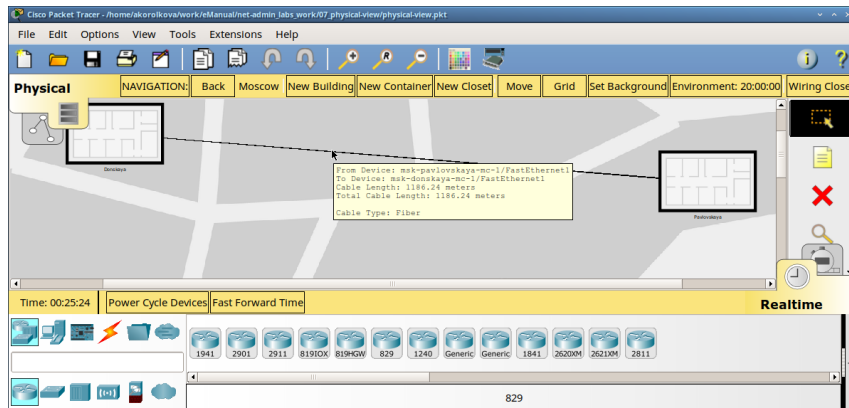


Рис. 7.8. Отображение соединения двух территорий в физической рабочей области Packet Tracer

14. Убедитесь в работоспособности соединения между msk-donskaya-sw-1 и msk-pavlovskaya-sw-1.

7.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

7.5. Контрольные вопросы

1. Перечислите возможные среды передачи данных. На какие характеристики среды передачи данных следует обращать внимание при планировании сети?
2. Перечислите категории витой пары. Чем они отличаются? Какая категория в каких условиях может применяться?
3. В чем отличие одномодового и многомодового оптоволокна? Какой тип кабеля в каких условиях может применяться?
4. Какие разъёмы встречаются на патчах оптоволокна? Чем они отличаются?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1–3].

Литература по теме

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
2. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 8. Настройка сетевых сервисов. DHCP

8.1. Цель работы

Приобретение практических навыков по настройке динамического распределения IP-адресов посредством протокола DHCP (Dynamic Host Configuration Protocol) [1] в локальной сети.

8.2. Задание

1. Добавить DNS-записи для домена `donskaya.rudn.ru` на сервер `dns`.
2. Настроить DHCP-сервис на маршрутизаторе.
3. Заменить в конфигурации оконечных устройствах статическое распределение адресов на динамическое.

8.3. Последовательность выполнения работы

1. В логическую рабочую область проекта добавьте сервер `dns` и подключите его к коммутатору `msk-donskaya-sw-3` через порт `Fa0/2` (рис. 8.1), не забыв активировать порт при помощи соответствующих команд на коммутаторе. В конфигурации сервера укажите в качестве адреса шлюза `10.128.0.1`, а в качестве адреса самого сервера — `10.128.0.5` с соответствующей маской `255.255.255.0`.

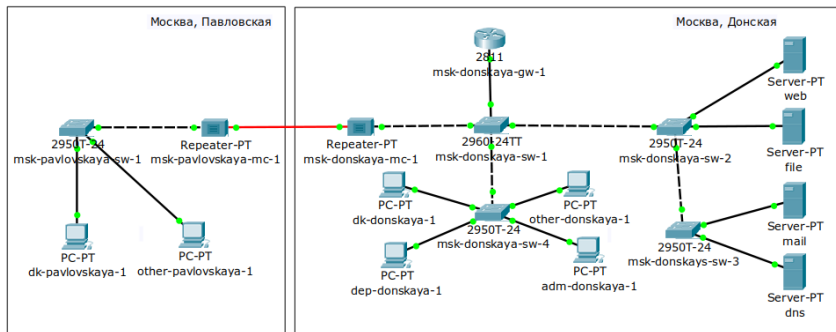


Рис. 8.1. Логическая схема локальной сети с добавленным DNS-сервером

2. Настройте сервис DNS (рис. 8.2):
 - в конфигурации сервера выберите службу DNS, активируйте её (выбрав флаг `On`);
 - в поле `Type` в качестве типа записи DNS выберите записи типа A (A Record);

- в поле Name укажите доменное имя, по которому можно обратиться, например, к web-серверу — `www.donskaya.rudn.ru`, затем укажите его IP-адрес в соответствующем поле `10.128.0.2`;
- нажав на кнопку `Add`, добавьте DNS-запись на сервер;
- аналогичным образом добавьте DNS-записи для серверов mail, file, dns согласно распределению адресов из табл. 3.2;
- сохраните конфигурацию сервера.

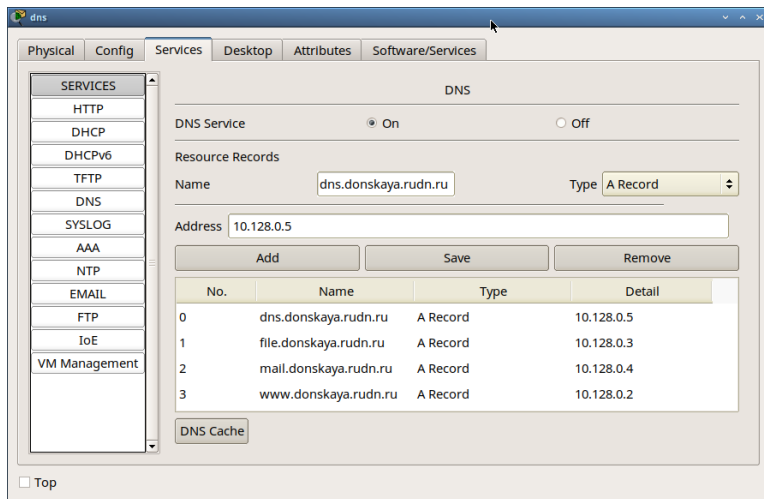


Рис. 8.2. Окно настройки сервиса DNS

3. Настройте DHCP-сервис на маршрутизаторе, используя приведённые ниже команды для каждой выделенной сети: укажите IP-адрес DNS-сервера; затем перейдите к настройке DHCP; задайте название конфигурируемому диапазону адресов (пулу адресов), укажите адрес сети, а также адреса шлюза и DNS-сервера; задайте пулы адресов, исключаемых из динамического распределения (см. табл. 3.2).

- Настройка DHCP:

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip name-server 10.128.0.5

msk-donskaya-gw-1(config)#service dhcp

msk-donskaya-gw-1(config)#ip dhcp pool dk
msk-donskaya-gw-1(dhcp-config)#network 10.128.3.0 255.255.255.0
msk-donskaya-gw-1(dhcp-config)#default-router 10.128.3.1
msk-donskaya-gw-1(dhcp-config)#dns-server 10.128.0.5
msk-donskaya-gw-1(dhcp-config)#exit
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.3.1 ←
10.128.3.29
```

```

msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.3.200 ←
10.128.3.254

msk-donskaya-gw-1(config)#ip dhcp pool departments
msk-donskaya-gw-1(dhcp-config)#network 10.128.4.0 255.255.255.0
msk-donskaya-gw-1(dhcp-config)#default-router 10.128.4.1
msk-donskaya-gw-1(dhcp-config)#dns-server 10.128.0.5
msk-donskaya-gw-1(dhcp-config)#exit
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.4.1 ←
10.128.4.29
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.4.200 ←
10.128.4.254

msk-donskaya-gw-1(config)#ip dhcp pool adm
msk-donskaya-gw-1(dhcp-config)#network 10.128.5.0 255.255.255.0
msk-donskaya-gw-1(dhcp-config)#default-router 10.128.5.1
msk-donskaya-gw-1(dhcp-config)#dns-server 10.128.0.5
msk-donskaya-gw-1(dhcp-config)#exit
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.4.5 ←
10.128.5.29
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.5.200 ←
10.128.5.254

msk-donskaya-gw-1(config)#ip dhcp pool other
msk-donskaya-gw-1(dhcp-config)#network 10.128.6.0 255.255.255.0
msk-donskaya-gw-1(dhcp-config)#default-router 10.128.6.1
msk-donskaya-gw-1(dhcp-config)#dns-server 10.128.0.5
msk-donskaya-gw-1(dhcp-config)#exit
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.6.1 ←
10.128.6.29
msk-donskaya-gw-1(config)#ip dhcp excluded-address 10.128.6.200 ←
10.128.6.254

```

– Информация о пулах DHCP:

```
msk-donskaya-gw-1#sh ip dhcp pool
```

– Информация об привязках выданных адресов:

```
msk-donskaya-gw-1#sh ip dhcp binding
```

4. На оконечных устройствах замените в настройках статическое распределение адресов на динамическое.
5. Проверьте, какие адреса выделяются оконечным устройствам, а также доступность устройств из разных подсетей.
6. В режиме симуляции изучите, каким образом происходит запрос адреса по протоколу DHCP (какие сообщения и какие отклики передаются по сети).

8.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).

4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

8.5. Контрольные вопросы

1. За что отвечает протокол DHCP?
2. Какие типы DHCP-сообщений передаются по сети?
3. Какие параметры могут быть переданы в сообщениях DHCP?
4. Что такое DNS?
5. Какие типы записи описания ресурсов есть в DNS и для чего они используются?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1–6].

Литература по теме

1. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03/1997. — P. 1–45. — No. 2136. — DOI: 10.17487/rfc2131.
2. *Королькова А. В., Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012.
3. *Королькова А. В., Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012.
4. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
5. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
6. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).

Лабораторная работа № 9. Использование протокола STP. Агрегирование каналов

9.1. Цель работы

Изучение возможностей протокола STP и его модификаций по обеспечению отказоустойчивости сети, агрегированию интерфейсов и перераспределению нагрузки между ними.

9.2. Предварительные сведения

9.2.1. Протокол STP

Основное назначение протокола STP (Spanning Tree Protocol, протокол остовного дерева) — устранение петель в топологии сети на базе технологии Ethernet при наличии избыточных соединений.

Протокол STP функционирует на канальном уровне модели OSI, его описание приведено в стандарте IEEE 802.1d [1]. В основе работы протокола лежит одноимённый алгоритм — Spanning Tree Algorithm (STA, алгоритм остовного дерева).

Принцип работы протокола STP заключается в следующем:

- одно из коммутационных устройств сети, являющееся частью топологии сети с избыточными соединениями, выбирается в качестве корневого устройства (Root Bridge);
- на основе алгоритма остовного дерева остальные коммутаторы сети определяют для себя так называемые «корневые порты» (Root Port) — порты, считающиеся по определённой метрике ближайшими относительно корневого устройства;
- остальные сетевые порты, имеющие соединение с корневым устройством, блокируются.

9.2.2. Bridge Protocol Data Unit

Во время функционирования протокола STP устройства сети обмениваются сообщениями BPDU (Bridge Protocol Data Unit), определёнными в стандарте IEEE 802.1d.

BPDU содержит следующие поля:

- идентификатор версии протокола STP (Protocol Identifier, 2 байта);
- номер версии протокола STP (Version, 1 байт);
- тип BPDU (Message Type, 1 байт) — конфигурационный (Configuration BPDU) или уведомляющий об изменении топологии (Topology Change Notification BPDU);
- флаги (Flags, 1 байт):
 - TC (Topology Change) — 1-й по порядку бит в поле флагов — указание на изменение топологии;
 - TCA (Topology Change Acknowledgment) — 8-й по порядку бит в поле флагов — подтверждение получения пакета BPDU с установленным битом TC;
- идентификатор корневого устройства (Root Bridge ID или Root ID, 8 байт);

- расстояние до корневого устройства (Root Path Cost, 4 байта);
- идентификатор отправителя (Bridge ID или Switch ID, 8 байт);
- идентификатор порта (Port ID, 2 байта);
- время жизни сообщения (Message Age, 2 байта);
- максимальное время жизни сообщения (Maximum Age, 2 байта);
- интервал hello (Hello Time, 2 байта) — интервал, через который посылаются пакеты BPDU;
- задержка смены состояний (Forward Delay, 2 байта) — минимальное время перехода коммутатора из активного в пассивное состояние, и наоборот.

9.2.3. Типы состояний портов, работающих по протоколу STP

Определены 4 типа состояний портов, работающих по протоколу STP:

- порт блокирован (Blocking State) — порт не участвует в обмене сообщениями;
- порт в состоянии прослушивания (Listening State) — осуществляется приём BPDU, но не происходит определения места назначения, операций фильтрации и передачи пользовательской информации; возможен переход порта в состояние блокировки или обучения;
- порт в состоянии обучения (Learning State) — состояние, предшествующее переходу в состояние передачи (при этом запоминается расположение ближайших устройств и обновление адресной таблицы);
- порт в состоянии передачи (Forwarding State) — порт участвует в обмене сообщениями, определении расположения станций в сети, фильтрации данных и передаче пользовательского трафика.

9.2.4. Модификации STP

Протокол Rapid Spanning Tree Protocol (RSTP) описан в документах IEEE 802.1w-2001 и IEEE 802.1D-2004. По сравнению с STP реализует ускоренную реконфигурацию дерева для исключения петель, т.е. уменьшилось время построения топологии, а также время восстановления работоспособности сети при смене маршрута следования пакетов. Порт может находиться в одном из трёх состояний: Discarding, Learning, Forwarding.

Per-VLAN Spanning Tree Protocol (PVSTP) — проприетарное расширение протокола STP, разработанное компанией Cisco. Позволяет использовать отдельные настройки (экземпляры) протокола STP для разных VLAN. Работает только при использовании портов в режиме ISL-транк (проприетарный протокол компании Cisco для передачи информации о принадлежности трафика к определённому VLAN).

PVSTP+ — модификация PVSTP, работающая при использовании портов в режиме 802.1Q-транк (тегирование трафика для передачи информации о принадлежности к VLAN).

Rapid PVST+ — модификация, объединяющая свойства PVST+ и RSTP за счёт использования мультикастовых фреймов.

Multiple Spanning Tree Protocol (MSTP) — используется один экземпляр протокола для нескольких VLAN при условии идентичности их топологий. Протокол MSTP описан в документах IEEE 802.1s и 802.1Q-2003.

9.3. Задание

1. Сформируйте резервное соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-3`.
2. Настройте балансировку нагрузки между резервными соединениями.
3. Настройте режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы.
4. Изучите отказоустойчивость резервного соединения.
5. Сформируйте и настройте агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-4`.

9.4. Последовательность выполнения работы

1. Сформируйте резервное соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-3` (рис. 9.1). Для этого:
 - замените соединение между коммутаторами `msk-donskaya-sw-1` (Gig0/2) и `msk-donskaya-sw-4` (Gig0/1) на соединение между коммутаторами `msk-donskaya-sw-1` (Gig0/2) и `msk-donskaya-sw-3` (Gig0/2);
 - сделайте порт на интерфейсе Gig0/2 коммутатора `msk-donskaya-sw-3` транковым:

```
msk-donskaya-sw-3(config)#int g0/2
msk-donskaya-sw-3(config-if)#switchport mode trunk
```

- соединение между коммутаторами `msk-donskaya-sw-1` и `msk-donskaya-sw-4` сделайте через интерфейсы Fa0/23, не забыв активировать их в транковом режиме.

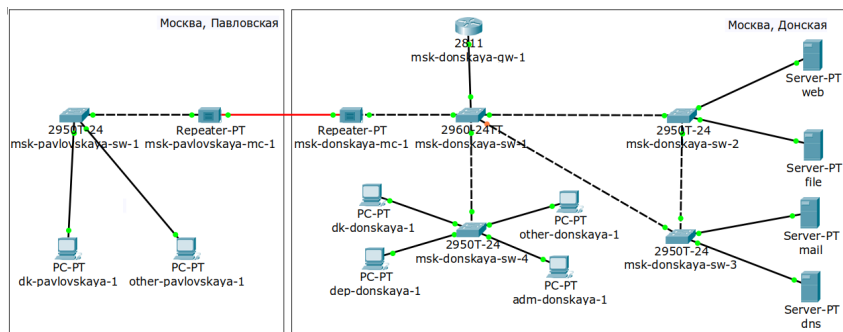


Рис. 9.1. Логическая схема локальной сети с резервным соединением

2. С оконечного устройства `dk-donskaya-1` пропингуйте серверы `mail` и `web`. В режиме симуляции проследите движение пакетов ICMP. Убедитесь, что движение пакетов происходит через коммутатор `msk-donskaya-sw-2`.
3. На коммутаторе `msk-donskaya-sw-2` посмотрите состояние протокола STP для vlan 3:

```
msk-donskaya-sw-2#show spanning-tree vlan 3
```

В результате будет выведена примерно следующая информация, связанная с протоколом STP:

```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    32771
            Address     0001.9698.29B8
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771 (priority 32768 sys-id-ext 3)
            Address     0001.9698.29B8
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Gi0/1	Desg	FWD	4	128.25	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Gi0/2	Desg	FWD	4	128.26	P2p

Здесь, в частности, указывается, что данное устройство является корневым (строка `This bridge is the root`).

4. В качестве корневого коммутатора STP настройте коммутатор `msk-donskaya-sw-1`:

```
msk-donskaya-sw-1#configure terminal
msk-donskaya-sw-1(config)#spanning-tree vlan 3 root primary
```

5. Используя режим симуляции, убедитесь, что пакеты ICMP пойдут от хоста `dk-donskaya-1` до `mail` через коммутаторы `msk-donskaya-sw-1` и `msk-donskaya-sw-3`, а от хоста `dk-donskaya-1` до `web` через коммутаторы `msk-donskaya-sw-1` и `msk-donskaya-sw-2`.
6. Настройте режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы:

```
msk-donskaya-sw-2(config)#interface f0/1
msk-donskaya-sw-2(config-if)#spanning-tree portfast
```

```
msk-donskaya-sw-2(config)#interface f0/2
msk-donskaya-sw-2(config-if)#spanning-tree portfast
```

```
msk-donskaya-sw-3(config)#interface f0/1
msk-donskaya-sw-3(config-if)#spanning-tree portfast
```

```
msk-donskaya-sw-3(config)#interface f0/2
msk-donskaya-sw-3(config-if)#spanning-tree portfast
```

7. Изучите отказоустойчивость протокола STP и время восстановления соединения при переключении на резервное соединение. Для этого используйте команду `ping -n 1000 mail.donskaya.rudn.ru` на хосте `dk-donskaya-1`, а разрыв соединения обеспечьте переводом соответствующего интерфейса коммутатора в состояние `shutdown`.
8. Переключите коммутаторы режим работы по протоколу Rapid PVST+:

```
msk-donskaya-sw-1(config)#spanning-tree mode rapid-pvst
msk-donskaya-sw-2(config)#spanning-tree mode rapid-pvst
msk-donskaya-sw-3(config)#spanning-tree mode rapid-pvst
```

```
msk-donskaya-sw-4(config)#spanning-tree mode rapid-pvst
msk-pavlovskaya-sw-1(config)#spanning-tree mode rapid-pvst
```

9. Изучите отказоустойчивость протокола Rapid PVST+ и время восстановления соединения при переключении на резервное соединение.
10. Сформируйте агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами msk-donskaya-sw-1 и msk-donskaya-sw-4 (рис. 9.2).

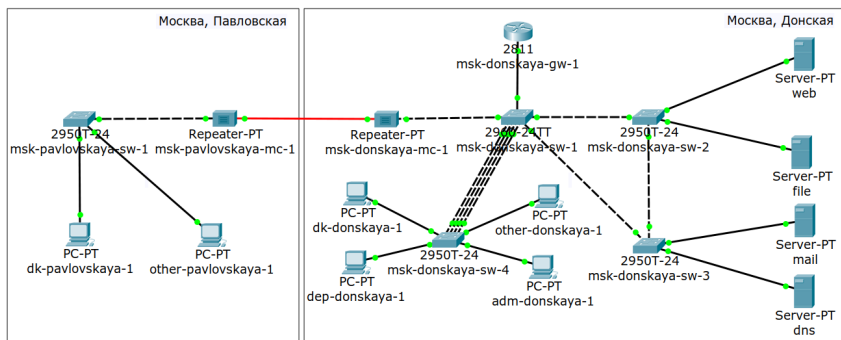


Рис. 9.2. Логическая схема локальной сети с агрегированным соединением

11. Настройте агрегирование каналов (режим EtherChannel):

```
msk-donskaya-sw-1(config)#interface range f0/20 - 23
msk-donskaya-sw-1(config-if-range)#channel-group 1 mode on
msk-donskaya-sw-1(config-if-range)#exit
msk-donskaya-sw-1(config)#interface port-channel 1
msk-donskaya-sw-1(config-if)#switchport mode trunk

msk-donskaya-sw-4(config)#int range f0/20 - 23
msk-donskaya-sw-4(config-if-range)#no switchport access vlan 104
msk-donskaya-sw-4(config-if-range)#exit

msk-donskaya-sw-4(config)#interface range f0/20 - 23
msk-donskaya-sw-4(config-if-range)#channel-group 1 mode on
msk-donskaya-sw-4(config-if-range)#exit
msk-donskaya-sw-4(config)#interface port-channel 1
msk-donskaya-sw-4(config-if)#switchport mode trunk
```

Здесь использована следующая терминология Cisco:

- **EtherChannel** — технология агрегирования каналов;
- **port-channel** — логический интерфейс, который объединяет физические интерфейсы;
- **channel-group** — команда, которая указывает, какому логическому интерфейсу принадлежит физический интерфейс и какой режим используется для агрегирования;
- возможные параметры **channel-group**:
 - **active** — включить LACP;
 - **passive** — включить LACP, только если придёт сообщение LACP;
 - **desirable** — включить PAgP;

- **auto** — включить PAgP, только если придёт сообщение PAgP;
- **on** — включить только EtherChannel.

9.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

9.6. Контрольные вопросы

1. Какую информацию можно получить, воспользовавшись командой определения состояния протокола STP для VLAN (на корневом и не на корневом устройстве)? Приведите примеры вывода подобной информации на устройствах.
2. При помощи какой команды можно узнать, в каком режиме, STP или Rapid PVST+, работает устройство? Приведите примеры вывода подобной информации на устройствах.
3. Для чего и в каких случаях нужно настраивать режим Portfast?
4. В чем состоит принцип работы агрегированного интерфейса? Для чего он используется?
5. В чём принципиальные отличия при использовании протоколов LACP (Link Aggregation Control Protocol), PAgP (Port Aggregation Protocol) и статического агрегирования без использования протоколов?
6. При помощи каких команд можно узнать состояние агрегированного канала EtherChannel?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1; 2].

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : tech. rep. / IEEE. — 2004. — P. 1-277. — DOI: 10.1109/IEEESTD.2004.94569.
2. Хилл Б. Полный справочник по Cisco. — М. : Вильямс, 2009.

Лабораторная работа № 10. Настройка списков управления доступом (ACL)

10.1. Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

10.2. Задание

1. Требуется настроить следующие правила доступа:
 - 1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
 - 2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
 - 3) почтовый сервер: разрешить пользователям работать по протоколам SMTP и POP3 (соответственно через порты 25 и 110 протокола TCP), а для администратора — открыть доступ по протоколам Telnet и FTP;
 - 4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
 - 5) разрешить icmp-сообщения, направленные в сеть серверов;
 - 6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;
 - 7) разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
2. Требуется проверить правильность действия установленных правил доступа.
3. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.

10.3. Последовательность выполнения работы

В рабочей области проекта подключите ноутбук администратора с именем `admin` к сети `other-donskaya-1` с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоедините ноутбук к порту 24 коммутатора `msk-donskaya-sw-4` и присвойте ему статический адрес `10.128.6.200`, указав в качестве gateway-адреса `10.128.6.1` и адреса DNS-сервера `10.128.0.5` (рис. 10.1).

Права доступа пользователей сети (см. рис. 9.2) будем настраивать на маршрутизаторе `msk-donskaya-gw-1`, поскольку именно через него проходит весь трафик сети. Ограничения можно накладывать как на входящий (in), так и на исходящий (out) трафик. По отношению к маршрутизатору накладываемые ограничения будут касаться в основном исходящего трафика.

Различают стандартные (standard) и расширенные (extended) списки контроля доступа (Access Control List, ACL). Стандартные ACL проверяют только адрес источника трафика, расширенные — адрес как источника, так и получателя, тип протокола и TCP/UDP порты.

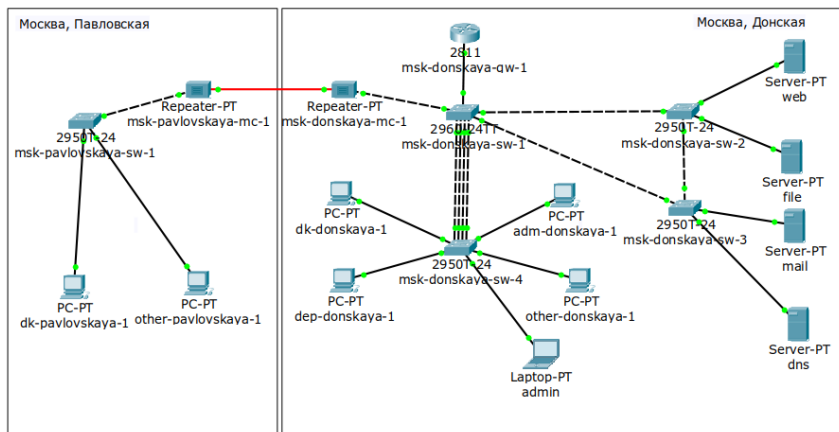


Рис. 10.1. Размещение ноутбука администратора в сети other-donskaya-1

Следует помнить, что на оборудовании Cisco правила в списке доступа проверяются по порядку сверху вниз до первого совпадения — как только одно из правил сработало, проверка списка правил прекращается и обработка трафика происходит на основе сработавшего правила. Поэтому рекомендуется сначала дать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Кроме того, после всех правил в конце дописывается неявное запрещение на всё, что не разрешено: `deny ip any any` (implicit deny).

1. Настройка доступа к web-серверу по порту tcp 80:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark web
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
```

Здесь: создан список контроля доступа с названием **servers-out** (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указано (в качестве комментария-напоминания **remark web**), что ограничения предназначены для работы с web-сервером; дано разрешение доступа (**permit**) по протоколу TCP всем (**any**) пользователям сети (**host**) на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80.

2. Добавление списка управления доступом к интерфейсу:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#interface f0/0.3
msk-donskaya-gw-1(config-subif)#ip access-group servers-out out
```

Здесь: к интерфейсу **f0/0.3** подключается список прав доступа **servers-out** и применяется к исходящему трафику (**out**).

Можно проверить, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера). При этом команда

ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера.

3. Дополнительный доступ для администратора по протоколам Telnet и FTP:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp ←
msk-donskaya-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet ←
```

Здесь: в список контроля доступа servers-out добавлено правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet.

Убедитесь, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введите ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. 10.2).

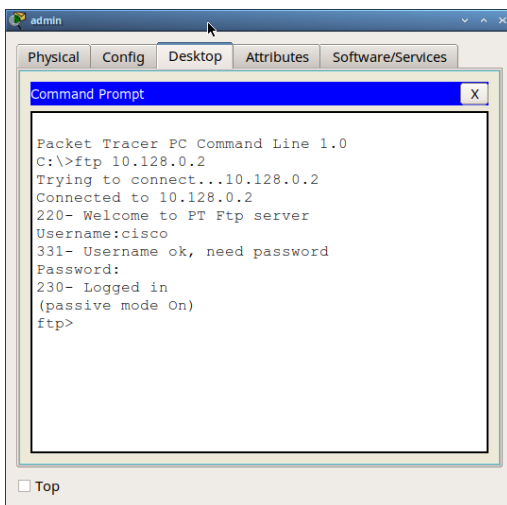


Рис. 10.2. Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Попробуйте провести аналогичную процедуру с другого устройства сети. Убедитесь, что доступ будет запрещён.

4. Настройка доступа к файловому серверу:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark file
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445 ←
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp ←
```

Здесь: в списке контроля доступа **servers-out** указано (в качестве комментария-напоминания **remark file**), что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

5. Настройка доступа к почтовому серверу:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark mail
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
```

Здесь: в списке контроля доступа **servers-out** указано (в качестве комментария-напоминания **remark mail**), что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP.

6. Настройка доступа к DNS-серверу:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark dns
msk-donskaya-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 ←
    host 10.128.0.5 eq 53
```

Здесь: в списке контроля доступа **servers-out** указано (в качестве комментария-напоминания **remark dns**), что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53.

Проверьте доступность web-сервера (через браузер) не только по ip-адресу, но и по имени.

7. Разрешение icmp-запросов:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#1 permit icmp any any
```

Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Номера строк правил в списке контроля доступа можно посмотреть с помощью команды

```
msk-donskaya-gw-1#show access-lists
```

8. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору **msk-donskaya-gw-1** является входящим трафиком):

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended other-in
msk-donskaya-gw-1(config-ext-nacl)#remark admin
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-gw-1(config-ext-nacl)#exit
msk-donskaya-gw-1(config-subif)#interface f0/0.104
msk-donskaya-gw-1(config-subif)#ip access-group other-in in
```

Здесь: в списке контроля доступа **other-in** указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с

адресом 10.128.6.200 на любые действия (**any**); к интерфейсу f0/0.104 подключается список прав доступа **other-in** и применяется к входящему трафику (**in**).

9. Настройка доступа администратора к сети сетевого оборудования:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended management-out
msk-donskaya-gw-1(config-ext-nacl)#remark admin
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 ←
10.128.1.0 0.0.0.255
msk-donskaya-gw-1(config-ext-nacl)#exit
msk-donskaya-gw-1(config)#interface f0/0.2
msk-donskaya-gw-1(config-subif)#ip access-group management-out out
```

Здесь: в списке контроля доступа **management-out** указано (в качестве комментария-напоминания **remark admin**), что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключается список прав доступа **management-out** и применяется к исходящему трафику (**out**).

10.4. Самостоятельная работа

1. Проверьте корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования.
2. Разрешите администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

10.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

10.6. Контрольные вопросы

1. Как задать действие правила для конкретного протокола?
2. Как задать действие правила сразу для нескольких портов?
3. Как узнать номер правила в списке прав доступа?
4. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Лабораторная работа № 11. Настройка NAT. Планирование

11.1. Цель работы

Провести подготовительные мероприятия по подключению локальной сети организации к Интернету.

11.2. Предварительные сведения

Network Address Translation (NAT) — механизм преобразования IP-адресов транзитных пакетов.

В частности, механизм NAT используется для обеспечения доступа устройств локальных сетей с внутренними IP-адресами к сети Интернет (рис. 11.1).



Рис. 11.1. Схема сети с NAT

Типы NAT:

- *статический NAT (Static NAT, SNAT)* — осуществляет преобразование адресов по принципу 1:1 (в частности, один локальный IP-адрес преобразуется во внешний адрес, выделенный, например, провайдером);
- *динамический NAT (Dynamic NAT, DNAT)* — осуществляет преобразование адресов по принципу 1:N (например, один адрес устройства локальной сети преобразуется в один из адресов диапазона внешних адресов);
- *NAT Overload (или NAT Masquerading, или Port Address Translation, PAT)* — осуществляет преобразование адресов по принципу N:1 (например, адреса группы устройств локальной подсети преобразуются в один внешний адрес, при этом дополнительно используется механизм адресации через номера портов).

11.3. Задание

1. Построить схему подключения локальной сети к Интернету.
2. Построить модельные сети провайдера и сети Интернет (рис. 11.2).
3. Построить схемы сетей L1, L2, L3.

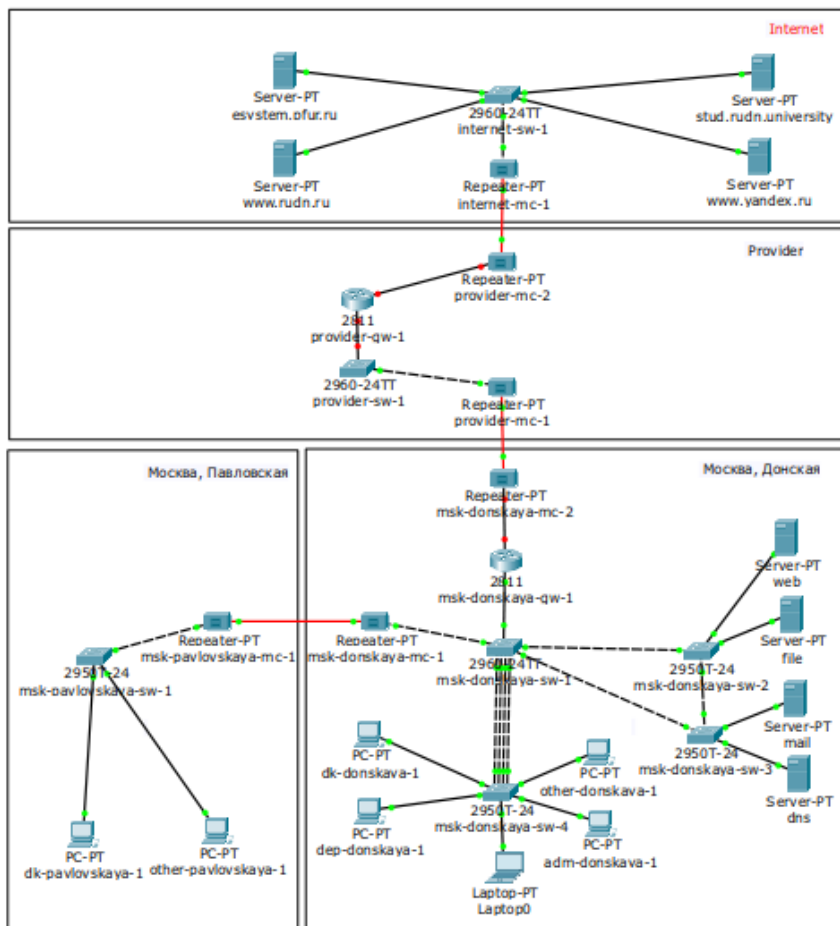


Рис. 11.2. Схема сети с выходом в Интернет

Модельные предположения:

- В сети провайдера располагаются 2 медиаконвертера provider-mc-1 и provider-mc-2 для связи с подсетью «Донская» и сетью модельного

Интернета, маршрутизатор `provider-gw-1` и коммутатор `provider-sw-1`. Оборудование соединяется между собой по Fast Ethernet согласно схеме (рис. 11.2).

- В модельной сети Интернет располагаются 4 сервера `www.yandex.ru`, `www.rudn.ru`, `stud.rudn.university` и `esystem.pfur.ru`, коммутатор `internet-sw-1` и медиаконвертер `internet-mc-1` для связи с сетью провайдера. Серверы подключены к коммутатору посредством Fast Ethernet, коммутатор подсоединён к медиаконвертеру также по Fast Ethernet (см. рис. 11.2).
- Имена и адреса серверам Интернет и маршрутизатору провайдера задаются согласно табл. 11.1. При этом учитывается, что под сеть адресов модельного Интернет выделяется адрес 192.0.2.0/24, а под сеть провайдера — 198.51.100.1 (как рекомендовано в [1] для использования в примерах и документации при описании тестовых сетей).

Таблица 11.1

Распределение ip-адресов модельного Интернет

IP-адреса	Примечание
192.0.2.1	provider-gw-1
192.0.2.11	www.yandex.ru
192.0.2.12	stud.rudn.university
192.0.2.13	esystem.pfur.ru
192.0.2.14	www.rudn.ru

11.4. Последовательность выполнения работы

1. Внесите изменения в схему L1 сети, добавив в неё сеть провайдера и сеть модельного Интернет с указанием названий оборудования и портов подключения.
2. Внесите изменения в схемы L2 и L3 сети, указав адреса и VLAN сети провайдера и модельной сети Интернет. Скорректируйте таблицы распределения IP-адресов и портов.
3. На схеме предыдущего вашего проекта разместите согласно рис. 11.2 необходимое оборудование для сети провайдера и сети модельного Интернет: 4 медиаконвертера (Repeater-PT), 2 коммутатора типа Cisco 2960-24TT, маршрутизатор типа Cisco 2811, 4 сервера.
4. Присвойте названия размещённым в сети провайдера и в сети модельного Интернет объектам согласно модельным предположениям и схеме L1.
5. В физической рабочей области добавьте здание провайдера и здание, имитирующее расположение серверов модельного Интернет (рис. 11.3). Присвойте им соответствующие названия.
6. Перенесите из сети «Донская» оборудование провайдера (рис. 11.4) и модельной сети Интернет (рис. 11.5) в соответствующие здания.

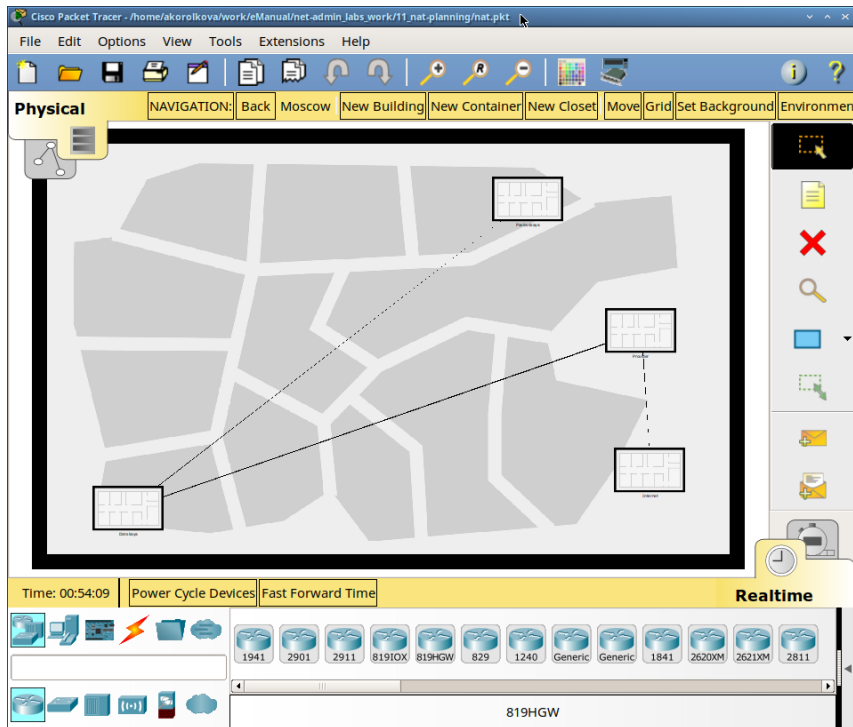


Рис. 11.3. Схема сети в физической рабочей области Packet Tracer

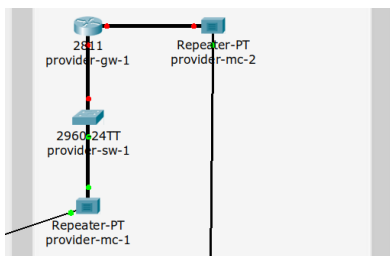


Рис. 11.4. Оборудование в здании сети провайдера

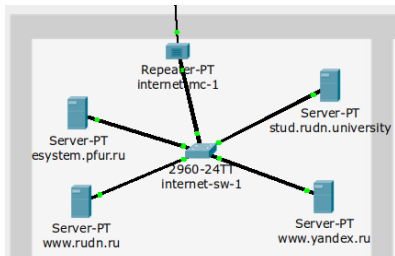


Рис. 11.5. Оборудование в здании сети модельного Интернета

7. На медиаконвертерах замените имеющиеся модули на PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE для подключения витой пары по технологии Fast Ethernet и оптоволокна соответственно (рис. 11.6).

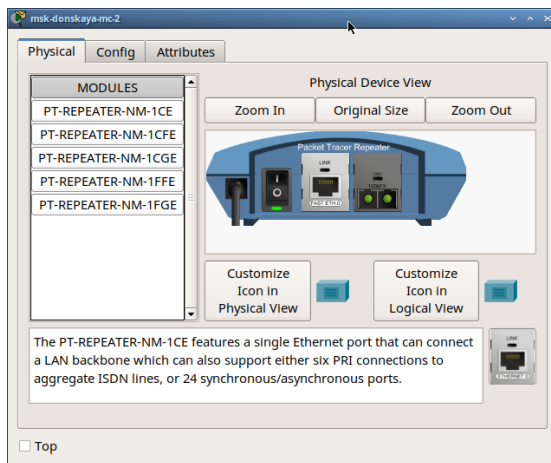


Рис. 11.6. Медиаконвертер с модулями PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE

8. Проведите соединение объектов согласно скорректированной Вами схеме L1.
9. Пропишите IP-адреса серверам согласно табл. 11.1.
10. Пропишите сведения о серверах на DNS-сервере сети «Донская» (рис. 11.7).

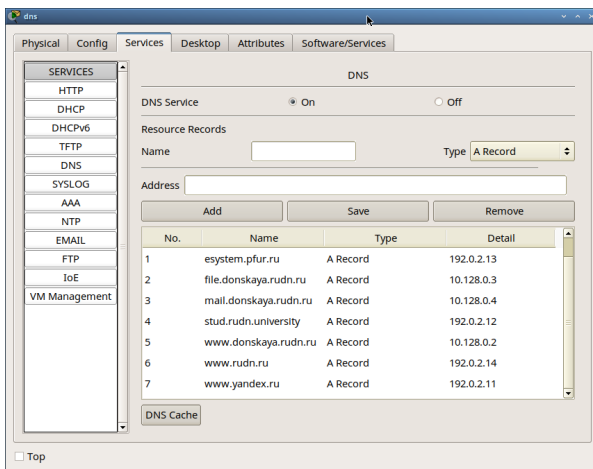


Рис. 11.7. DNS-записи на сервере DNS в сети «Донская»

11.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания, схемы L1, L2, L3, таблицы VLAN, IP-адресов и портов подключения оборудования с комментариями.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

11.6. Контрольные вопросы

1. Что такое Network Address Translation (NAT)?
2. Как определить, находится ли узел сети за NAT?
3. Какое оборудование отвечает за преобразование адреса методом NAT?
4. В чём отличие статического, динамического и перегруженного NAT?
5. Охарактеризуйте типы NAT.

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [2—4].

Литература по теме

1. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01/2010. — P. 1–11. — No. 5735. — DOI: 10.17487/rfc5735.
2. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
3. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
4. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.

Лабораторная работа № 12. Настройка NAT

12.1. Цель работы

Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT.

12.2. Постановка задачи

Требуется подключить локальную сеть организации к сети Интернет (распределение внешних ip-адресов дано в табл. 12.1) с учётом ограничений, накладываемых на определённые подсети локальной сети (VLAN подсетей даны в табл. 12.2):

- 1) сеть управления устройствами не должна иметь доступ в Интернет;
- 2) оконечные устройства сети дисплейных классов должны иметь доступ только к сайтам, необходимым для учёбы (в данном случае к www.yandex.ru, stud.rudn.university);
- 3) пользователям из сети кафедр разрешено работать только с образовательными сайтами (в данном случае это esystem.pfur.ru);
- 4) пользователям сети администрации разрешено работать только с сайтом университета www.rudn.ru;
- 5) в сети для других пользователей компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи — не должны выходить в Интернет;
- 6) ограничения для серверов:
 - WEB-сервер должен быть доступен по порту 80;
 - почтовый сервер должен быть доступен по портам 25 и 110;
 - файловый сервер должен быть доступен извне по портам протокола FTP;
- 7) компьютер администратора должен быть доступен из внешней сети по протоколу удалённого рабочего стола (Remote Desktop Protocol, RDP).

Таблица 12.1

Распределение внешних ip-адресов

IP-адреса	Примечание	VLAN
198.51.100.0/28	Выделено провайдером	4
198.51.100.1	Маршрутизатор провайдера	
198.51.100.2	msk-donskaya-gw-1	
198.51.100.2–198.51.100.14	Пул адресов для NAT	
198.51.100.2	Web	
198.51.100.3	File	
198.51.100.4	Mail	

Таблица 12.2

Таблица VLAN

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4	nat	Линк в Интернет
5-100		Зарезервировано
101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей

12.3. Задание

1. Сделать первоначальную настройку маршрутизатора **provider-gw-1** и коммутатора **provider-sw-1** провайдера: задать имя, настроить доступ по паролю и т.п. (см. разделы 12.4.1, 12.4.2).
2. Настроить интерфейсы маршрутизатора **provider-gw-1** и коммутатора **provider-sw-1** провайдера: (см. разделы 12.4.3, 12.4.4).
3. Настроить интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера (см. раздел 12.4.5).
4. Настроить на маршрутизаторе сети «Донская» NAT с правилами, указанными в разделе 12.2 (см. разделы 12.4.6–12.4.8).
5. Настроить доступ из внешней сети в локальную сеть организации, как указано в разделе 12.2 (см. раздел 12.4.9).
6. Проверить работоспособность заданных настроек.

12.4. Последовательность выполнения работы

12.4.1. Первоначальная настройка маршрутизатора **provider-gw-1**

```

provider-gw-1>enable
provider-gw-1#configure terminal

provider-gw-1(config)#line vty 0 4
provider-gw-1(config-line)#password cisco
provider-gw-1(config-line)#login
provider-gw-1(config-line)#exit

provider-gw-1(config)#line console 0
provider-gw-1(config-line)#password cisco
provider-gw-1(config-line)#login
provider-gw-1(config-line)#exit

provider-gw-1(config)#enable secret cisco
provider-gw-1(config)#service password-encryption

```

```
provider-gw-1(config)#username admin privilege 1 secret cisco
```

12.4.2. Первоначальная настройка коммутатора provider-sw-1

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#line vty 0 4
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit

provider-sw-1(config)#line console 0
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit

provider-sw-1(config)#enable secret cisco
provider-sw-1(config)#service password-encryption
provider-sw-1(config)#username admin privilege 1 secret cisco
```

12.4.3. Настройка интерфейсов маршрутизатора provider-gw-1

```
provider-gw-1>enable
provider-gw-1#configure terminal

provider-gw-1(config)#interface f0/0
provider-gw-1(config-if)#no shutdown
provider-gw-1(config-if)#exit

provider-gw-1(config)#interface f0/0.4
provider-gw-1(config-subif)#encapsulation dot1Q 4
provider-gw-1(config-subif)#ip address 198.51.100.1 255.255.255.240
provider-gw-1(config-subif)#description mks-donskaya
provider-gw-1(config-subif)#exit

provider-gw-1(config)#interface f0/1
provider-gw-1(config-if)#no shutdown
provider-gw-1(config-if)#ip address 192.0.2.1 255.255.255.0
provider-gw-1(config-if)#description internet
provider-gw-1(config-if)#exit
provider-gw-1(config)#exit
```

12.4.4. Настройка интерфейсов коммутатора provider-sw-1

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#interface f0/1
provider-sw-1(config-if)#switchport mode trunk
provider-sw-1(config-if)#exit

provider-sw-1(config)#interface f0/2
provider-sw-1(config-if)#switchport mode trunk
provider-sw-1(config-if)#exit

provider-sw-1(config)#vlan 4
provider-sw-1(config-vlan)#name nat
```

```

provider-sw-1(config-vlan)#exit

provider-sw-1(config)#interface vlan4
provider-sw-1(config-if)#no shutdown
provider-sw-1(config-if)#exit

```

В этой лабораторной работе можно использовать подключение маршрутизатора provider-gw-1 напрямую к медиаконвертеру provider-mc-1.

12.4.5. Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

```

msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface f0/1
msk-donskaya-gw-1(config-if)#no shutdown
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#interface f0/1.4
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 4
msk-donskaya-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-gw-1(config-subif)#description internet
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#exit

msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1
msk-donskaya-gw-1(config)#exit

```

12.4.6. Настройка пула адресов для NAT

```

msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip nat pool main-pool 198.51.100.2 ←
198.51.100.14 netmask 255.255.255.240

```

12.4.7. Настройка списка доступа для NAT

```

msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip access-list extended nat-inet

```

12.4.7.1. Сеть дисплейных классов

Хосты из сети дисплейных классов имеют доступ только к сайтам, необходимым для учёбы (www.yandex.ru (192.0.2.11), stud.rudn.university (192.0.2.12)).

```

msk-donskaya-gw-1(config-ext-nacl)#remark dk
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host ←
192.0.2.11 eq 80
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host ←
192.0.2.12 eq 80

```

12.4.7.2. Сеть кафедр

Сеть кафедр работает только с образовательными сайтами (`esystem.pfur.ru` (192.0.2.13)).

```
msk-donskaya-gw-1(config-ext-nacl)#remark departments
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.13 eq 80 ←
```

12.4.7.3. Сеть администрации

Сеть администрации имеет возможность работать только с сайтом университета (`www.rudn.ru` (192.0.2.14)).

```
msk-donskaya-gw-1(config-ext-nacl)#remark adm
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq 80 ←
```

12.4.7.4. Доступ для компьютера администратора

В сети для других пользователей компьютер администратора имеет полный доступ в Интернет. Другие не имеют доступа.

```
msk-donskaya-gw-1(config-ext-nacl)#remark admin
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
```

12.4.8. Настройка NAT

Настроить Port Address Translation (PAT)¹:

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip nat inside source list nat-inet pool ←
main-pool overload
```

Настройка интерфейсов для NAT:

```
msk-donskaya-gw-1(config)#int f0/0.3
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config)#interface f0/0.101
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.102
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.103
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/0.104
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#interface f0/1.4
msk-donskaya-gw-1(config-subif)#ip nat outside
msk-donskaya-gw-1(config-subif)#exit
```

¹Другие названия: NAT Overload, IP Masquerading, Many-to-One NAT, Network Address Port Translation (NAPT).

12.4.9. Настройка доступа из Интернета

12.4.9.1. WWW-сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80 ←  
198.51.100.2 80
```

12.4.9.2. Файловый сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 ←  
198.51.100.3 20  
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 ←  
198.51.100.3 21
```

12.4.9.3. Почтовый сервер

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25 ←  
198.51.100.4 25  
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.4 ←  
110 198.51.100.4 110
```

12.4.9.4. Доступ по RDP

Компьютер администратора доступен из Интернета по RDP.

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.6.200 ←  
3389 198.51.100.10 3389
```

12.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

12.6. Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)?
2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?
3. Можно ли применить Cisco IOS NAT к субинтерфейсам?
4. Что такое пулы IP NAT?
5. Что такое статические преобразования NAT?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1–5].

Литература по теме

1. NAT Order of Operation. — URL: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html>.
2. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
3. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
4. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009.
5. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.

Лабораторная работа № 13. Статическая маршрутизация в Интернете. Планирование

13.1. Цель работы

Провести подготовительные мероприятия по организации взаимодействия через сеть провайдера посредством статической маршрутизации локальной сети с сетью основного здания, расположенного в 42-м квартале в Москве, и сетью филиала, расположенного в г. Сочи.

13.2. Модельные предположения

Схема L1 сети с дополнительными площадками представлена на рис. 13.1.

- Сеть основной территории организации, состоящая из главного здания и общежитий, расположена в 42-м квартале в Москве:
 - подключение к сети провайдера осуществляется по оптоволокну через медиаконвертер `msk-q42-mc-1` и маршрутизатор `msk-q42-gw-1` по Fast Ethernet;
 - к маршрутизатору по Fast Ethernet подключён коммутатор `msk-q42-sw-1`, через который работает локальная подсеть здания (имитируем её через PC-PT `pc-q42-1`);
 - подсети общежитий подключаются по Fast Ethernet к маршрутизатору `msk-q42-gw-1` через маршрутизирующий коммутатор Cisco 3560 `msk-hostel-gw-1` посредством коммутатора `msk-hostel-sw-1` (имитируем через PC-PT `pc-hostel-1`).
- Филиал организации расположен в г. Сочи:
 - подключение к сети провайдера осуществляется по оптоволокну через медиаконвертер `sch-sochi-mc-1`, коммутатор `sch-sochi-sw-1` и маршрутизатор с одним интерфейсом `sch-sochi-gw-1` по Fast Ethernet;
 - локальную подсеть филиала имитируем через PC-PT `pc-sochi-1`.

Названия VLAN и выделяемое адресное пространство указано в табл. 13.1–13.4.

13.3. Задание

1. Внести изменения в схемы L1, L2 и L3 сети, добавив в них информацию о сети основной территории (42-й квартал в Москве) и сети филиала в г. Сочи.
2. Дополнить схему проекта, добавив подсеть основной территории организации 42-го квартала в Москве и подсеть филиала в г. Сочи (раздел 13.4.1).
3. Сделать первоначальную настройку добавленного в проект оборудования (разделы 13.4.2 и 13.4.3).

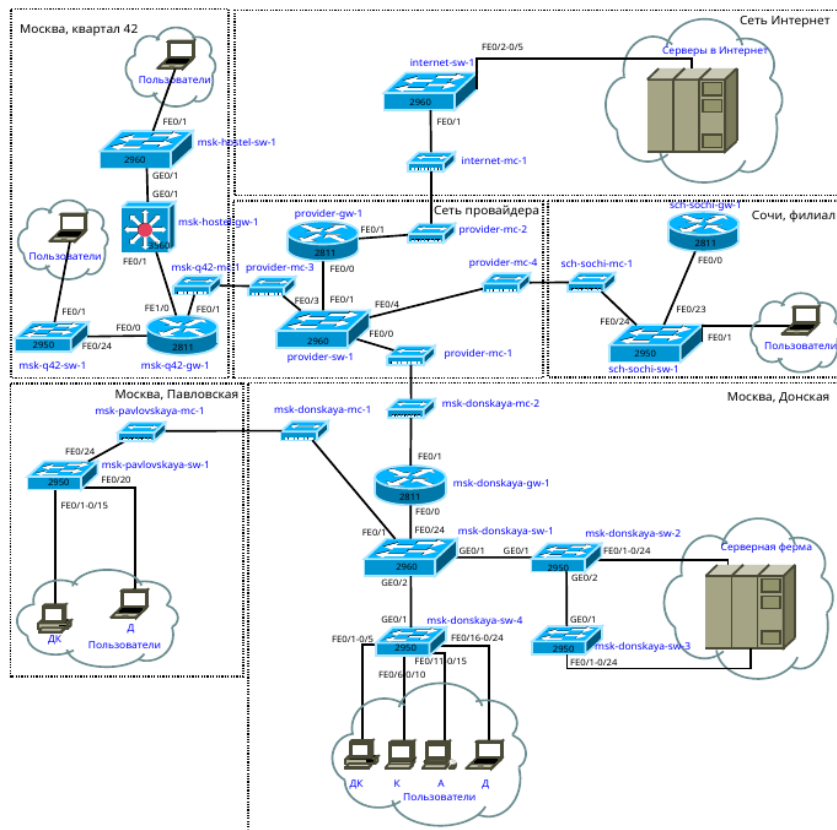


Рис. 13.1. Схема L1 сети с дополнительными площадками

Таблица 13.1

Таблица VLAN сети основной территории и сети филиала в г. Сочи

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	management	Для управления устройствами
3	servers	Для серверной фермы
4	nat	Линк в Интернет
5	q42	Линк в сеть квартала 42 в Москве
6	sochi	Линк в сеть филиала в Сочи
101	dk	Дисплейные классы (ДК)
102	departments	Кафедры
103	adm	Администрация
104	other	Для других пользователей
201	q42-main	Основной для квартала 42 в Москве
202	q42-management	Для управления устройствами 42-го квартала в Москве
301	hostel-main	Основной для общежитий в квартале 42 в Москве
401	sochi-main	Основной для филиала в Сочи
402	sochi-management	Для управления устройствами в филиале в Сочи

Таблица 13.2

Таблица IP для связующих разные территории линков

IP-адреса	Примечание	VLAN
10.128.255.0/24	Вся сеть для линков	
10.128.255.0/30	Линк на 42-й квартал	5
10.128.255.1	msk-donskaya-gw-1	
10.128.255.2	msk-q42-gw-1	
10.128.255.4/30	Линк в Сочи	6
10.128.255.5	msk-donskaya-gw-1	
10.128.255.6	sch-sochi-gw-1	

Таблица 13.3

Таблица IP для сети основной территории (42-й квартал г. Москва)

IP-адреса	Примечание	VLAN
10.129.0.0/16	Вся сеть квартала 42 в Москве	
10.129.0.0/24	Основная сеть квартала 42 в Москве	201
10.129.0.1	msk-q42-gw-1	
10.129.0.200	pc-q42-1	
10.129.1.0/24	Сеть для управления устройствами в сети квартала 42 в Москве	202
10.129.1.1	msk-q42-gw-1	
10.129.1.2	msk-hostel-gw-1	
10.129.128.0/17	Вся сеть hostel	
10.129.128.0/24	Основная сеть hostel	301
10.129.128.1	msk-hostel-gw-1	
10.129.128.200	pc-hostel-1	

Таблица 13.4

Таблица IP для филиала в г. Сочи

IP-адреса	Примечание	VLAN
10.130.0.0/16	Вся сеть филиала в Сочи	
10.130.0.0/24	Основная сеть филиала в Сочи	301
10.130.0.1	sch-sochi-gw-1	
10.130.0.200	pc-sochi-1	
10.130.1.0/24	Сеть для управления устройствами в Сочи	302
10.130.1.1	sch-sochi-gw-1	

13.4. Последовательность выполнения работы

13.4.1. Изменение схемы сети

1. Внесите изменения в схемы L1, L2 и L3 сети.
2. На схеме предыдущего вашего проекта разместите согласно рис. 13.2 необходимое оборудование: 4 медиаконвертера (Repeater-PT), 2 маршрутизатора типа Cisco 2811, 1 маршрутизирующий коммутатор типа Cisco 3560-24PS, 2 коммутатора типа Cisco 2950-24, коммутатор Cisco 2950-24T, 3 оконечных устройства типа PC-PT.

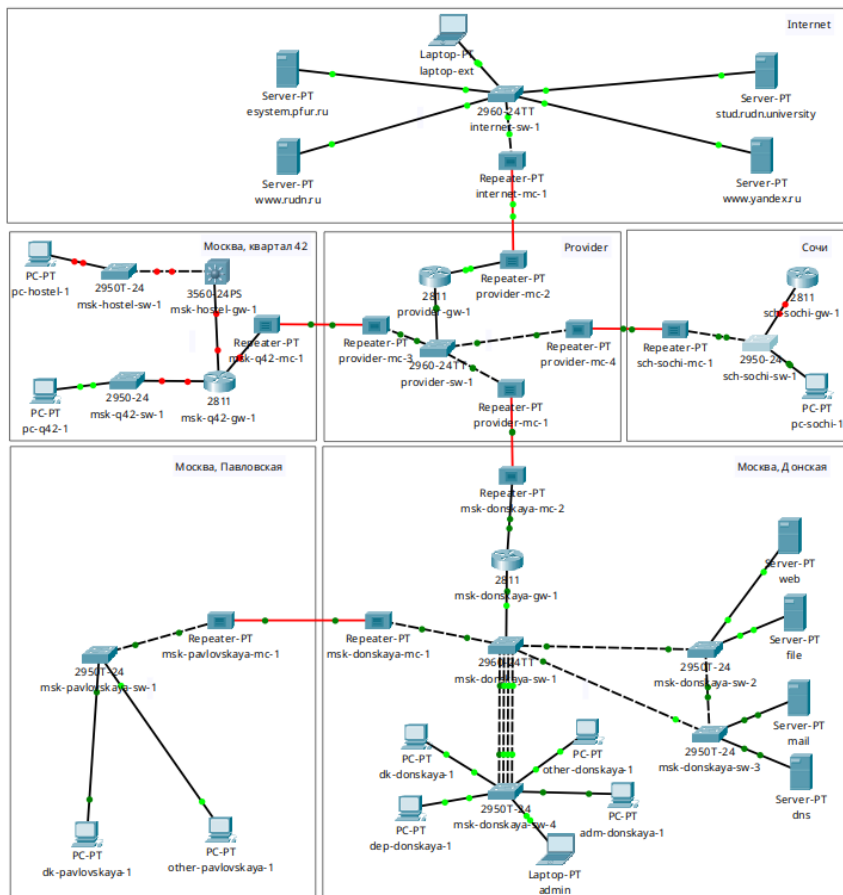


Рис. 13.2. Схема сети с дополнительными площадками

3. Присвойте названия размещённым согласно рис. 13.2 объектам.
4. На медиаконвертерах замените имеющиеся модули на PT-REPEATER-NM-1CFE и PT-REPEATER-NM-1CFE для подключения витой пары по технологии Fast Ethernet и оптоволокна соответственно (рис. 13.3).

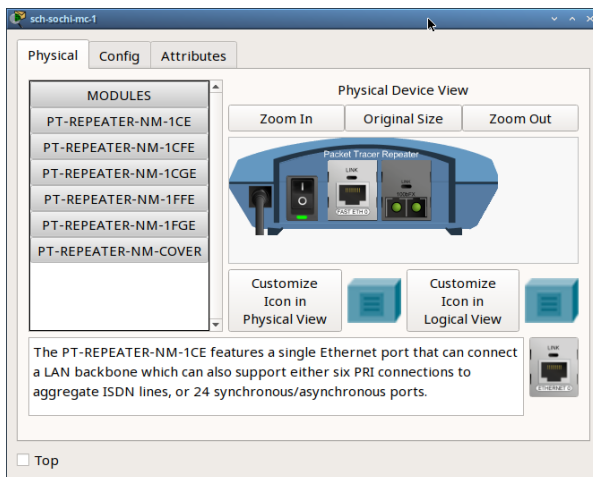


Рис. 13.3. Медиаконвертер с модулями PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE

5. На маршрутизаторе msk-q42-gw-1 добавьте дополнительный интерфейс NM-2FE2W (рис. 13.4).

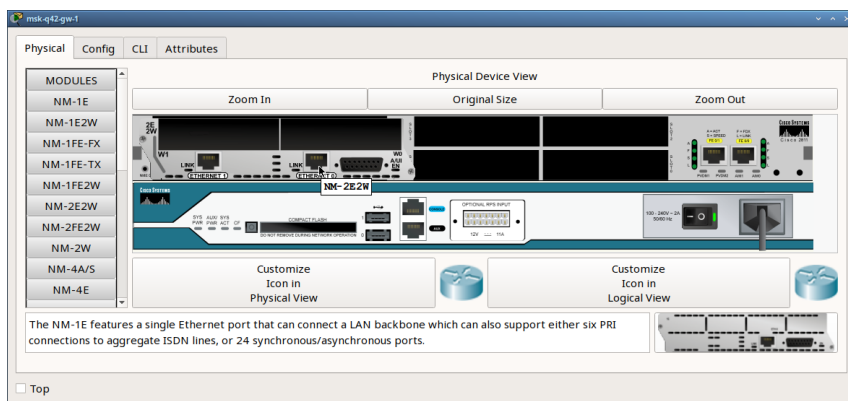


Рис. 13.4. Маршрутизатор с дополнительным интерфейсом NM-2FE2W

6. В физической рабочей области Packet Tracer добавьте в г. Москва здание 42-го квартала (рис. 13.5), присвойте ему соответствующее название.

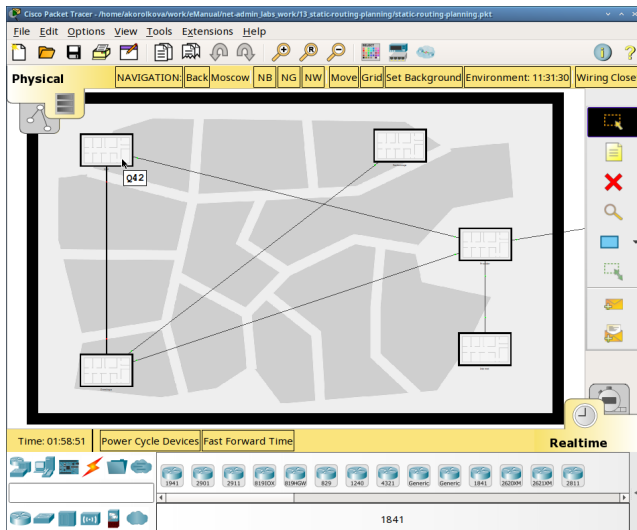


Рис. 13.5. Здание основной территории организации в Москве на физической схеме проекта

7. В физической рабочей области Packet Tracer добавьте город Сочи (рис. 13.6) и в нём здание филиала, присвойте ему соответствующее название.
8. Перенесите из сети «Донская» оборудование сети 42-го квартала и сети филиала в соответствующие здания (рис. 13.7, 13.8).
9. Проведите соединение объектов согласно скорректированной вами схеме L1.

13.4.2. Схема подключения подсети 42-го квартала

13.4.2.1. Первоначальная настройка маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#line vty 0 4
msk-q42-gw-1(config-line)#password cisco
msk-q42-gw-1(config-line)#login
msk-q42-gw-1(config-line)#exit

msk-q42-gw-1(config)#line console 0
msk-q42-gw-1(config-line)#password cisco
msk-q42-gw-1(config-line)#login
```

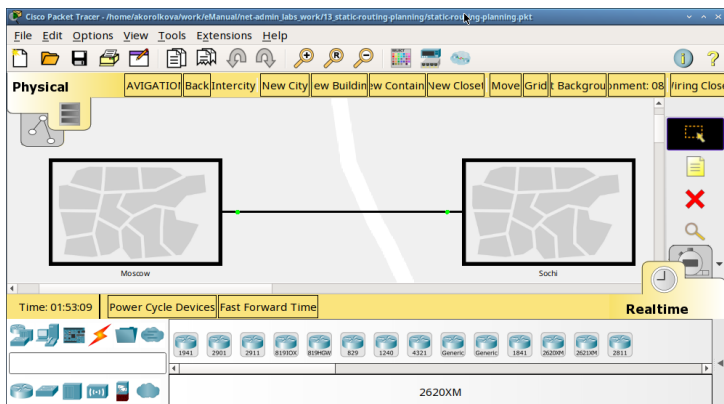


Рис. 13.6. Москва и Сочи на физической схеме проекта

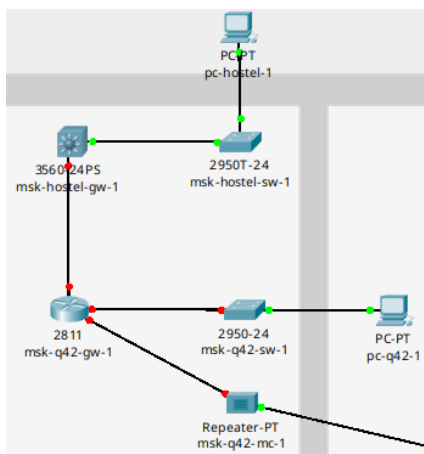


Рис. 13.7. Размещение объектов в основном здании 42-го квартала в Москве

```
msk-q42-gw-1(config-line)#exit

msk-q42-gw-1(config)#enable secret cisco
msk-q42-gw-1(config)#service password-encryption
msk-q42-gw-1(config)#username admin privilege 1 secret cisco

msk-q42-gw-1(config)#ip domain-name q42.rudn.edu
msk-q42-gw-1(config)#crypto key generate rsa
msk-q42-gw-1(config)#line vty 0 4
msk-q42-gw-1(config-line)#transport input ssh
```

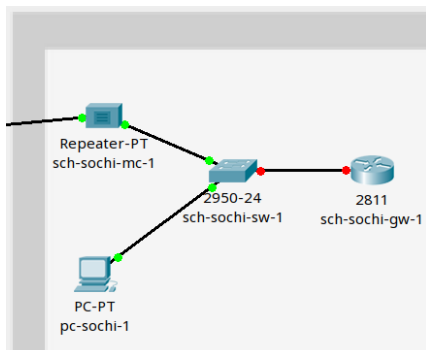


Рис. 13.8. Размещение объектов в здании филиала в г. Сочи

13.4.2.2. Первоначальная настройка коммутатора msk-q42-sw-1

```

msk-q42-sw-1>enable
msk-q42-sw-1#configure terminal

msk-q42-sw-1(config)#line vty 0 4
msk-q42-sw-1(config-line)#password cisco
msk-q42-sw-1(config-line)#login
msk-q42-sw-1(config-line)#exit

msk-q42-sw-1(config)#line console 0
msk-q42-sw-1(config-line)#password cisco
msk-q42-sw-1(config-line)#login
msk-q42-sw-1(config-line)#exit

msk-q42-sw-1(config)#enable secret cisco
msk-q42-sw-1(config)#service password-encryption
msk-q42-sw-1(config)#username admin privilege 1 secret cisco

msk-q42-sw-1(config)#ip domain-name q42.rudn.edu
msk-q42-sw-1(config)#crypto key generate rsa
msk-q42-sw-1(config)#line vty 0 4
msk-q42-sw-1(config-line)#transport input ssh
  
```

13.4.2.3. Первоначальная настройка маршрутизирующего коммутатора msk-hostel-gw-1

```

msk-hostel-gw-1>enable
msk-hostel-gw-1#configure terminal

msk-hostel-gw-1(config)#line vty 0 4
msk-hostel-gw-1(config-line)#password cisco
msk-hostel-gw-1(config-line)#login
msk-hostel-gw-1(config-line)#exit

msk-hostel-gw-1(config)#line console 0
msk-hostel-gw-1(config-line)#password cisco
msk-hostel-gw-1(config-line)#login
msk-hostel-gw-1(config-line)#exit
  
```

```
msk-hostel-gw-1(config)#enable secret cisco
msk-hostel-gw-1(config)#service password-encryption
msk-hostel-gw-1(config)#username admin privilege 1 secret cisco

msk-hostel-gw-1(config)#ip ssh version 2
msk-hostel-gw-1(config)#ip domain-name hostel.rudn.edu
msk-hostel-gw-1(config)#crypto key generate rsa
msk-hostel-gw-1(config)#line vty 0 4
msk-hostel-gw-1(config-line)#transport input ssh
```

13.4.2.4. Первоначальная настройка коммутатора msk-hostel-sw-1

```
msk-hostel-sw-1>enable
msk-hostel-sw-1#configure terminal

msk-hostel-sw-1(config)#line vty 0 4
msk-hostel-sw-1(config-line)#password cisco
msk-hostel-sw-1(config-line)#login
msk-hostel-sw-1(config-line)#exit

msk-hostel-sw-1(config)#line console 0
msk-hostel-sw-1(config-line)#password cisco
msk-hostel-sw-1(config-line)#login
msk-hostel-sw-1(config-line)#exit

msk-hostel-sw-1(config)#enable secret cisco
msk-hostel-sw-1(config)#service password-encryption
msk-hostel-sw-1(config)#username admin privilege 1 secret cisco

msk-hostel-gw-1(config)#ip domain-name hostel.rudn.edu
msk-hostel-gw-1(config)#crypto key generate rsa
msk-hostel-gw-1(config)#line vty 0 4
msk-hostel-gw-1(config-line)#transport input ssh
```

13.4.3. Схема подключения подсети филиала в г. Сочи

13.4.3.1. Первоначальная настройка коммутатора sch-sochi-sw-1

```
sch-sochi-sw-1>enable
sch-sochi-sw-1#configure terminal

sch-sochi-sw-1(config)#line vty 0 4
sch-sochi-sw-1(config-line)#password cisco
sch-sochi-sw-1(config-line)#login
sch-sochi-sw-1(config-line)#exit

sch-sochi-sw-1(config)#line console 0
sch-sochi-sw-1(config-line)#password cisco
sch-sochi-sw-1(config-line)#login
sch-sochi-sw-1(config-line)#exit

sch-sochi-sw-1(config)#enable secret cisco
sch-sochi-sw-1(config)#service password-encryption
sch-sochi-sw-1(config)#username admin privilege 1 secret cisco

msk-sochi-sw-1(config)#ip domain-name sochi.rudn.edu
msk-sochi-sw-1(config)#crypto key generate rsa
msk-sochi-sw-1(config)#line vty 0 4
msk-sochi-sw-1(config-line)#transport input ssh
```


13.4.3.2. Первоначальная настройка маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#line vty 0 4
sch-sochi-gw-1(config-line)#password cisco
sch-sochi-gw-1(config-line)#login
sch-sochi-gw-1(config-line)#exit

sch-sochi-gw-1(config)#line console 0
sch-sochi-gw-1(config-line)#password cisco
sch-sochi-gw-1(config-line)#login
sch-sochi-gw-1(config-line)#exit

sch-sochi-gw-1(config)#enable secret cisco
sch-sochi-gw-1(config)#service password-encryption
sch-sochi-gw-1(config)#username admin privilege 1 secret cisco

msk-sochi-gw-1(config)#ip domain-name sochi.rudn.edu
msk-sochi-gw-1(config)#crypto key generate rsa
msk-sochi-gw-1(config)#line vty 0 4
msk-sochi-gw-1(config-line)#transport input ssh
```

13.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - схемы сети L1, L2, L3;
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

13.6. Контрольные вопросы

1. В каких случаях следует использовать статическую маршрутизацию? Приведите примеры.
2. Укажите основные принципы статической маршрутизации между VLANs.

Лабораторная работа № 14. Статическая маршрутизация в Интернете. Настройка

14.1. Цель работы

Настроить взаимодействие через сеть провайдера посредством статической маршрутизации локальной сети организации с сетью основного здания, расположенного в 42-м квартале в Москве, и сетью филиала, расположенного в г. Сочи.

14.2. Задание

1. Настроить связь между территориями (см. раздел 14.3.1).
2. Настроить оборудование, расположенное в квартале 42 в Москве (см. раздел 14.3.2).
3. Настроить оборудование, расположенное в филиале в г. Сочи (см. раздел 14.3.3).
4. Настроить статическую маршрутизацию между территориями (см. раздел 14.3.4).
5. Настроить статическую маршрутизацию на территории квартала 42 в г. Москве (см. раздел 14.3.5).
6. Настроить NAT на маршрутизаторе `msk-donskaya-gw-1` (см. раздел 14.3.6).

14.3. Последовательность выполнения работы

14.3.1. Настройка линка между площадками

14.3.1.1. Настройка интерфейсов коммутатора `provider-sw-1`

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#interface f0/3
provider-sw-1(config-if)#switchport mode trunk
provider-sw-1(config-if)#exit

provider-sw-1(config)#interface f0/4
provider-sw-1(config-if)#switchport mode trunk
provider-sw-1(config-if)#exit

provider-sw-1(config)#vlan 5
provider-sw-1(config-vlan)#name q42
provider-sw-1(config-vlan)#exit

provider-sw-1(config)#interface vlan5
provider-sw-1(config-if)#no shutdown
provider-sw-1(config-if)#exit

provider-sw-1(config)#vlan 6
provider-sw-1(config-vlan)#name sochi
provider-sw-1(config-vlan)#exit
```

```
provider-sw-1(config)#interface vlan6
provider-sw-1(config-if)#no shutdown
provider-sw-1(config-if)#exit
```

14.3.1.2. Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface f0/1.5
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 5
msk-donskaya-gw-1(config-subif)#ip address 10.128.255.1 255.255.255.252
msk-donskaya-gw-1(config-subif)#description q42
msk-donskaya-gw-1(config-subif)#exit

msk-donskaya-gw-1(config)#interface f0/1.6
msk-donskaya-gw-1(config-subif)#encapsulation dot1Q 6
msk-donskaya-gw-1(config-subif)#ip address 10.128.255.5 255.255.255.252
msk-donskaya-gw-1(config-subif)#description sochi
msk-donskaya-gw-1(config-subif)#exit
msk-donskaya-gw-1(config)#exit
```

14.3.1.3. Настройка интерфейсов маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#interface f0/1
msk-q42-gw-1(config-if)#no shutdown
msk-q42-gw-1(config-if)#exit

msk-q42-gw-1(config)#interface f0/1.5
msk-q42-gw-1(config-subif)#encapsulation dot1Q 5
msk-q42-gw-1(config-subif)#ip address 10.128.255.2 255.255.255.252
msk-q42-gw-1(config-subif)#description donsкаya
msk-q42-gw-1(config-subif)#exit
msk-q42-gw-1(config)#exit
```

14.3.1.4. Настройка интерфейсов коммутатора sch-sochi-sw-1

```
sch-sochi-sw-1>enable
sch-sochi-sw-1#configure terminal

sch-sochi-sw-1(config)#interface f0/23
sch-sochi-sw-1(config-if)#switchport mode trunk
sch-sochi-sw-1(config-if)#exit

sch-sochi-sw-1(config)#interface f0/24
sch-sochi-sw-1(config-if)#switchport mode trunk
sch-sochi-sw-1(config-if)#exit

sch-sochi-sw-1(config)#vlan 6
sch-sochi-sw-1(config-vlan)#name sochi
sch-sochi-sw-1(config-vlan)#exit

sch-sochi-sw-1(config)#interface vlan6
sch-sochi-sw-1(config-if)#no shutdown
sch-sochi-sw-1(config-if)#exit
```

14.3.1.5. Настройка интерфейсов маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#interface f0/0
sch-sochi-gw-1(config-if)#no shutdown
sch-sochi-gw-1(config-if)#exit

sch-sochi-gw-1(config)#interface f0/0.6
sch-sochi-gw-1(config-subif)#encapsulation dot1Q 6
sch-sochi-gw-1(config-subif)#ip address 10.128.255.6 255.255.255.252
sch-sochi-gw-1(config-subif)#description donskaya
sch-sochi-gw-1(config-subif)#exit
sch-sochi-gw-1(config)#exit
```

14.3.2. Настройка площадки 42-го квартала

14.3.2.1. Настройка интерфейсов маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#interface f0/0
msk-q42-gw-1(config-if)#no shutdown
msk-q42-gw-1(config-if)#exit

msk-q42-gw-1(config)#interface f0/0.201
msk-q42-gw-1(config-subif)#encapsulation dot1Q 201
msk-q42-gw-1(config-subif)#ip address 10.129.0.1 255.255.255.0
msk-q42-gw-1(config-subif)#description q42-main
msk-q42-gw-1(config-subif)#exit

msk-q42-gw-1(config)#interface f1/0
msk-q42-gw-1(config-if)#no shutdown
msk-q42-gw-1(config-if)#exit

msk-q42-gw-1(config)#interface f1/0.202
msk-q42-gw-1(config-subif)#encapsulation dot1Q 202
msk-q42-gw-1(config-subif)#ip address 10.129.1.1 255.255.255.0
msk-q42-gw-1(config-subif)#description q42-management
msk-q42-gw-1(config-subif)#exit
```

14.3.2.2. Настройка интерфейсов коммутатора msk-q42-sw-1

```
msk-q42-sw-1>enable
msk-q42-sw-1#configure terminal

msk-q42-sw-1(config)#interface f0/24
msk-q42-sw-1(config-if)#switchport mode trunk
msk-q42-sw-1(config-if)#exit

msk-q42-sw-1(config)#interface f0/1
msk-q42-sw-1(config-if)#switchport mode access
msk-q42-sw-1(config-if)#switchport access vlan 201
msk-q42-sw-1(config-if)#exit

msk-q42-sw-1(config)#vlan 201
msk-q42-sw-1(config-vlan)#name q42-main
msk-q42-sw-1(config-vlan)#exit
```

```
msk-q42-sw-1(config)#interface vlan201
msk-q42-sw-1(config-if)#no shutdown
msk-q42-sw-1(config-if)#exit
```

14.3.2.3. Настройка интерфейсов маршрутизирующего коммутатора msk-hostel-gw-1

```
msk-hostel-gw-1>enable
msk-hostel-gw-1#configure terminal

msk-hostel-sw-1(config)#interface g0/1
msk-hostel-gw-1(config-if)#switchport trunk encapsulation dot1q
msk-hostel-sw-1(config-if)#switchport mode trunk
msk-hostel-sw-1(config-if)#exit

msk-hostel-sw-1(config)#interface f0/24
msk-hostel-gw-1(config-if)#switchport trunk encapsulation dot1q
msk-hostel-sw-1(config-if)#switchport mode trunk
msk-hostel-sw-1(config-if)#exit

msk-hostel-sw-1(config)#vlan 202
msk-hostel-sw-1(config-vlan)#name q42-management
msk-hostel-sw-1(config-vlan)#exit

msk-hostel-sw-1(config)#interface vlan202
msk-hostel-sw-1(config-if)#no shutdown
msk-hostel-sw-1(config-if)#ip address 10.129.1.2 255.255.255.0
msk-hostel-sw-1(config-if)#exit

msk-hostel-sw-1(config)#vlan 301
msk-hostel-sw-1(config-vlan)#name hostel-main
msk-hostel-sw-1(config-vlan)#exit

msk-hostel-sw-1(config)#interface vlan301
msk-hostel-sw-1(config-if)#no shutdown
msk-hostel-sw-1(config-if)#ip address 10.129.128.1 255.255.255.0
msk-hostel-sw-1(config-if)#exit
```

14.3.2.4. Настройка интерфейсов коммутатора msk-hostel-sw-1

```
msk-hostel-sw-1>enable
msk-hostel-sw-1#configure terminal

msk-hostel-sw-1(config)#interface g0/1
msk-hostel-sw-1(config-if)#switchport mode trunk
msk-hostel-sw-1(config-if)#exit

msk-hostel-sw-1(config)#interface f0/1
msk-hostel-sw-1(config-if)#switchport mode access
msk-hostel-sw-1(config-if)#switchport access vlan 301
msk-hostel-sw-1(config-if)#exit

msk-hostel-sw-1(config)#vlan 301
msk-hostel-sw-1(config-vlan)#name hostel-main
msk-hostel-sw-1(config-vlan)#exit

msk-hostel-sw-1(config)#interface vlan301
msk-hostel-sw-1(config-if)#no shutdown
msk-hostel-sw-1(config-if)#exit
```

14.3.3. Настройка площадки в Сочи

14.3.3.1. Настройка интерфейсов маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#interface f0/0.301
sch-sochi-gw-1(config-subif)#encapsulation dot1Q 301
sch-sochi-gw-1(config-subif)#ip address 10.130.0.1 255.255.255.0
sch-sochi-gw-1(config-subif)#description sochi-main
sch-sochi-gw-1(config-subif)#exit

sch-sochi-gw-1(config)#interface f0/0.302
sch-sochi-gw-1(config-subif)#encapsulation dot1Q 302
sch-sochi-gw-1(config-subif)#ip address 10.130.1.1 255.255.255.0
sch-sochi-gw-1(config-subif)#description sochi-management
sch-sochi-gw-1(config-subif)#exit
```

14.3.3.2. Настройка интерфейсов коммутатора sch-sochi-sw-1

```
sch-sochi-sw-1>enable
sch-sochi-sw-1#configure terminal

sch-sochi-sw-1(config)#interface f0/1
sch-sochi-sw-1(config-if)#switchport mode access
sch-sochi-sw-1(config-if)#switchport access vlan 301
sch-sochi-sw-1(config-if)#exit

sch-sochi-sw-1(config)#vlan 301
sch-sochi-sw-1(config-vlan)#name sochi-main
sch-sochi-sw-1(config-vlan)#exit

sch-sochi-sw-1(config)#interface vlan301
sch-sochi-sw-1(config-if)#no shutdown
sch-sochi-sw-1(config-if)#exit
```

14.3.4. Настройка маршрутизации между площадками

14.3.4.1. Настройка маршрутизатора msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#ip route 10.129.0.0 255.255.0.0 10.128.255.2
msk-donskaya-gw-1(config)#ip route 10.130.0.0 255.255.0.0 10.128.255.6
```

14.3.4.2. Настройка маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#ip route 0.0.0.0 0.0.0.0 10.128.255.1
```

14.3.4.3. Настройка маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#ip route 0.0.0.0 0.0.0.0 10.128.255.5
```

14.3.5. Настройка маршрутизации на 42 квартале

14.3.5.1. Настройка маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#ip route 10.129.128.0 255.255.128.0 10.129.1.2
```

14.3.5.2. Настройка интерфейсов маршрутизирующего коммутатора msk-hostel-gw-1

```
msk-hostel-gw-1>enable
msk-hostel-gw-1#configure terminal

msk-hostel-gw-1(config)#ip routing

msk-hostel-gw-1(config)#ip route 0.0.0.0 0.0.0.0 10.129.1.1
```

14.3.6. Настройка NAT на маршрутизаторе msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface f0/1.5
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit

msk-donskaya-gw-1(config)#interface f0/1.6
msk-donskaya-gw-1(config-subif)#ip nat inside
msk-donskaya-gw-1(config-subif)#exit

msk-donskaya-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-gw-1(config-ext-nacl)#remark q42
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.129.0.200 any
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.129.128.200 any
msk-donskaya-gw-1(config-ext-nacl)#remark sochi
msk-donskaya-gw-1(config-ext-nacl)#permit ip host 10.130.0.200 any
msk-donskaya-gw-1(config-ext-nacl)#exit
```

14.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - схемы L1, L2, L3 сети;
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

14.5. Контрольные вопросы

1. Приведите пример настройки статической маршрутизации между двумя подсетями организации.
2. Опишите процесс обращения устройства из одного VLAN к устройству из другого VLAN.
3. Как проверить работоспособность маршрута?
4. Как посмотреть таблицу маршрутизации?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—5].

Литература по теме

1. *Кларк К., Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series).
2. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
3. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
4. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
5. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009.

Лабораторная работа № 15. Динамическая маршрутизация

15.1. Цель работы

Настроить динамическую маршрутизацию между территориями организации.

15.2. Предварительные сведения

Протокол внутренней маршрутизации Open Shortest Path First (OSPF, RFC 2328) [1] используется на маршрутизаторах для распространения данных маршрутизации внутри одной автономной системы. Под автономной системой (autonomous system) в данном случае понимается группа маршрутизаторов, использующих общий протокол маршрутизации для обмена маршрутной информацией.

В основе работы OSPF лежит технология отслеживания состояния канала (link-state technology), которая использует алгоритм Дейкстры для нахождения кратчайшего пути.

Для обозначения области действия протокола OSPF внутри автономной системы используется понятие *зоны (area)* — совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны. Для определения маршрутизаторов внутри зоны используется уникальный идентификатор каждого маршрутизатора (router ID, RID).

В табл. 15.1 представлены IP-адреса, выделяемые в моделируемой нами сети для идентификации маршрутизаторов по протоколу OSPF.

Таблица 15.1

Идентификация маршрутизаторов

IP-адреса	Примечание
10.128.254.0/24	Сеть для идентификации маршрутизаторов
10.128.254.1	msk-donskaya-gw-1
10.128.254.2	msk-q42-gw-1
10.128.254.3	msk-hostel-gw-1
10.128.254.4	sch-sochi-gw-1

В табл. 15.2 представлены IP-адреса, выделяемые в моделируемой нами сети для организации прямого соединения между сетью квартала 42 в Москве и сетью филиала в г. Сочи.

Таблица 15.2

Таблица IP линка 42 квартал—Сочи

IP-адреса	Примечание	VLAN
10.128.255.8/30	Линк между 42 кварталом и Сочи	7
10.128.255.9	msk-q42-gw-1	
10.128.255.10	sch-sochi-gw-1	

15.3. Задание

1. Настроить динамическую маршрутизацию по протоколу OSPF на маршрутизаторах `msk-donskaya-gw-1`, `msk-q42-gw-1`, `msk-hostel-gw-1`, `sch-sochi-gw-1` (см. раздел 15.4.1).
2. Настроить связь сети квартала 42 в Москве с сетью филиала в г. Сочи напрямую (см. раздел 15.4.2).
3. В режиме симуляции отследить движение пакета ICMP с ноутбука администратора сети на Донской в Москве (`Laptop-PT admin`) до компьютера пользователя в филиале в г. Сочи `pc-sochi-1`.
4. На коммутаторе провайдера отключить временно `vlan 6` и в режиме симуляции убедиться в изменении маршрута прохождения пакета ICMP с ноутбука администратора сети на Донской в Москве (`Laptop-PT admin`) до компьютера пользователя в филиале в г. Сочи `pc-sochi-1`.
5. На коммутаторе провайдера восстановить `vlan 6` и в режиме симуляции убедиться в изменении маршрута прохождения пакета ICMP с ноутбука администратора сети на Донской в Москве (`Laptop-PT admin`) до компьютера пользователя в филиале в г. Сочи `pc-sochi-1`.

15.4. Последовательность выполнения работы

15.4.1. Настройка OSPF

15.4.1.1. Настройка маршрутизатора `msk-donskaya-gw-1`

Включение OSPF на маршрутизаторе предполагает, во-первых, включение процесса OSPF командой `router ospf <process-id>`, во-вторых — назначение областей (зон) интерфейсам с помощью команды `network <network or IP address> <mask> area <area-id>`:

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#router ospf 1
msk-donskaya-gw-1(config-router)#router-id 10.128.254.1
msk-donskaya-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
msk-donskaya-gw-1(config-router)#exit
```

Идентификатор процесса OSPF (`process-id`) по сути идентифицирует маршрутизатор в автономной системе, и, вообще говоря, он не должен совпадать с идентификаторами процессов на других маршрутизаторах.

Значение идентификатора области (`area-id`) может быть целым числом от 0 до 4294967295 или может быть представлено в виде IP-адреса: A.B.C.D.

Область 0 называется магистралью, области с другими идентификаторами должны подключаться к магистральной.

15.4.1.2. Проверка состояния протокола OSPF на маршрутизаторе msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#sh ip ospf
msk-donskaya-gw-1#sh ip ospf neighbor
msk-donskaya-gw-1#sh ip route
```

Маршрутизаторы с общим сегментом являются соседями в этом сегменте. Соседи выбираются с помощью протокола Hello. Команда `show ip ospf neighbor` показывает статус всех соседей в заданном сегменте. Команда `show ip ospf route` (или `show ip route`) выводит информацию из таблицы маршрутизации.

15.4.1.3. Настройка маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#router ospf 1
msk-q42-gw-1(config-router)#router-id 10.128.254.2
msk-q42-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
msk-q42-gw-1(config-router)#exit
```

15.4.1.4. Настройка маршрутизирующего коммутатора msk-hostel-gw-1

```
msk-hostel-gw-1>enable
msk-hostel-gw-1#configure terminal

msk-hostel-gw-1(config)#router ospf 1
msk-hostel-gw-1(config-router)#router-id 10.128.254.3
msk-hostel-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
msk-hostel-gw-1(config-router)#exit
```

15.4.1.5. Настройка маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#router ospf 1
sch-sochi-gw-1(config-router)#router-id 10.128.254.4
sch-sochi-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
sch-sochi-gw-1(config-router)#exit
```

Проверьте состояние протокола OSPF на всех маршрутизаторах. Что можно сказать о соседях OSPF на разных маршрутизаторах? Что можно сказать о маршрутных таблицах на разных маршрутизаторах?

15.4.2. Настройка линка 42-й квартал–Сочи

15.4.2.1. Настройка интерфейсов коммутатора provider-sw-1

```
provider-sw-1>enable
provider-sw-1#configure terminal

provider-sw-1(config)#vlan 7
provider-sw-1(config-vlan)#name q42-sochi
provider-sw-1(config-vlan)#exit

provider-sw-1(config)#interface vlan7
provider-sw-1(config-if)#no shutdown
provider-sw-1(config-if)#exit
```

15.4.2.2. Настройка маршрутизатора msk-q42-gw-1

```
msk-q42-gw-1>enable
msk-q42-gw-1#configure terminal

msk-q42-gw-1(config)#interface f0/1.7
msk-q42-gw-1(config-subif)#encapsulation dot1Q 7
msk-q42-gw-1(config-subif)#ip address 10.128.255.9 255.255.255.252
msk-q42-gw-1(config-subif)#description sochi
msk-q42-gw-1(config-subif)#exit
```

15.4.2.3. Настройка коммутатора sch-sochi-sw-1

```
sch-sochi-sw-1>enable
sch-sochi-sw-1#configure terminal

sch-sochi-sw-1(config)#vlan 7
sch-sochi-sw-1(config-vlan)#name q42-sochi
sch-sochi-sw-1(config-vlan)#exit

sch-sochi-sw-1(config)#interface vlan7
sch-sochi-sw-1(config-if)#no shutdown
sch-sochi-sw-1(config-if)#exit
```

15.4.2.4. Настройка маршрутизатора sch-sochi-gw-1

```
sch-sochi-gw-1>enable
sch-sochi-gw-1#configure terminal

sch-sochi-gw-1(config)#interface f0/0.7
sch-sochi-gw-1(config-subif)#encapsulation dot1Q 7
sch-sochi-gw-1(config-subif)#ip address 10.128.255.10 255.255.255.252
sch-sochi-gw-1(config-subif)#description q42
sch-sochi-gw-1(config-subif)#exit
```

15.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;

- подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
 5. Ответы на контрольные вопросы.

15.6. Контрольные вопросы

1. Какие протоколы относятся к протоколам динамической маршрутизации?
2. Охарактеризуйте принципы работы протоколов динамической маршрутизации.
3. Опишите процесс обращения устройства из одной подсети к устройству из другой подсети по протоколу динамической маршрутизации.
4. Опишите выводимую информацию при просмотре таблицы маршрутизации.

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1–5].

Литература по теме

1. *Мой J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — P. 244. — DOI: 10.17487/rfc2328.
2. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series).
3. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
4. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016.
5. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009.

Получение навыков настройки VPN-туннеля через незащищённое Интернет-соединение.

Настроить VPN-туннель между сетью Университета г. Пиза (Италия) и сетью «Донская» в г. Москва (см. рис. 16.1).

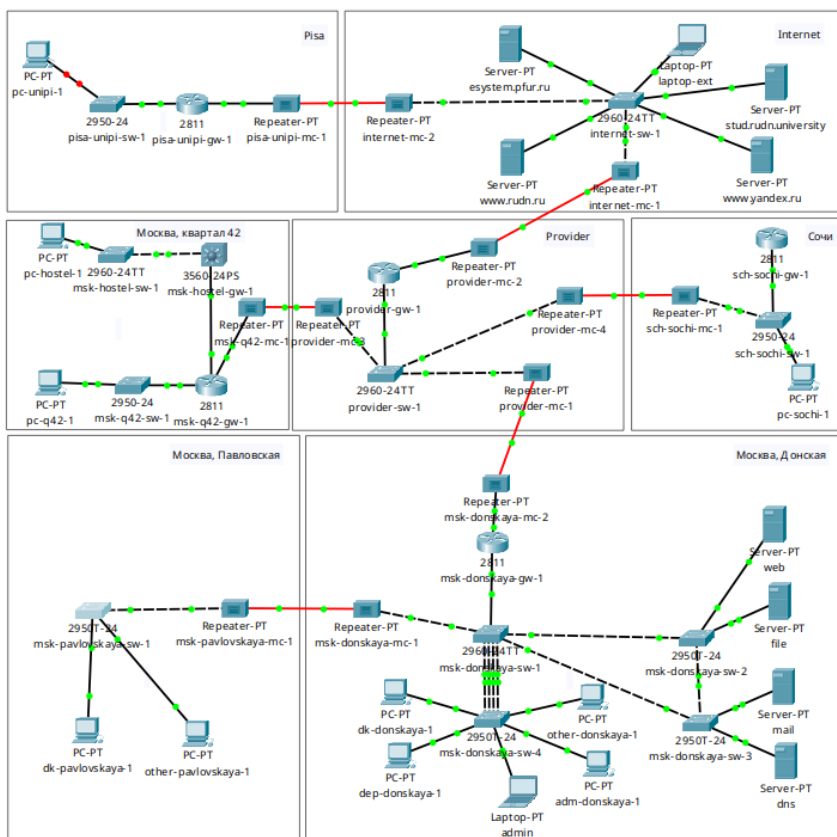


Рис. 16.1. Схема сети с дополнительными площадками

16.3. Предварительные сведения

Виртуальная частная сеть (Virtual Private Network, VPN) — технология, обеспечивающая одно или несколько сетевых соединений поверх другой сети (например, Интернет).

Для организации защищённого VPN-туннеля может использоваться протокол общей инкапсуляции маршрутов (Generic Routing Encapsulation, GRE) компании Cisco. Основное назначение GRE — инкапсуляция пакетов сетевого уровня сетевой модели взаимодействия открытых систем (Open Systems Interconnection Basic Reference Model), например, IP, CLNP, IPX, AppleTalk и др., в IP пакеты.

16.4. Модельные предположения

Сеть Университета г. Пиза (Италия) содержит маршрутизатор Cisco 2811 `pisa-inip1-gw-1`, коммутатор Cisco 2950 `pisa-unip1-sw-1` и конечное устройство PC `pc-unip1-1` (см. общую схему сети на рис. 16.1).

Адреса для организации VPN-туннеля представлены в табл. 16.1.

Таблица 16.1

Адреса туннеля VPN

IP-адреса	Примечание
10.128.255.252/30	Линк VPN
10.128.255.253	msk-donskaya-gw-1
10.128.255.254	pisa-unip1-gw-1

Для идентификации маршрутизаторов предполагается использовать loopback-адреса (табл. 16.2).

Таблица 16.2

Адреса интерфейсов loopback

IP-адреса	Примечание
10.128.254.0/24	Сеть адресов loopback интерфейсов
10.128.254.1/32	msk-donskaya-gw-1
10.128.254.2/32	msk-q42-gw-1
10.128.254.3/32	msk-hostel-gw-1
10.128.254.4/32	sch-sochi-gw-1
10.128.254.5/32	pisa-unip1-gw-1

16.5. Последовательность выполнения работы

1. Разместить в рабочей области проекта в соответствии с модельными предположениями оборудование для сети Университета г. Пиза.
2. В физической рабочей области проекта создать город Пиза, здание Университета г. Пиза. Переместить туда соответствующее оборудование.
3. Сделать первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза (см. раздел 16.5.1).
4. Настроить VPN на основе протокола GRE [1] (см. раздел 16.5.2).
5. Проверить доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская».

16.5.1. Настройка площадки в г. Пиза

16.5.1.1. Первоначальная настройка маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#line vty 0 4
pisa-unipi-gw-1(config-line)#password cisco
pisa-unipi-gw-1(config-line)#login
pisa-unipi-gw-1(config-line)#exit

pisa-unipi-gw-1(config)#line console 0
pisa-unipi-gw-1(config-line)#password cisco
pisa-unipi-gw-1(config-line)#login
pisa-unipi-gw-1(config-line)#exit

pisa-unipi-gw-1(config)#enable secret cisco
pisa-unipi-gw-1(config)#service password-encryption
pisa-unipi-gw-1(config)#username admin privilege 1 secret cisco

pisa-unipi-gw-1(config)#ip domain-name unpipi.edu
pisa-unipi-gw-1(config)#crypto key generate rsa
pisa-unipi-gw-1(config)#line vty 0 4
pisa-unipi-gw-1(config-line)#transport input ssh
```

16.5.1.2. Первоначальная настройка коммутатора pisa-unipi-sw-1

```
pisa-unipi-sw-1>enable
pisa-unipi-sw-1#configure terminal

pisa-unipi-sw-1(config)#line vty 0 4
pisa-unipi-sw-1(config-line)#password cisco
pisa-unipi-sw-1(config-line)#login
pisa-unipi-sw-1(config-line)#exit

pisa-unipi-sw-1(config)#line console 0
pisa-unipi-sw-1(config-line)#password cisco
pisa-unipi-sw-1(config-line)#login
pisa-unipi-sw-1(config-line)#exit

pisa-unipi-sw-1(config)#enable secret cisco
pisa-unipi-sw-1(config)#service password-encryption
pisa-unipi-sw-1(config)#username admin privilege 1 secret cisco
```



```
pisa-unipi-sw-1(config)#ip domain-name unipi.edu
pisa-unipi-sw-1(config)#crypto key generate rsa
pisa-unipi-sw-1(config)#line vty 0 4
pisa-unipi-sw-1(config-line)#transport input ssh
```

16.5.1.3. Настройка интерфейсов маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#interface f0/0
pisa-unipi-gw-1(config-if)#no shutdown
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#interface f0/0.401
pisa-unipi-gw-1(config-subif)#encapsulation dot1Q 401
pisa-unipi-gw-1(config-subif)#ip address 10.131.0.1 255.255.255.0
pisa-unipi-gw-1(config-subif)#description unipi-main
pisa-unipi-gw-1(config-subif)#exit

pisa-unipi-gw-1(config)#interface f0/1
pisa-unipi-gw-1(config-if)#no shutdown
pisa-unipi-gw-1(config-if)#ip address 192.0.2.20 255.255.255.0
pisa-unipi-gw-1(config-if)#description internet
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1
```

16.5.1.4. Настройка интерфейсов коммутатора pisa-unipi-sw-1

```
pisa-unipi-sw-1>enable
pisa-unipi-sw-1#configure terminal

pisa-unipi-sw-1(config)#interface f0/24
pisa-unipi-sw-1(config-if)#switchport mode trunk
pisa-unipi-sw-1(config-if)#exit

pisa-unipi-sw-1(config)#interface f0/1
pisa-unipi-sw-1(config-if)#switchport mode access
pisa-unipi-sw-1(config-if)#switchport access vlan 401
pisa-unipi-sw-1(config-if)#exit

pisa-unipi-sw-1(config)#vlan 401
pisa-unipi-sw-1(config-vlan)#name unipi-main
pisa-unipi-sw-1(config-vlan)#exit

pisa-unipi-sw-1(config)#interface vlan401
pisa-unipi-sw-1(config-if)#no shutdown
pisa-unipi-sw-1(config-if)#exit
```

16.5.2. Настройка VPN на основе GRE

16.5.2.1. Настройка маршрутизатора msk-donskaya-gw-1

```
msk-donskaya-gw-1>enable
msk-donskaya-gw-1#configure terminal

msk-donskaya-gw-1(config)#interface Tunnel0
msk-donskaya-gw-1(config-if)#ip address 10.128.255.253 255.255.255.252
msk-donskaya-gw-1(config-if)#tunnel source f0/1.4
msk-donskaya-gw-1(config-if)#tunnel destination 192.0.2.20
```

```
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#interface loopback0
msk-donskaya-gw-1(config-if)#ip address 10.128.254.1 255.255.255.255
msk-donskaya-gw-1(config-if)#exit

msk-donskaya-gw-1(config)#ip route 10.128.254.5 255.255.255.255 ←
10.128.255.254
```

16.5.2.2. Настройка маршрутизатора pisa-unipi-gw-1

```
pisa-unipi-gw-1>enable
pisa-unipi-gw-1#configure terminal

pisa-unipi-gw-1(config)#interface Tunnel0
pisa-unipi-gw-1(config-if)#ip address 10.128.255.254 255.255.255.252
pisa-unipi-gw-1(config-if)#tunnel source f0/1
pisa-unipi-gw-1(config-if)#tunnel destination 198.51.100.2
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#interface loopback0
pisa-unipi-gw-1(config-if)#ip address 10.128.254.5 255.255.255.255
pisa-unipi-gw-1(config-if)#exit

pisa-unipi-gw-1(config)#ip route 10.128.254.1 255.255.255.255 ←
10.128.255.253

pisa-unipi-gw-1(config)#router ospf 1
pisa-unipi-gw-1(config-router)#router-id 10.128.254.5
pisa-unipi-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
pisa-unipi-gw-1(config-router)#exit
```

16.6. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание настроек сетевого оборудования в соответствии с заданием;
 - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтвержденные скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

16.7. Контрольные вопросы

1. Что такое VPN?
2. В каких случаях следует использовать VPN?
3. Как с помощью VPN обойти NAT?

Литература по теме

1. Хилл Б. Полный справочник по Cisco. — М. : Вильямс, 2009.

Рекомендуемая литература

1. *A J. Packet Tracer Network Simulator.* — Packt Publishing, 2014.
2. *Neumann J. C. Cisco Routers for the Small Business A Practical Guide for IT Professionals.* — Apress, 2009.
3. *Odom S., Nottingham H. Cisco Switching: Black Book.* — The Coriolis Group, 2001.
4. *Tetz E. Cisco Networking All-in-One For Dummies.* — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies).
5. *Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco.* — М. : Вильямс, 2003. — (Cisco Press Core Series).
6. *Королькова А. В., Кулябов Д. С. Архитектура и принципы построения современных сетей и систем телекоммуникаций.* — М. : Издательство РУДН, 2009.
7. *Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Курс лекций.* — М. : РУДН, 2012.
8. *Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Лабораторные работы.* — М. : РУДН, 2012.
9. *Королькова А. В., Кулябов Д. С. Сетевые технологии. Лабораторные работы.* — М. : РУДН, 2014.
10. *Куроуз Д. Ф., Росс К. В. Компьютерные сети. Нисходящий подход.* — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).
11. *Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101.* — М. : Вильямс, 2017. — (Cisco Press Core Series).
12. *Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация.* — М. : Вильямс, 2016. — (Cisco Press Core Series).
13. *Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы.* — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов).
14. *Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.].* — М. : Изд-во Юрайт, 2016.
15. *Таненбаум Э., Уэзеролл Д. Компьютерные сети.* — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science).
16. *Хилл Б. Полный справочник по Cisco.* — М. : Вильямс, 2009.

Глоссарий

Безопасная оболочка (Secure Shell, SSH) Сетевой протокол удалённого доступа к устройствам сети с возможностью туннелирования TCP-соединений. 26

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) Технология виртуальных локальных сетей, позволяющая создавать в едином канале (Ethernet-сегменте) независимые логические области, ограничивающие на канальном уровне распространение трафика (в том числе и широковещательного). 16, 19, 20, 29, 32, 47, 51, 63, 70

Виртуальная частная сеть (Virtual Private Network, VPN) Технология, обеспечивающая одно или несколько сетевых соединений поверх другой сети. 94

Витая пара Вид кабеля связи, представляющий собой одну или несколько пар изолированных проводников, скрученных между собой с целью уменьшения взаимных наводок при передаче сигнала. 39, 75

Возвратный адрес (Loopback) Адрес для внутреннего взаимодействия процессов узла. 94

Домен (Domain) Название зоны в системе доменных имён (DNS) Интернета, выделенной какой-либо стране, организации или для иных целей. 42

Запись DNS (RR-запись) описание ресурса сети в зоне DNS: NS-запись — перечисляет DNS-серверы зоны; A — отображение имён узлов в адреса; PTR — отображение адресов в имена узлов; CNAME — каноническое имя (для псевдонимов); MX — отображение имён почтовых серверов. 42, 43

Канальный уровень (Data Link Layer) ISO/OSI Обеспечивает функциональные и процедурные средства для установления, поддержания и разрыва соединений канального уровня между сетевыми логическими объектами и для передачи сервисных блоков данных этого уровня. 19, 20

Качество обслуживания (Quality of Service, QoS) Мера производительности передающей системы, отражающая качество передачи и доступность услуг. 19

Концентратор (Hub) Многопортовый повторитель с автосегментацией, в котором сигнал, полученный от одной из подключённых к нему станций, транслируется на все его активные порты. 13

Локальная сеть (Local Area Network, LAN) Сеть здания или организации. 70

Маршрутизатор (Router) Сетевое устройство, соединяющее отдельные сегменты сети разного типа и обеспечивающее доступ локальной сети к глобальной сети, при этом имеющее возможность управлять трафиком на основе протокола сетевого уровня. 8, 10, 13, 16, 19, 20, 32, 59, 70, 89, 94

Маска подсети (Subnet Mask) IPv4 32-разрядное двоичное число, в разрядах расширенного префикса содержащая единицу, а в остальных разрядах — ноль. 10, 25, 42

Определение маршрута перемещения пакета (маршрутизация)

Процесс, использующий таблицы маршрутизации для определения адреса (сетевое уровня) следующего маршрутизатора или непосредственно получателя по имеющемуся адресу (сетевое уровня), после чего выбирается определённый выходной физический порт маршрутизатора. 88

Повторитель (Repeater) Сетевое устройство для физического соединения двух или более сегментов кабеля локальной сети с целью увеличения общей длины сети. 39

Протокол динамической настройки узла (DHCP) Сетевой протокол, позволяющий узлам сети динамически получать IP-адреса и некоторые другие параметры сети. 42–44

Сетевой коммутатор (Switch) Сетевое устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента и хранящее в памяти таблицу MAC-адресов, в которой указывается соответствие MAC-адреса узла порту коммутатора. 8, 10, 13, 16, 19, 20, 29, 35, 39, 42, 46, 48, 49, 70, 74

Сетевой уровень (Network Layer) ISO/OSI Предоставляет средства установления, поддержания и разрыва сетевого соединения, а также функциональные и процедурные средства для обмена по сетевому соединению сетевыми сервисными блоками данных между транспортными логическими объектами. 19, 21

Система доменных имён (Domain Name System, DNS) Распределённая система, ставящая в соответствие доменному имени сетевого устройства IP-адрес, и наоборот. 42, 43

Физический уровень (Physical Layer) ISO/OSI Обеспечивает передачу битовых потоков без каких-либо изменений между логическими объектами уровня звена данных по физическим соединениям. 19, 20

Широковещание (Broadcast) Пакет передаётся всем узлам сети. 115

Шлюз (Gateway) Сетевое устройство, соединяющее отдельные сегменты сети с разными типами системного и прикладного программного обеспечения. 13

Шлюз по-умолчанию (Default Gateway) Специальный узел, куда необходимо передать дейтаграммы, адрес сети назначения которых не указан в таблице маршрутизации. 42

Эталонная модель взаимодействия открытых систем (ISO/OSI)

Модель стека сетевых протоколов, которая чётко определяет уровни взаимодействия систем, стандартизует имена уровней систем и указывает услуги и функции каждого уровня системы. 19–21, 46

Учебно-методический комплекс

Рекомендуется для направлений подготовки

02.03.01 — «Математика и компьютерные науки»

02.03.02 — Фундаментальная информатика и информационные технологии

09.03.03 «Прикладная информатика»

Квалификация (степень) выпускника: бакалавр

Программа дисциплины

1. Цели и задачи дисциплины

Целью дисциплины является введение учащихся в предметную область администрирования локальных сетей.

В процессе преподавания дисциплины решаются следующие задачи:

- анализ принципов построения сети;
- конфигурирование компьютерных сетей, настройка маршрутизации, VPN, NAT, BGP.

2. Место дисциплины в структуре ОП ВО

Дисциплина относится к вариативной части блока 1 учебного плана.

В табл. 16.3–16.5 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций обучающегося в соответствии с матрицей компетенций ОП ВО по направлениям 02.03.01, 02.03.02, 09.03.03 соответственно.

Таблица 16.3

**Предшествующие и последующие дисциплины, направленные
на формирование компетенций по направлению 02.03.01**

№ п/п	Шифр компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общекультурные компетенции			
1.	-	-	-
Общепрофессиональные компетенции			
1.	ОПК-2	Операционные системы; Компьютерные сети; Сетевые технологии; Администрирование сетевых подсистем	Информационная безопасность
Профессиональные компетенции			
-	-	-	-
Профессионально-специализированные компетенции специализации			
-	-	-	-

Описание компетенций для направления 02.03.01:

ОПК-2 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

Таблица 16.4

**Предшествующие и последующие дисциплины, направленные
на формирование компетенций по направлению 02.03.02**

№ п/п	Шифр компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общекультурные компетенции			
1.	-	-	-
Общепрофессиональные компетенции			
1.	ОПК-2	Операционные системы; Компьютерные сети; Сетевые технологии; Администрирование сетевых подсистем	-
2.	ОПК-4	Компьютерные сети	Информационная безопасность
Профессиональные компетенции			
-	-	-	-
Профессионально-специализированные компетенции специализации			
-	-	-	-

Описание компетенций для направления 02.03.02:

ОПК-2 — способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий;

ОПК-4 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

Описание компетенций для направления 09.03.03:

ОПК-4 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности;

ПК-9 — способность составлять техническую документацию проектов автоматизации и информатизации прикладных процессов;

ПК-13 — способность осуществлять установку и настройку параметров программного обеспечения информационных систем.

Таблица 16.5

**Предшествующие и последующие дисциплины, направленные
на формирование компетенций по направлению 09.03.03**

№ п/п	Шифр компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общекультурные компетенции			
1.	-	-	-
Общепрофессиональные компетенции			
1.	ОПК-4	Вычислительные системы; сети и телекоммуникации; Сетевые технологии	Информационная безопасность
Профессиональные компетенции — проектная деятельность			
1.	ПК-9	Сетевые технологии; Администрирование сетевых подсистем	Информационная безопасность
Профессиональные компетенции — производственно-технологическая деятельность			
1.	ПК-13	Операционные системы; Основы администрирования операционных систем; Сетевые технологии; Администрирование сетевых подсистем	Информационная безопасность
Профессионально-специализированные компетенции специализации			
-	-	-	-

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: ОПК-2 (по направлениям 02.03.01 и 02.03.02) и ОПК-4, ПК-9, ПК-13 (по направлению 09.03.03).

В результате изучения дисциплины студент должен:

Знать:

- основы конфигурирования компьютерных сетей;
- основы настройки маршрутизации, NAT, VPN и т.д.

Уметь:

- применять в профессиональной, исследовательской и прикладной деятельности современные сетевые технологии, международные и профессиональные стандарты в области сетевых технологий;
- осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в сети Интернет, отслеживать динамику развития направлений в области сетевых технологий;

- применять на практике международные и профессиональные стандарты сетевых технологий, современные парадигмы и методологии, инструментальные средства, относящиеся к сетевым технологиям.

Владеть:

- навыками планирования сети и адресного пространства организации;
- навыками конфигурирования коммутационного и сетевого оборудования.

4. Объем дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет 3 зачётные единицы.

Вид учебной работы	Всего часов	Семестры
		6
Аудиторные занятия (всего)	54	54
В том числе:		
<i>Лекции</i>	18	18
<i>Практические занятия (ПЗ)</i>	-	-
<i>Семинары (С)</i>	-	-
<i>Лабораторные работы (ЛР)</i>	36	36
Самостоятельная работа (всего)	54	54
Общая трудоёмкость:		
час.	108	108
зач. ед.	3	3

5. Содержание дисциплины

5.1 Содержание разделов дисциплины

Раздел 1. Администрирование коммутируемой сети.

Тема 1. Программное средство Cisco PacketTracer.

Тема 2. Предварительная настройка оборудования Cisco.

Тема 3. Планирование сети.

Тема 4. Первоначальное конфигурирование сети.

Тема 5. Конфигурирование VLAN.

Тема 6. Статическая маршрутизация VLAN.

Тема 7. Учёт физических параметров сети.

Тема 8. Использование протокола STP. Агрегирование каналов.

Раздел 2. Администрирование маршрутизируемой сети.

Тема 9. Настройка сетевых сервисов. DHCP.

Тема 10. Настройка списков управления доступом (ACL).

Тема 11. Настройка NAT. Планирование.

Тема 12. Настройка NAT.

Тема 13. Статическая маршрутизация в Internet. Планирование.

Тема 14. Статическая маршрутизация в Internet. Настройка.

Тема 15. Динамическая маршрутизация.

Тема 16. Настройка VPN.

5.2 Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	Се-мин.	СРС	Всего час.
1.	Администрирование коммутируемой сети	9		18		27	54
2.	Администрирование маршрутизируемой сети	9		18		27	54
Итого:		18		36		54	108

6. Лабораторный практикум

Раздел 1. Администрирование коммутируемой сети.

Лабораторная работа 1. Программное средство Cisco PacketTracer.

Лабораторная работа 2. Предварительная настройка оборудования Cisco.

Лабораторная работа 3. Планирование сети.

Лабораторная работа 4. Первоначальное конфигурирование сети.

Лабораторная работа 5. Конфигурирование VLAN.

Лабораторная работа 6. Статическая маршрутизация VLAN.

Лабораторная работа 7. Учёт физических параметров сети.

Лабораторная работа 8. Использование протокола STP. Агрегирование каналов.

Раздел 2. Администрирование маршрутизируемой сети.

Лабораторная работа 9. Настройка сетевых сервисов. DHCP.

Лабораторная работа 10. Настройка списков управления доступом (ACL).

Лабораторная работа 11. Настройка NAT. Планирование.

Лабораторная работа 12. Настройка NAT.

Лабораторная работа 13. Статическая маршрутизация в Интернете. Планирование.

Лабораторная работа 14. Статическая маршрутизация в Интернете. Настройка.

Лабораторная работа 15. Динамическая маршрутизация.

Лабораторная работа 16. Настройка VPN.

7. Практические занятия (семинары)

Практические занятия (семинары) не предусмотрены.

8. Материально-техническое обеспечение дисциплины

Дисплейные классы ДК3, ДК4, ДК6 (Москва, ул. Орджоникидзе, д. 3, корп. 5) с компьютеризированными рабочими местами обучающихся с процессором Intel Core i3-550 3.2 GHz или выше.

9. Информационное обеспечение дисциплины

- а) программное обеспечение: ОС Linux, PacketTracer.
- б) базы данных, информационно-справочные и поисковые системы: Request for Comments (RFC) — <https://www.ietf.org/rfc.html>.

10. Учебно-методическое обеспечение дисциплины

- а) Основная литература:
- 1. Кулябов Д.С., Королькова А.В. Администрирование локальных сетей. Лабораторные работы: учебное пособие. — Москва: РУДН, 2017.
- 2. Документация по продуктам Cisco. URL: <http://www.cisco.com>.
- б) Дополнительная литература
- 1. Jesin A. Packet Tracer Network Simulator. — Packt Publishing, 2014. — 134 p.
- 2. Сети и системы передачи информации: телекоммуникационные сети: учебник и практикум для вузов / Самуйлов К. Е., Шалимов И. А., Васин Н. Н., Василевский В. В., Кулябов Д. С., Королькова А. В. — Изд-во Юрайт, 2016.
- 3. Королькова А.В., Кулябов Д.С. Сетевые технологии: лабораторные работы: учебное пособие. — Москва: РУДН, 2014. — 106 с.: ил. ISBN 978-5-209-05606-5.
- 4. Самуйлов К.Е., Кулябов Д.С., Королькова А.В., Гайдамака Ю.В., Гудкова И.А., Абаев П.О. Современные концепции управления инфокоммуникациями [Текст]: учебно-методический комплекс. — М.: РУДН, 2013. — 234 с.
- 5. Кулябов Д.С., Королькова А.В. Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М.: РУДН, 2008. — <http://lib.rudn.ru/polnotekstovye-knigi/61-Kulyabov.pdf>.

11. Методические указания для обучающихся по освоению дисциплины

Учебным планом на изучение дисциплины отводится один семестр. В дисциплине предусмотрены лекции, лабораторный практикум, контрольные мероприятия. В конце семестра проводится итоговый контроль знаний.

11.1 Методические указания по самостоятельному освоению теоретического материала по дисциплине

Лекционный материал дисциплины охватывает темы, указанные в разделе 5.1 программы дисциплины. В ТУИС (<http://esystem.pfur.ru>) по темам лекций размещены презентации. Рекомендуется по указанным темам в дополнение к презентациям изучить литературу, указанную в п. 10 программы дисциплины.

11.2 Методические указания по выполнению лабораторных работ

Задания по лабораторным работам выполняются индивидуально каждым студентом в дисплейных классах в соответствии с календарным планом и методическими указаниями по выполнению лабораторных работ по дисциплине. Часть лабораторных работ предусматривает задания для индивидуальной самостоятельной работы студента, обязательные для выполнения. Выполнение заданий для самостоятельной работы позволяет студенту приобрести дополнительные навыки и закрепить знания по изучаемой теме.

По результатам выполнения каждой лабораторной работы студентом готовится отчёт. Отчёты в электронном виде сдаются студентом на проверку через соответствующие разделы ТУИС (<http://esystem.pfur.ru>).

11.3. Методические указания по подготовке к контрольным мероприятиям

Контрольные мероприятия по дисциплине проводятся в форме тестирования в ТУИС (<http://esystem.pfur.ru>). Итоговый контроль в форме теста проводится по темам всех разделов дисциплины. Вопросы для подготовки к промежуточному и итоговому тестированию размещены в соответствующем разделе ТУИС (<http://esystem.pfur.ru>).

Паспорт фонда оценочных средств

Код компетенции	Контролируемый раздел	Контролируемая тема	ФОСы		Баллы темы	Баллы раздела
			Ауд. раб.	За-чёт		
			Вып. ЛР	Итог. контроль		
ОПК-2 (для направлений 02.03.01 и 02.03.02); ОПК-4, ПК-9, ПК-13 (для направления 09.03.03)	Администрирование коммутлируемой сети	Программное средство Cisco PacketTracer	5	10	6	50
		Предварительная настройка оборудования Cisco	5		6	
		Планирование сети	5		6	
		Первоначальное конфигурирование сети	5		6	
		Конфигурирование VLAN	5		7	
		Статическая маршрутизация VLAN	5		7	
		Учёт физических параметров сети	5		6	
		Использование протокола STP. Агрегирование каналов	5		6	
	Администрирование маршрутизируемой сети	Настройка сетевых сервисов. DHCP	5	10	6	50
		Настройка списков управления доступом (ACL)	5		6	
		Настройка NAT. Планирование	5		6	
		Настройка NAT	5		6	
		Статическая маршрутизация в Интернете. Планирование	5		7	
		Статическая маршрутизация в Интернете. Настройка	5		7	
		Динамическая маршрутизация	5		6	
		Настройка VPN	5		6	
Итого:			80	20	100	100

Описание компетенций для направления 02.03.01:

ОПК-2 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

Описание компетенций для направления 02.03.02:

ОПК-2 — способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий.

Описание компетенций для направления 09.03.03:

ОПК-4 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности;

ПК-9 — способность составлять техническую документацию проектов автоматизации и информатизации прикладных процессов;

ПК-13 — способность осуществлять установку и настройку параметров программного обеспечения информационных систем.

Фонд оценочных средств

Балльно-рейтинговая система оценки уровня знаний

Сводная оценочная таблица дисциплины

Раздел	Тема	Формы контроля		Баллы темы	Баллы раздела
		Ауд. раб.	За- чёт		
		Вып. ЛР	Итог. кон- троль		
Администрирование коммутационной сети	Программное средство Cisco PacketTracer	5	10	6	50
	Предварительная настройка оборудования Cisco	5		6	
	Планирование сети	5		6	
	Первоначальное конфигурирование сети	5		6	
	Конфигурирование VLAN	5		7	
	Статическая маршрутизация VLAN	5		7	
	Учёт физических параметров сети	5		6	
	Использование протокола STP. Агрегирование каналов	5		6	
Администрирование маршрутизируемой сети	Настройка сетевых сервисов. DHCP	5	10	6	50
	Настройка списков управления доступом (ACL)	5		6	
	Настройка NAT. Планирование	5		6	
	Настройка NAT	5		6	
	Статическая маршрутизация в Интернете. Планирование	5		7	
	Статическая маршрутизация в Интернете. Настройка	5		7	
	Динамическая маршрутизация	5		6	
	Настройка VPN	5		6	
Итого:		80	20	100	100

Таблица соответствия баллов и оценок

Баллы БРС	Традиционные оценки РФ	Оценки ECTS
95–100	5	A
86–94		B
69–85	4	C
61–68	3	D
51–60		E
31–50	2	FX
0–30		F
51–100	Зачёт	Passed

Правила применения БРС

1. Раздел (тема) учебной дисциплины считается освоенным, если студент набрал более 50% от возможного числа баллов по этому разделу (теме).
2. Студент не может быть аттестован по дисциплине, если он не освоил все темы и разделы дисциплины, указанные в сводной оценочной таблице дисциплины.
3. По решению преподавателя и с согласия студентов, не освоивших отдельные разделы (темы) изучаемой дисциплины, в течение учебного семестра могут быть повторно проведены мероприятия текущего контроля успеваемости или выданы дополнительные учебные задания по этим темам или разделам. При этом студентам за данную работу засчитывается минимально возможный положительный балл (51% от максимального балла).
4. При выполнении студентом дополнительных учебных заданий или повторного прохождения мероприятий текущего контроля полученные им баллы засчитываются за конкретные темы. Итоговая сумма баллов не может превышать максимальное количество баллов, установленное по данным темам (в соответствии с приказом Ректора № 564 от 20.06.2013). По решению преподавателя предыдущие баллы, полученные студентом по учебным заданиям, могут быть аннулированы.
5. График проведения мероприятий текущего контроля успеваемости формируется в соответствии с календарным планом курса. Студенты обязаны сдавать все задания в сроки, установленные преподавателем.
6. Время, которое отводится студенту на выполнение мероприятий текущего контроля успеваемости, устанавливается преподавателем. По завершении отведённого времени студент должен сдать работу преподавателю, вне зависимости от того, завершена она или нет.
7. Использование источников (в том числе конспектов лекций и лабораторных работ) во время выполнения контрольных мероприятий возможно только с разрешения преподавателя.

8. Отсрочка в прохождении мероприятий текущего контроля успеваемости считается уважительной только в случае болезни студента, что подтверждается наличием у него медицинской справки, заверенной круглой печатью в поликлинике № 25, предоставляемой преподавателю не позднее двух недель после выздоровления. В этом случае выполнение контрольных мероприятий осуществляется после выздоровления студента в срок, назначенный преподавателем. В противном случае отсутствие студента на контрольном мероприятии признается неуважительным.
9. Студент допускается к итоговому контролю знаний с любым количеством баллов, набранных в семестре.
10. Итоговый контроль знаний оценивается из 20 баллов, независимо от числа баллов за семестр.
11. Если в итоге за семестр студент получил менее 31 балла, то ему выставляется оценка F и студент должен повторить эту дисциплину в установленном порядке. Если же в итоге студент получил 31–50 баллов, т.е. FX, то студенту разрешается добор необходимого (до 51) количества баллов путем повторного однократного выполнения предусмотренных контрольных мероприятий, при этом по усмотрению преподавателя аннулируются соответствующие предыдущие результаты. Ликвидация задолженностей проводится в период с 07.02 по 28.02 (с 07.09 по 28.09) по согласованию с деканатом.

Критерии оценки по дисциплине

95–100 баллов:

- полное и своевременное выполнение на высоком уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы, умение делать обоснованные выводы;
- безупречное владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- выраженная способность самостоятельно и творчески решать поставленные задачи;
- полная самостоятельность и творческий подход при изложении материала по программе дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной программой дисциплины и преподавателем.

86–94 балла:

- полное и своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

- хорошее владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать поставленные задачи в нестандартных производственных ситуациях;
- усвоение основной и дополнительной литературы, нормативных и законодательных актов, рекомендованных программой дисциплины и преподавателем.

69–85 баллов:

- своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- хороший уровень культуры исполнения лабораторных работ;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать проблемы в рамках программы дисциплины;
- усвоение основной литературы.

51–68 баллов:

- выполнение на удовлетворительном уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- удовлетворительное владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

31–50 баллов, НЕ ЗАЧТЕНО:

- невыполнение, несвоевременное выполнение или выполнение на неудовлетворительном уровне лабораторных работ, непрохождение контрольных мероприятий, предусмотренных программой курса;
- недостаточно полный объем навыков и компетенции в рамках программы дисциплины;
- неумение использовать в практической деятельности научной терминологии, изложение ответа на вопросы с существенными стилистическими и логическими ошибками;
- слабое владение программным обеспечением по разделам программы дисциплины, некомпетентность в решении стандартных (типовых) производственных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы.

0–30 баллов, НЕ ЗАЧТЕНО:

- отсутствие умений, навыков, знаний и компетенций в рамках программы дисциплины;
- невыполнение лабораторных заданий, непрохождение контрольных мероприятий, предусмотренных программой курса; отказ от ответов по программе дисциплины;
- игнорирование занятий по дисциплине по неуважительной причине.

Примерный перечень оценочных средств

п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Аудиторная работа			
1.	Лабораторная работа	Система практических заданий, направленных на формирование практических навыков у обучающихся	Фонд практических заданий
2.	Тест	Система стандартизированных заданий (вопросов), позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	База тестовых заданий
3.	Зачёт	Форма проверки качества выполнения студентами лабораторных работ, домашних заданий и др. заданий контрольных мероприятий в соответствии с утверждённой программой	Примеры заданий
Самостоятельная работа			
1.	Подготовка отчётов по результатам выполнения лабораторных работ	Форма проверки качества выполнения студентами лабораторных работ в соответствии с утверждённой программой	Фонд практических заданий в рамках лабораторного практикума по дисциплине

Учебным планом на изучение дисциплины отводится один семестр. В дисциплине предусмотрены лекции, лабораторный практикум, контрольные мероприятия. В конце семестра проводится итоговый контроль знаний.

Оценивание результатов освоения дисциплины производится в соответствии с балльно-рейтинговой системой. По дисциплине предусмотрен зачёт.

Итоговый контроль знаний по дисциплине проводится в форме тестирования, но при необходимости зачет может проводиться в форме письменного ответа на вопросы из билетов.

Комплект заданий для итогового контроля знаний

Итоговый контроль знаний по дисциплине проводится в форме компьютерного тестирования.

1. Как можно узнать состояние агрегированного канала EtherChannel?
2. Какие из идентификаторов соответствуют порту Fast Ethernet?
3. Какой тип кабеля применяется для соединения с консольным портом Cisco?
4. Для чего используется AUX порт на Cisco?
5. Вы конфигурируете DCE окончание последовательного соединения типа точка-точка. Какую из команд вы зададите?
6. В какой порт маршрутизатора подключается внешний CSU/DSU интерфейс?
7. Какой тип модуля используется для установки внутреннего CSU/DSU интерфейса?
8. Где хранится рабочая конфигурация устройств Cisco?
9. Что из ниже перечисленного сохраняется в ROM на устройствах Cisco?
10. Какая команда используется для сохранения рабочей конфигурации устройств Cisco в качестве стартовой?
11. Где ищется образ Cisco IOS при загрузке маршрутизатора Cisco?
12. Где находится стартовая конфигурация при первой загрузке маршрутизатора Cisco?
13. Вы подсоединяетесь к коммутатору для удалённого администрирования. Какую команду вы используете?
14. Как сконфигурировать протокол удалённого подключения?
15. Какая команда позволяет переходить от привилегированного режима к пользовательскому?
16. Как получить список параметров команды ping?
17. Какое из приглашений представляет режим глобальной конфигурации?
18. Какая команда переводит устройство в режим глобальной конфигурации?
19. Какие операции можно выполнить, когда в Cisco IOS стоит приглашение R1(config-if)#?
20. Какая команда на устройствах Cisco запускает диалог первоначальной конфигурации?
21. При каких условиях появляется диалог первоначальной конфигурации?
22. Каково предназначение POST?
23. Что произойдёт, если маршрутизатор запустится без стартовой конфигурации?
24. С помощью какой команды можно посмотреть количество портов Fast Ethernet?
25. С помощью какой команды можно посмотреть версию Cisco IOS?
26. С помощью какой команды можно посмотреть значение регистра конфигурации?
27. Как задать широковещательный адрес (broadcast address) сети?
28. Вам надо разбить сеть 129.65.0.0 на 6 подсетей. Какую маску подсети вы должны задать?
29. Какова будет маска для сети 135.44.33.22/20?
30. Вам надо разбить сеть 142.65.0.0 на 12 подсетей. Какую маску подсети вы должны задать?
31. Сколько бит на хостовую часть нужно выделить для 1010 систем?
32. Сколько бит нужно замаскировать для создания 20 подсетей?
33. Как можно выделить префикс сети?

34. Сколько хостов может быть в сети 180.45.10.20/20?
35. Сколько бит нужно выделить, чтобы создать 6 подсетей?
36. Какую опцию на маршрутизаторе Cisco следует задать, чтобы можно было использовать нулевую и широковещательную сети?
37. Система имеет адрес 145.68.23.45/25. Сколько систем может быть в данной подсети?
38. Какую маску следует выбрать, чтобы в подсети можно было присвоить 92 адреса?
39. Какое минимальное число хостовых битов в маске необходимо для поддержки 510 хостов?
40. Вам нужно разделить на подсети сеть 137.15.0.0 так, чтобы в каждой подсети можно было разместить по 8190 хостов. Какова будет маска, при условии, что вы используете наименьшие размеры подсети?
41. Сколько хостов можно разместить в сети 201.10.20.30/27?
42. Какую маску следует выбрать, чтобы в подсети можно было присвоить 60 адресов?
43. Какая из сетей является третьей подсетью в сети 220.55.66.0/27?
44. Вы соединяете две сети для подключения к одному WAN-линку. Какую из масок подсети вы будете использовать на WAN-интерфейсах для оптимизации использования адресного пространства?
45. Какой протокол устанавливает соответствие между логическим и физическим адресами?
46. На какой адрес 2-го уровня посылается ARP-запрос?

Критерии оценки итогового тестирования

Итоговое тестирование оценивается в соответствии с БРС и паспортом ФОС. Проверяется правильность ответов на вопросы теста.

Комплект разноуровневых задач (заданий)

1. Задания репродуктивного уровня

В качестве заданий репродуктивного уровня предлагаются вопросы для самопроверки и обсуждения по темам курса (см. лабораторный практикум).

2. Задания реконструктивного уровня

В качестве заданий реконструктивного уровня предполагаются задания лабораторного практикума.

Критерии оценки выполнения заданий по лабораторным работам

Оцениваются полнота выполнения работы, оформление результатов, полнота ответов на контрольные вопросы, если это предусмотрено заданием.

Сведения об авторах

Кулябов Дмитрий Сергеевич — доцент, кандидат физико-математических наук, доцент кафедры прикладной информатики и теории вероятностей РУДН.

Королькова Анна Владиславовна — доцент, кандидат физико-математических наук, доцент кафедры прикладной информатики и теории вероятностей РУДН.

Учебное издание

Дмитрий Сергеевич Кулябов
Анна Владиславовна Королькова

Администрирование локальных систем

Редактор *И. Л. Панкратова*
Технический редактор *Н. А. Ясько*
Дизайн обложки *Ю. Н. Ефремова*
Компьютерная вёрстка *А. В. Королькова, Д. С. Кулябов*

Тематический план изданий
учебной и научной литературы 2017 г., № 13

Подписано в печать 02.11.2017 г. Формат 60×84/16. Печать офсетная.
Усл. печ. л. 7,5. Тираж 500 экз. Заказ № 1703.

Российский университет дружбы народов
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3

Типография РУДН
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3, тел. 952-04-41