

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**  
**ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»**

---

**ВЫСШАЯ ШКОЛА ТЕХНОЛОГИИ И ЭНЕРГЕТИКИ**

# **АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ**

**Методические указания по выполнению  
курсовой работы**

**Санкт-Петербург**  
**2017**

УДК 681.3 (075)

ББК 73я7

П770

Администрирование информационных систем: методические указания по выполнению курсовой работы по дисциплине «Администрирование информационных систем» для студентов института энергетики и автоматизации /сост. Стеклова Г.А, Тихов С.В. ВШТЭ СПб ГУПТД. - СПб., 2017. – 39 с.

Методические указания разработаны в соответствии с программой курса «Администрирование информационных систем» Федерального государственного образовательного стандарта для бакалавров по направлению подготовки 01.03.02 «Прикладная математика и информатика».

Рецензенты: канд. техн. наук., доцент кафедры «Вычислительная техника» Санкт-Петербургского государственного электротехнического университета (ЛЭТИ) Дудкин В.С.;

канд. техн. наук., доцент кафедры «Прикладная математика и информатика» ВШТЭ СПбГУПТД Антонюк П.Е.

Подготовлены и рекомендованы к печати кафедрой прикладной математики и информатики ВШТЭ СПбГУПТД (протокол № 10 от 24.05.2017 г.).

Утверждены к изданию методической комиссией института энергетики и автоматизации ВШТЭ СПбГУПТД (протокол № 8 от 30.06.2017 г.).

Рекомендованы к изданию Редакционно-издательским советом ВШТЭ СПбГУПТД

В авторской редакции

Темплан 2017, поз. 129

Подп. к печати 27.12.2017. Формат 60х84/16. Бумага тип № 1.

Печать офсетная. Объем 2,43 печ.л.; 2,43 уч. изд.л. Тираж 30 экз. Изд. № 129, Цена “С”. Заказ

---

Ризограф Высшей школы технологии и энергетики СПбГУПТД, СПб., 198095, ул. Ивана Черных, 4.

© Высшая школа технологии и энергетики СПбГУПТД, 2017

© Стеклова Г.А., Тихов С.В., 2017

### **Введение.**

Дисциплина "Администрирование информационных систем" имеет целью сформировать у студентов компетенции в области теоретических и практических основ организации и функционирования компьютерных сетей. В практическом аспекте в результате освоения данной дисциплины студенты должны:

- владеть навыками поиска и обмена информации в глобальных и локальных компьютерных сетях; техническими и программными средствами защиты информации при работе с сетевыми программными средствами;
- уметь производить установку, настройку, базовое конфигурирование серверных и клиентских операционных систем;
- владеть основами автоматизации решения задач в профессиональной деятельности в соответствии с направлениями обучения.

Методические указания разработаны в соответствии с программой курса «Администрирование информационных систем» Федерального государственного образовательного стандарта для бакалавров по направлению подготовки 01.03.02 «Прикладная математика и информатика».

Работа состоит из трех разделов, введения, заключения и списка литературы.

## **1. Описание пакета программ Cisco Packet Tracer**

Cisco Packet Tracer (CPT) - это пакет программ для эмуляции работы компьютерных сетей. Пакет программ позволяет создавать визуальные модели сети, производить настройку элементов этой сети при помощи графического интерфейса и команд Cisco IOS. Пакет позволяет эмулировать работу конкретных сетевых и пользовательских устройств: коммутаторов, маршрутизаторов, серверов, рабочих станций. Предоставляет возможности устанавливать различные модули расширения в серверы, компьютеры, коммутаторы и маршрутизаторы. Пакет программ позволяет создавать макеты компьютерных сетей довольно сложных топологий, проверять работоспособность и проводить исследования.

Пакет Cisco Packet Tracer выполняет следующие основные функции, позволяющие исследовать принципы построения и функционирования компьютерных сетей с применением различных активных сетевых коммуникационных и пользовательских устройств:

- Визуальное построение сети, содержащей активное оборудование, оконечные устройства и линии связи;
- Настройка активного оборудования через консоль (клавиатуру) по интерфейсу командной строки CLI (интерфейс командной строки – это средство взаимодействия с компьютерной программой, когда пользователь формирует команды в форме текстовых строк); применяется метод, используемый в современном оборудовании;
- Настройка основных параметров активного оборудования через графический интерфейс;
- Добавление модулей активных устройств (сетевые карты, модули для Cisco и т.д.) в среде эмуляции, аналогичное подключению дополнительных модулей в реальном оборудовании;
- Эмуляция включения и настройки различных сервисов в рабочих станциях (почта, WEB, командная строка и т.д.) и демонстрация их работы;
- Наблюдение за прохождением пакетов по сети и поддержка нескольких десятков различных протоколов в визуальном режиме;
- Создание физической схемы сети (в пределах стойки, комнаты, этажа, здания, города).

Наименования и функции для основных полей главного окна Cisco Packet Tracer (рис.1) приведены ниже:

- Главное меню содержит стандартные для многих программ меню: Файл, Правка, Настройки, Вид, Инструменты, Расширения, Помощь. Особого внимания заслуживает меню «Расширения», содержащее мастер проектов, многопользовательский режим и ряд других дополнительных функций;
- Переключатель логической и физической организации рабочего пространства;
- Панель инструментов, содержащая средства выделения, удаления, перемещения, масштабирования объектов, а также формирования и передачи пакетов данных (PDU) между устройствами;

- Панель выбора устройств, конечных станций и линий связи;
- Панель создания пользовательских сценариев;
- Рабочее пространство.

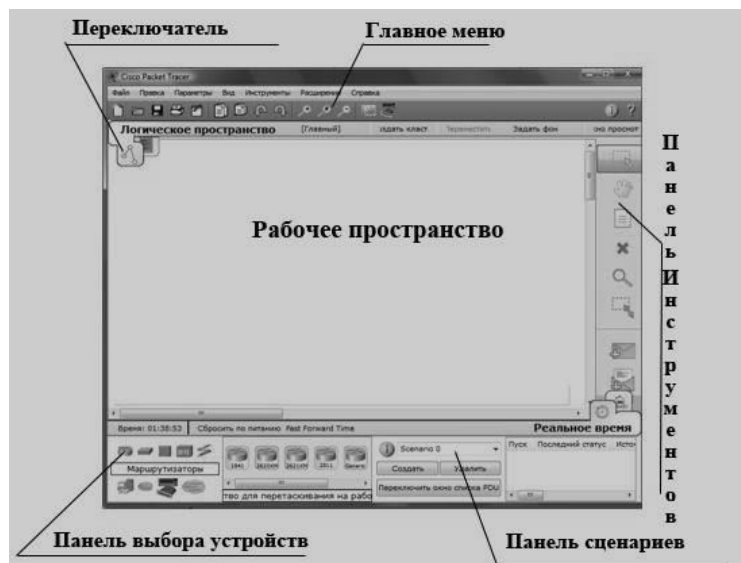


Рис.1. Интерфейс Cisco Packet Tracer

## 2. Задание и структура курсовой работы

Целью курсовой работы является приобретение навыков по базовому конфигурированию компьютерной сети и включает в себя:

- настройку коммутаторов и маршрутизаторов;
- декомпозицию сети на несколько подсетей;
- статическую и динамическую маршрутизацию;
- фильтрацию трафика по листам доступа.

Структурными элементами курсовой работы являются: титульный лист, задание, оглавление, введение, основная часть, заключение, список литературы, приложения.

*Титульный лист* курсовой работы должен содержать следующие сведения:

- полное наименование учебного заведения, отделение;
- название темы курсовой работы;
- название вида документа;
- сведения об исполнителе (ФИО студента, номер группы, подпись), сведения о преподавателе (руководителе) (ФИО, подпись);
- наименование места и года выполнения.

В *задании* указывают:

- тему курсового проекта;
- перечень основных вопросов, подлежащих изучению и разработке;
- срок сдачи курсового проекта.

*Оглавление* должно содержать перечень структурных элементов курсового проекта с указанием номеров страниц, с которых начинается их

местоположение в тексте, в том числе:

- введение;
- главы, параграфы, пункты;
- заключение;
- список литературы;
- обзор литературы;
- приложения.

Текст *введения* должен кратко раскрывать актуальность и значение темы.

*Основная часть* должна содержать обзор литературы по изучаемому вопросу, развёрнутые ответы на поставленные вопросы, подробное решение предложенных задач, а также дополнительные сведения.

В *заключении* должны быть приведены выводы о положительных и отрицательных моментах, которые были подмечены при изучении поставленного вопроса, о сильных и слабых сторонах рассматриваемых методов решения задач.

Список литературы должен содержать библиографический перечень источников (включая и Интернет-ресурсы), информация из которых использовалась при выполнении курсовой работы.

В случае необходимости в курсовую работу допускается включать приложения. Приложения должны содержать дополнительную информацию по изучаемой предметной области, не вошедшую в основную часть.

Необходимо выполнить проектирование и настройку компьютерной сети, представленной на рис.2. Общими исходными данными для курсовой работы являются:

- Тип организации сети: клиент-сервер;
- Адресация IP: по классу С.

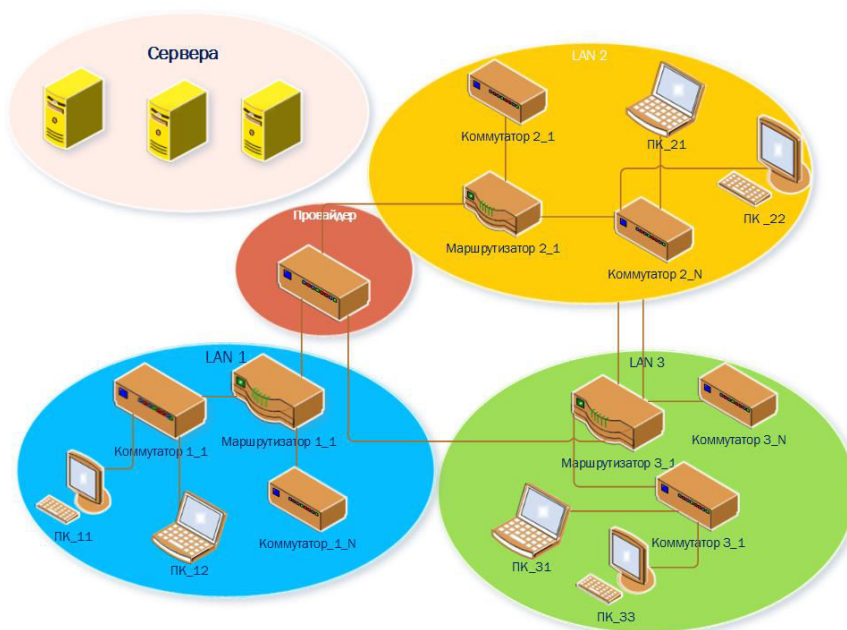


Рис.2. Общая схема сети

Другие исходные данные для проектирования выбираются студентом из приведенных ниже данных (табл.1.) самостоятельно с учетом своего шифра (порядкового номера в ведомости).

Таблица 1. Варианты задания

| № варианта                                     | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 10 | 12 | 13 | 14 | 15 | 16 |
|------------------------------------------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| <b>Количество подсетей (VLAN)</b>              | 8 | 6 | 8 | 7 | 6 | 7 | 9 | 7 | 6 | 7  | 6  | 7  | 6  | 7  | 9  | 9  |
| <b>Минимальное количество ПК в каждой VLAN</b> | 3 | 4 | 4 | 4 | 4 | 3 | 5 | 4 | 6 | 4  | 4  | 4  | 5  | 4  | 4  | 4  |

*Начальный IP адрес и маска для проектируемой сети по вариантам:*

1. 192.168.10.0 255.255.255.0  
Хост(min): 192.168.10.1  
Хост(max): 192.168.10.254
2. 192.168.11.0 255.255.255.0  
Хост(min): 192.168.11.1  
Хост(max): 192.168.11.254
3. 192.168.12.0 255.255.255.0  
Хост(min): 192.168.12.1  
Хост(max): 192.168.12.254
4. 192.168.14.0 255.255.255.0  
Хост(min): 192.168.14.1  
Хост(max): 192.168.14.254
5. 192.168.15.0 255.255.255.0  
Хост(min): 192.168.15.1  
Хост(max): 192.168.15.254
6. 192.168.16.0 255.255.255.0  
Хост(min): 192.168.16.1  
Хост(max): 192.168.16.254
7. 192.168.17.0 255.255.255.0  
Хост(min): 192.168.17.1  
Хост(max): 192.168.17.254
8. 192.168.18.0 255.255.255.0  
Хост(min): 192.168.18.1  
Хост(max): 192.168.18.254
9. 192.168.19.0 255.255.255.0  
Хост(min): 192.168.19.1  
Хост(max): 192.168.19.254
10. 192.168.20.0 255.255.255.0  
Хост(min): 192.168.20.1  
Хост(max): 192.168.20.254
11. 192.168.21.0 255.255.255.0  
Хост(min): 192.168.21.1  
Хост(max): 192.168.21.254
12. 192.168.22.0 255.255.255.0  
Хост(min): 192.168.22.1

Хост(max):192.168.22.254

13. 192.168.23.0 255.255.255.0

Хост(min): 192.168.23.1

Хост(max):192.168.23.254

14. 192.168.24.0 255.255.255.0

Хост(min): 192.168.24.1

Хост(max):192.168.24.254

15. 192.168.25.0 255.255.255.0

Хост(min): 192.168.5.1

Хост(max):192.168.5.254

16. 192.168.26.0 255.255.255.0

Хост(min): 192.168.15.1

Хост(max):192.168.15.254

При выполнении курсовой работы рекомендуется соблюдать следующую последовательность:

1. Подготовить структурную схему сети и задать IP-адреса:

- дать названия всем устройствам сети;
- составить таблицу VLAN;
- составить IP план выделив диапазон адресов для каждого из VLAN;
- составить таблицу подключения оборудования по портам.

*Примечание. Серверную ферму можно подключить к любой локальной сети как отдельную VLAN.*

2. Настроить VLAN, access и trunk порты.

- дать названия всем VLAN;
- настроить все access-порты и задать им имя;
- настроить все trunk порты и задать им имя.

3. Настроить маршрутизацию между VLAN в каждой локальной сети.

4. Настроить порт подключения к провайдеру.

5. Настроить (прописать) статическую маршрутизацию между любыми тремя хостами, расположенными в разных локальных сетях.

6. Настроить динамическую маршрутизацию между всеми хостами сети используя протоколы RIP или OSPF.

7. Настроить сервера: WEB, DHCP.

8. Разрешить доступ к серверу FTP для одного PC из каждой локальной сети для всех остальных запретить.

### **3. Пример выполнения курсовой работы**

Исходные данные:

- Тип организации сети: клиент-сервер;
- Адресация IP: по классу C;
- Количество VLAN 6;
- Минимальное количество ПК в каждой VLAN 3.

Начальный IP адрес и маска для проектируемой сети:

**192.168.13.0 255.255.255.0**

**Хост(min): 192.168.13.1**  
**Хост(max): 192.168.13.254**

### 3.1. Подготовка структурной схемы сети и задание IP-адресов

#### 3.1.1. Разработка структурной схемы сети

Есть четыре группы пользователей: бухгалтерия (Accounting), финансово-экономический отдел (FEO), производственно-технический отдел (PTO), другие пользователи (Ether). А также есть сервера (Server), которые вынесены в отдельную группу. Все группы разграничены и не имеют прямого доступа друг к другу.

На представленной схеме (рис. 3) ядром будет маршрутизатор 2811 в каждой локальной сети, коммутатор 2960-24TT (provider) отнесём к уровню распространения, поскольку на нём соединяются все VLAN в общий канал связи. Коммутаторы 2950T-24 будут устройствами доступа. К ним будут подключаться конечные пользователи, офисная техника, сервера.

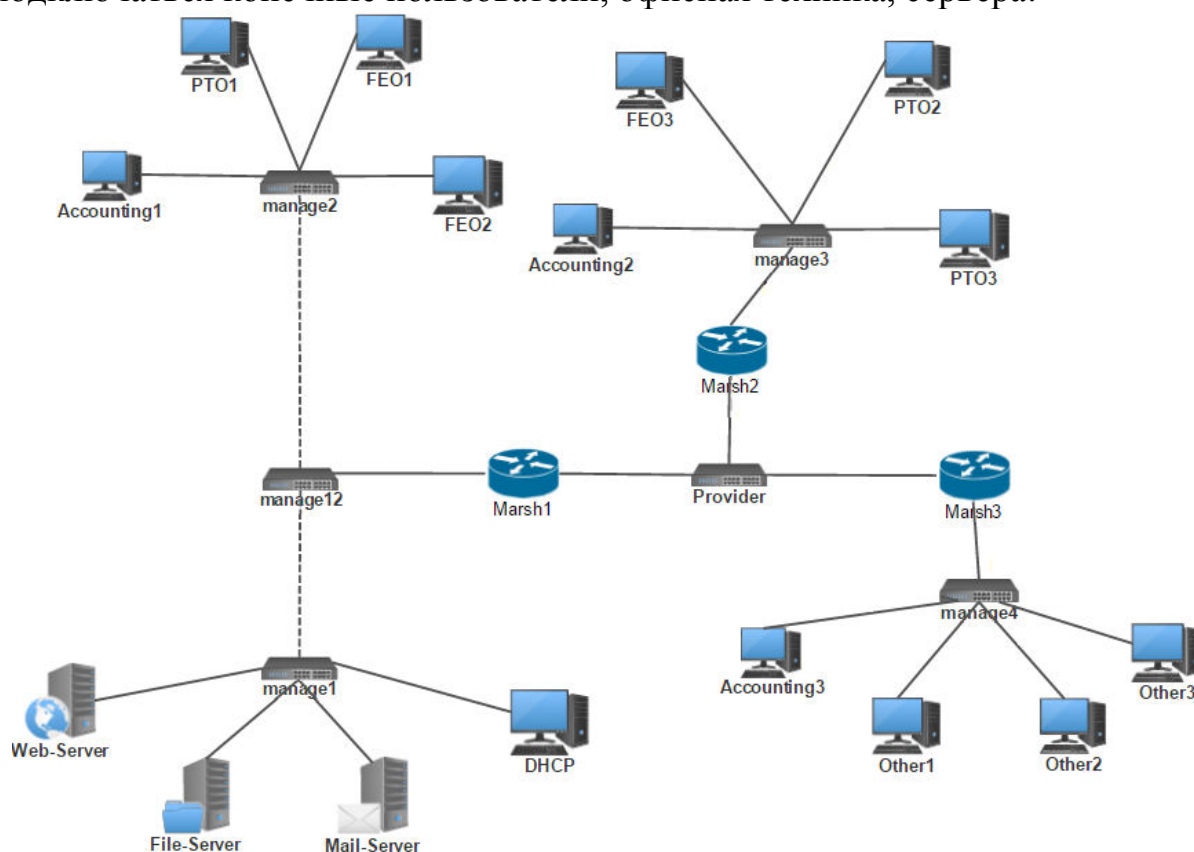


Рис. 3. Структурная схема проектируемой сети

#### 3.1.2 Создание теоретической схемы сетей уровня L-1, L-2, L-3

На схеме L1 (рис.4) изображены физические устройства сети с номерами портов: что куда подключено, на схеме L2 (рис.5) – показаны подключение устройств по VLAN, а на рис. 6 схема взаимодействия устройств сети на третьем уровне.

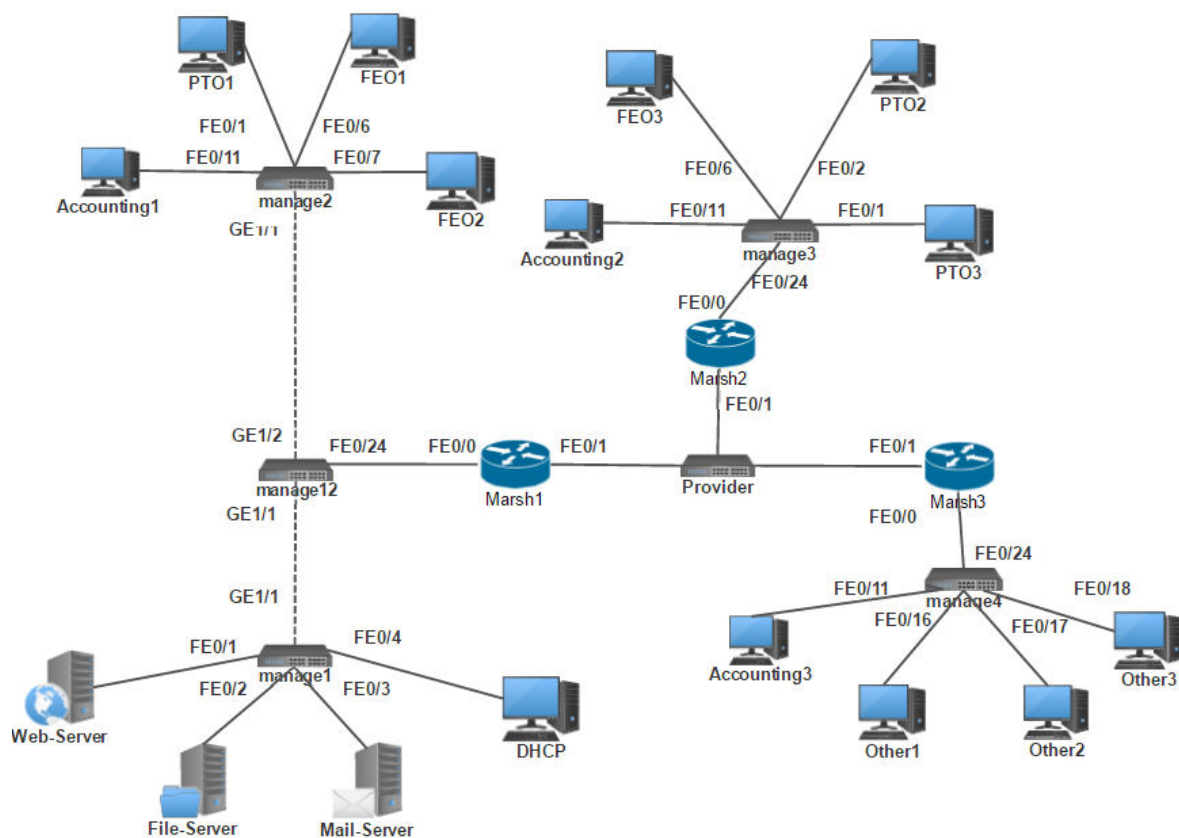


Рис. 4. Схема уровня сети L-1

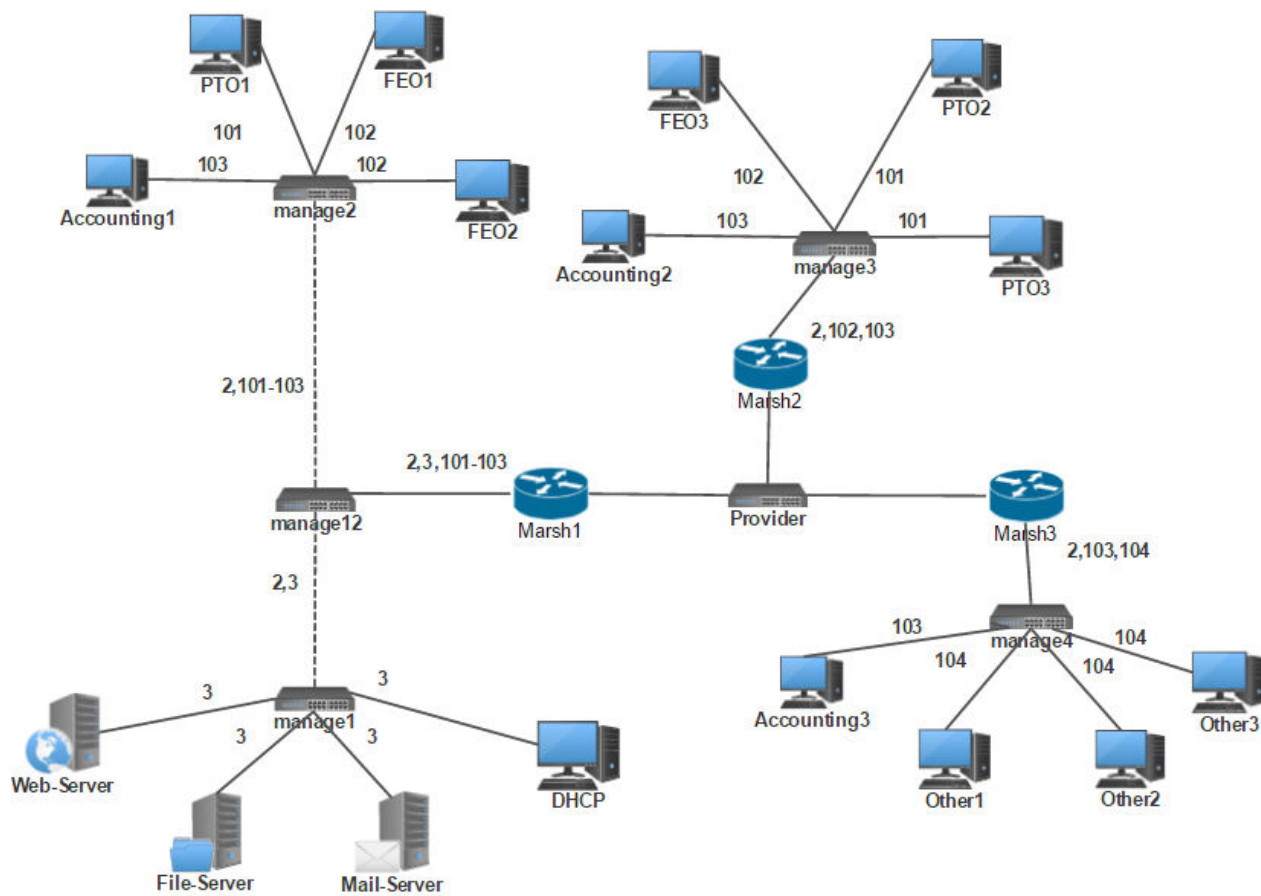


Рис.5. Схема уровня сети L-2

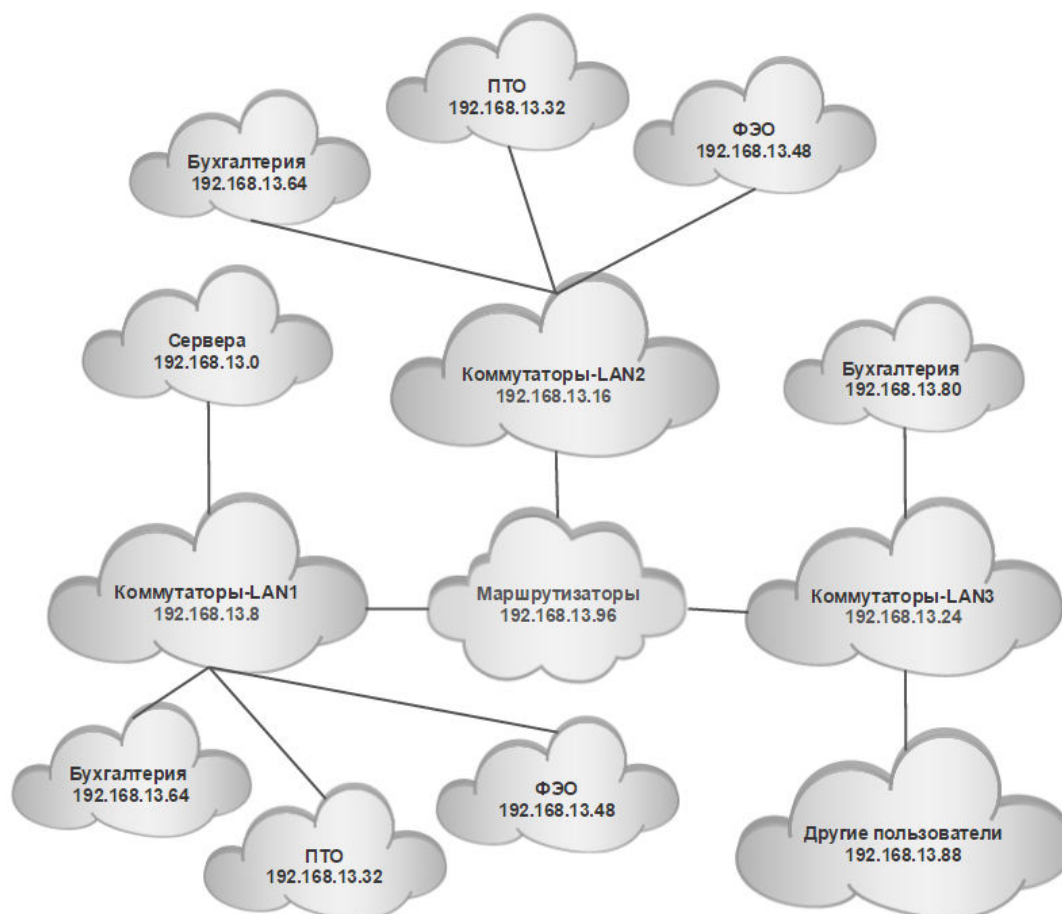


Рис.6. Схема уровня сети L-3

### 3.1.3 Разработка плана подключения оборудования

Составим таблицу подключения оборудования по портам, она приведена в табл. 2.

Таблица 2. Подключение оборудования по портам

| Имя      | Название    | FE   | Gigabit | Access | Trunk     |
|----------|-------------|------|---------|--------|-----------|
| manage1  | WEB         | 0/1  |         | 3      |           |
|          | File        | 0/2  |         | 3      |           |
|          | Mail        | 0/3  |         | 3      |           |
|          | DHCP        | 0/4  |         | 3      |           |
|          | manage12    |      | 1/1     |        | 2,101-104 |
| manage2  | PTO1        | 0/1  |         | 101    |           |
|          | FEO1        | 0/7  |         | 102    |           |
|          | FEO2        | 0/6  |         | 102    |           |
|          | Accounting1 | 0/11 |         | 103    |           |
|          | manage12    |      | 1/1     |        | 2,101-104 |
| manage12 | manage1     |      | 1/1     |        | 2,101-104 |
|          | manage2     |      | 1/2     |        | 2,101-104 |
|          | Marsh1      | 0/24 |         |        | 2,101-104 |
| manage3  | PTO3        | 0/1  |         | 101    |           |

|         |             |      |  |     |           |
|---------|-------------|------|--|-----|-----------|
| manage4 | PTO2        | 0/2  |  | 101 |           |
|         | FEO3        | 0/6  |  | 102 |           |
|         | Accounting2 | 0/11 |  | 103 |           |
|         | Marsh2      | 0/24 |  |     | 2,101-104 |
|         | Accounting3 | 0/11 |  | 103 |           |
|         | Other1      | 0/16 |  | 104 |           |
|         | Other2      | 0/17 |  | 104 |           |
|         | Other3      | 0/18 |  | 104 |           |
|         | Marsh3      | 0/24 |  |     | 2,101-104 |

Каждому устройству в сети необходимо задать IP-адрес и маску подсети. IP-адрес – это уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. Маска подсети – это битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая - к адресу самого узла в сети. Также маска определяет размер подсети, в которую входит диапазон IP-адресов.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И).

Настройка IP-адресов для ПК и серверов производится на вкладке “Desktop”, в меню “IP Configuration” (рис. 7).

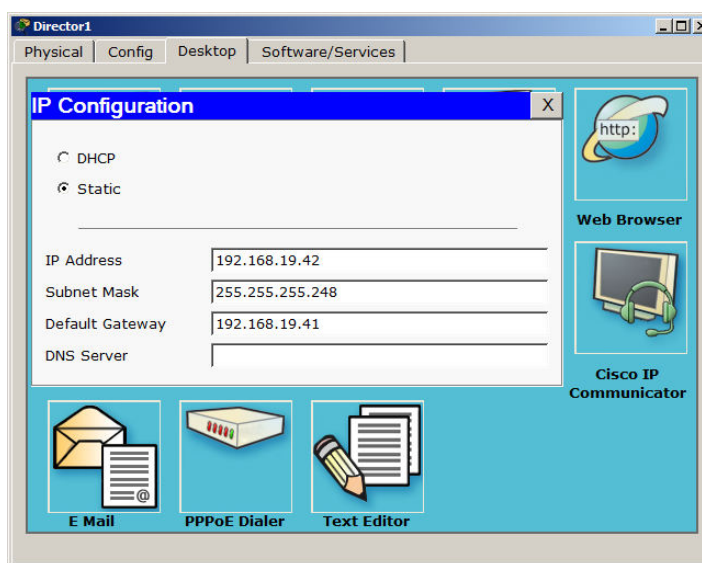


Рис.7. Настройка IP-адреса, маски подсети и шлюза для ПК

Составим IP-план, который будет включать в себя название устройства, его адрес, номер подсети и принадлежность к VLAN (табл. 3).

Таблица 3. IP-план проектируемой сети

| IP-адрес               | Имя устройства  | VLAN |
|------------------------|-----------------|------|
| <b>192.168.13.0/24</b> |                 |      |
| 192.168.13.0/29        | Серверная ферма | 3    |
| 192.168.13.1           | Шлюз            |      |

| IP-адрес                    | Имя устройства   | VLAN |
|-----------------------------|------------------|------|
| 192.168.13.2                | Web              |      |
| 192.168.13.3                | File             |      |
| 192.168.13.4                | Mail             |      |
| 192.168.13.5                | DHCP             |      |
| 192.168.13.6                | Зарезервировано  |      |
| 192.168.13.8/29             | Управление LAN1  | 2    |
| 192.168.13.9                | Шлюз             |      |
| 192.168.13.10               | manage1          |      |
| 192.168.13.11               | manage2          |      |
| 192.168.13.12               | manage12         |      |
| 192.168.13.13-192.168.13.14 | Зарезервировано  |      |
| 192.168.13.16/29            | Управление LAN2  |      |
| 192.168.13.17               | Шлюз             |      |
| 192.168.13.18               | manage3          |      |
| 192.168.13.19-192.168.13.22 | Зарезервировано  |      |
| 192.168.13.24/29            | Управление LAN3  |      |
| 192.168.13.25               | Шлюз             |      |
| 192.168.13.26               | manage4          |      |
| 192.168.13.27-192.168.13.30 | Зарезервировано  |      |
| 192.168.13.32/29            | ПТО LAN1         | 101  |
| 192.168.13.33               | Шлюз             |      |
| 192.168.13.34               | РТО1             |      |
| 192.168.13.35-192.168.13.38 | Зарезервировано  |      |
| 192.168.13.40/29            | ПТО LAN2         |      |
| 192.168.13.41               | Шлюз             |      |
| 192.168.13.42               | РТО2             |      |
| 192.168.13.43               | РТО3             |      |
| 192.168.13.44-192.168.13.46 | Зарезервировано  |      |
| 192.168.13.48/29            | ФЭО LAN1         | 102  |
| 192.168.13.49               | шлюз             |      |
| 192.168.13.50               | ФЕО1             |      |
| 192.168.13.51               | ФЕО2             |      |
| 192.168.13.52-192.168.13.54 | Зарезервировано  |      |
| 192.168.13.56/29            | ФЭО LAN2         |      |
| 192.168.13.57               | шлюз             |      |
| 192.168.13.58               | ФЕО3             |      |
| 192.168.13.59-192.168.13.62 | Зарезервировано  |      |
| 192.168.13.64/29            | Бухгалтерия LAN1 | 103  |
| 192.168.13.65               | Шлюз             |      |

| IP-адрес                      | Имя устройства      | VLAN |
|-------------------------------|---------------------|------|
| 192.168.13.66                 | Accounting1         |      |
| 192.168.13.67-192.168.13.70   | Зарезервировано     |      |
| 192.168.13.72/29              | Бухгалтерия LAN2    |      |
| 192.168.13.73                 | Шлюз                |      |
| 192.168.13.74                 | Accounting2         |      |
| 192.168.13.75-192.168.13.78   | Зарезервировано     |      |
| 192.168.13.80/29              | Бухгалтерия LAN3    |      |
| 192.168.13.81                 | Шлюз                |      |
| 192.168.13.82                 | Accounting3         |      |
| 192.168.13.83-192.168.13.86   | Зарезервировано     |      |
| 192.168.13.88/29              | Другие пользователи | 104  |
| 192.168.13.89                 | Шлюз                |      |
| 192.168.13.90                 | Other1              |      |
| 192.168.13.91                 | Other2              |      |
| 192.168.13.92                 | Other3              |      |
| 192.168.13.93-192.168.13.94   | Зарезервировано     |      |
| 192.168.13.96/29              | Connection          | 4    |
| 192.168.13.97                 | Шлюз                |      |
| 192.168.13.98                 | Marsh1              |      |
| 192.168.13.99                 | Marsh2              |      |
| 192.168.13.100                | Marsh3              |      |
| 192.168.13.101-192.168.13.102 | Зарезервировано     |      |

### 3.2. Настройка VLAN, access и trunk-портов проектируемой сети.

VLAN (Virtual Local Area Network) - группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях. В современных сетях VLAN - главный механизм для создания логической архитектуры сети, не зависящей от её физической топологии.

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения.

Каждый VLAN - это отдельный широковещательный домен. Например, коммутатор - это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене.

Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен. Коммутатор знает, что компьютер, который подключен к определённому порту, находится в соответствующем VLAN. Трафик, приходящий на порт определённого VLAN, ничем особенным не отличается от трафика другого VLAN. Другими словами, никакой информации о принадлежности трафика определённому VLAN в нём нет.

Однако, если через порт проходит трафик разных VLAN'ов, коммутатор должен их различать. Для этого каждый кадр (frame) трафика должен быть помечен особым образом. Пометка должна говорить о том, какому VLAN трафик принадлежит. VLAN могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах и на хостах.

Составим таблицу VLAN (табл. 4).

Таблица. 4. Соответствие узлов сети номеру VLAN

| №VLAN | Имя VLAN   | Примечание                    |
|-------|------------|-------------------------------|
| 1     | default    | не используется               |
| 2     | Management | Для управления устройствами   |
| 3     | Servers    | Для серверной фермы           |
| 4     | Connection | Связь между маршрутизаторами  |
| 5-100 |            | Зарезервировано               |
| 101   | PTO        | Для пользователей ПТО         |
| 102   | FEO        | Для пользователей ФЭО         |
| 103   | Accounting | Для пользователей Бухгалтерии |
| 104   | Other      | Для других пользователей      |

Каждая группа будет выделена в отдельный VLAN. Таким образом мы ограничим широковещательные домены. Также введём специальный VLAN для управления устройствами. Номера VLAN с 5 по 100 зарезервированы для дальнейшей модернизации сети.

### 3.2.1. Настройка каналов коммутации между VLAN

Используя данные таблиц подключения оборудования по портам (табл.2), IP-адресов (табл.3) и соответствия узлов сети номеру VLAN (табл.4) создадим в Cisco Packet Tracer схему, приведенную на рис. 8.



4) Настроить все транковые порты и задать им имя:

*Switch(config-if)#description DESCRIPTION-OF-INTERFACE*

*Switch(config-if)#switchport mode trunk*

*Switch(config-if)#switchport trunk allowed vlan VLAN-NUMBERS*

В соответствии с принятой последовательностью создадим все Vlan для LAN1:

*Switch#enable*

*Switch#configure terminal*

*Switch(config)#hostname manage1*

*manage1 (config)#vlan 2*

*manage1 (config-vlan)#name Management*

*manage1 (config-vlan)#vlan 3*

*manage1 (config-vlan)#name Servers*

*Switch#enable*

*Switch#configure terminal*

*Switch(config)#hostname manage2*

*manage2 (config)#vlan 2*

*manage2 (config-vlan)#name Management*

*manage2 (config-vlan)#vlan 3*

*manage2 (config-vlan)#name Servers*

*manage2 (config-vlan)#vlan 101*

*manage2 (config-vlan)#name PTO*

*manage2 (config-vlan)#vlan 102*

*manage2 (config-vlan)#name FEO*

*manage2 (config-vlan)#vlan 103*

*manage2 (config-vlan)#name Accounting*

*Switch#enable*

*Switch#configure terminal*

*Switch(config)#hostname manage12*

*manage12 (config)#vlan 2*

*manage12 (config-vlan)#name Management*

*manage12 (config-vlan)#vlan 3*

*manage12 (config-vlan)#name Servers*

*manage12 (config-vlan)#vlan 101*

*manage12 (config-vlan)#name PTO*

*manage12 (config-vlan)#vlan 102*

*manage12 (config-vlan)#name FEO*

*manage12 (config-vlan)#vlan 103*

*manage12 (config-vlan)#name Accounting*

Создадим все Vlan для LAN2:

```
Switch#enable
Switch#configure terminal
Switch(config)#hostname manage3
manage3 (config)#vlan 2
manage3 (config-vlan)#name Management
manage3 (config-vlan)#vlan 101
manage3 (config-vlan)#name PTO
manage3 (config-vlan)#vlan 102
manage3 (config-vlan)#name FEO
manage3 (config-vlan)#vlan 103
manage3 (config-vlan)#name Accounting
```

Создадим все Vlan для LAN3:

```
Switch#enable
Switch#configure terminal
Switch(config)#hostname manage4
manage4 (config)#vlan 2
manage4 (config-vlan)#name Management
manage4 (config-vlan)#vlan 103
manage4 (config-vlan)#name Accounting
manage4 (config-vlan)#vlan 104
manage4 (config-vlan)#name Other
```

### **3.2.2. Настройка портов доступа (access)**

Access port (порт доступа) - к нему подключаются, как правило, конечные узлы. Трафик между этим портом и устройством не тегированный. За каждым access-портом закреплён определённый VLAN. Весь трафик, приходящий на этот порт от конечного устройства, получает метку этого VLAN, а исходящий уходит без метки.

Настроим порты Access на manage1, manage2, manage12, manage3, manage4, для этого заходим на вкладку CLI в окне управления, переводим коммутатор в режим глобальной конфигурации и набираем в командной строке:

1) Для manage1:

```
manage1(config)#interface FastEthernet0/1
manage1 (config-if)#description Servers
manage1 (config-if)#switchport mode access
manage1 (config-if)#switchport access vlan 3
manage1 (config)#interface FastEthernet0/2
manage1 (config-if)#description Servers
manage1 (config-if)#switchport access vlan 3
manage1 (config-if)#switchport mode access
manage1 (config)#interface FastEthernet0/3
manage1 (config-if)#description Servers
```

*manage1 (config-if)#switchport access vlan 3*  
*manage1 (config-if)#switchport mode access*  
*manage1 (config)#interface FastEthernet0/4*  
*manage1 (config-if)#description Servers*  
*manage1 (config-if)#switchport access vlan 3*  
*manage1 (config-if)#switchport mode access*

2) Для manage2:

*manage2 (config)#interface FastEthernet0/1*  
*manage2 (config-if)#description PTO*  
*manage2 (config-if)#switchport access vlan 101*  
*manage2 (config-if)#switchport mode access*  
*manage2 (config)#interface FastEthernet0/6*  
*manage2 (config-if)#description FEO*  
*manage2 (config-if)#switchport access vlan 102*  
*manage2 (config-if)#switchport mode access*  
*manage2 (config)#interface FastEthernet0/7*  
*manage2 (config-if)#description FEO*  
*manage2 (config-if)#switchport access vlan 102*  
*manage2 (config-if)#switchport mode access*  
*manage2 (config)#interface FastEthernet0/11*  
*manage2 (config-if)#description Accounting*  
*manage2 (config-if)#switchport access vlan 103*  
*manage2 (config-if)#switchport mode access*

3) Для manage3:

*manage3 (config)#interface FastEthernet0/1*  
*manage3 (config-if)#description PTO*  
*manage3 (config-if)#switchport access vlan 101*  
*manage3 (config-if)#switchport mode access*  
*manage3 (config)#interface FastEthernet0/2*  
*manage3 (config-if)#description PTO*  
*manage3 (config-if)#switchport access vlan 101*  
*manage3 (config-if)#switchport mode access*  
*manage3 (config)#interface FastEthernet0/6*  
*manage3 (config-if)#description FEO*  
*manage3 (config-if)#switchport access vlan 102*  
*manage3 (config-if)#switchport mode access*  
*manage3 (config)#interface FastEthernet0/11*  
*manage3 (config-if)#description Accounting*  
*manage3 (config-if)#switchport access vlan 103*  
*manage3 (config-if)#switchport mode access*

4) Для manage4:

*manage4 (config)#interface FastEthernet0/11*  
*manage4 (config-if)#description Accounting*  
*manage4 (config-if)#switchport access vlan 103*

```

manage4 (config-if)#switchport mode access
manage4 (config)#interface FastEthernet0/16
manage4 (config-if)#description Other
manage4 (config-if)#switchport access vlan 104
manage4 (config-if)#switchport mode access
manage4 (config)#interface FastEthernet0/17
manage4 (config-if)#description Other
manage4 (config-if)#switchport access vlan 104
manage4 (config-if)#switchport mode access
manage4 (config)#interface FastEthernet0/18
manage4 (config-if)#description Other
manage4 (config-if)#switchport access vlan 104
manage4 (config-if)#switchport mode access

```

Произведем проверку связи между узлами сети относящимися к одному VLAN, например, между PTO2 и PTO3 используя команду **ping** (рис. 9). Следует особо отметить, что пингование проходит только между хостами, относящимися к одному VLAN, хосты принадлежащие разным VLAN не могут обмениваться между собой данными без дополнительных настроек и подключения к маршрутизатору.

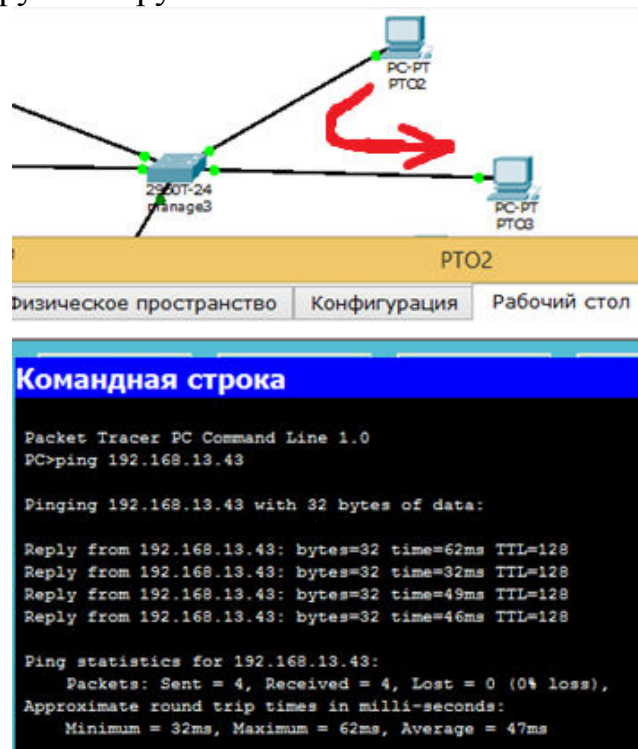


Рис. 9. Выполнение команды ping от PTO2 к PTO3

### 3.2.3. Настройка trunk-портов

Настроим trunk порт между тремя коммутаторами: manage1, manage2 и manage12. Пропишем сразу все VLAN связанные с *interface Gigabit Ethernet1/1*:

```

manage1 (config)#interface GigabitEthernet1/1

```

```
manage1 (config-if)#description manage12
manage1 (config-if)#switchport trunk allowed vlan 2,101-104
manage1 (config-if)#switchport mode trunk
```

На самом деле, достаточно команды `#switchport mode trunk`, чтобы через этот порт уже пошли тегированные кадры всех VLAN, потому что по умолчанию trunk порт пропускает всё. Однако, при администрировании сети важно, чтобы через нее проходило только то, что разрешено администратором. Как только поступает команда `switchport trunk allowed vlan 101`, через порт не пройдет кадр никаких VLAN, кроме 101 (VLAN 1 проходит по умолчанию и не тегированным). Таким образом:

1) Access порт - принимает и отправляет только не тегированный трафик. Пакеты, помеченные каким-либо тегом, отбрасываются, даже если они принадлежат тому же VLAN, в котором находится этот порт.

2) trunk-порт, по умолчанию пропускает весь трафик, неважно есть тег или нет.

Примечание. Однако командой: `switchport trunk allowed vlan 2,101,104` - можно запретить все VLAN кроме 2, 101 и 104. Также и пакеты не тегированного VLAN пройти через такой порт не смогут, если явно не разрешить им это делать командой: `switchport trunk allowed vlan add 1`.

Переходим к manage2. На нём необходимо настроить порты:

```
manage2 (config)#interface GigabitEthernet1/1
manage2 (config-if)#description manage12
manage2 (config-if)#switchport trunk allowed vlan 2,101-104
manage2 (config-if)#switchport mode trunk
```

Настроим порты на manage12:

```
manage12(config)#interface GigabitEthernet1/1
manage12 (config-if)# manage1
manage12 (config-if)#switchport trunk allowed vlan 2,101,104
manage12 (config-if)#switchport mode trunk
manage12(config)#interface GigabitEthernet1/2
manage12 (config-if)# manage2
manage12 (config-if)switchport trunk allowed vlan 2,101,104
manage12 (config-if)switchport mode trunk
```

Для организации взаимодействия между хостами, принадлежащими различным VLAN нужно настроить сеть управления. В случае использования cisco эмулятора этого не потребуются (настройки осуществляются через окно PT), однако, при проектировании реальной сети это необходимо. Создадим интерфейс и укажем номер соответствующего VLAN. А далее с ним можно работать, как с самым обычным физическим интерфейсом. Настроим IP-адрес для управления (рис. 8):

### **1) manage12**

```
manage12(config)#interface vlan 2  
manage12 (config-if)#description Management  
manage12 (config-if)#ip address 192.168.13.12 255.255.255.248  
manage12#write memory
```

### **2) manage1**

```
manage1 (config)#interface vlan 2  
manage1 (config-if)#description Management  
manage1 (config-if)#ip address 192.168.13.10 255.255.255.248
```

### **3) manage2**

```
manage2 (config)#interface vlan 2  
manage2 (config-if)#description Management  
manage2 (config-if)#ip address 192.168.13.11 255.255.255.248
```

### **4) manage3**

```
manage3 (config)#interface vlan 2  
manage3 (config-if)#description Management  
manage3 (config-if)#ip address 192.168.13.18 255.255.255.248
```

### **5) manage4**

```
manage4 (config)#interface vlan 2  
manage4 (config-if)#description Management  
manage4 (config-if)#ip address 192.168.13.26 255.255.255.248
```

## **3.2.4. Настройка каналов коммутации между VLAN**

На данный момент устройства различных VLAN не могут обмениваться данными. Для маршрутизации между VLAN будем использовать роутер *cisco 2811*. Иными словами, он будет терминировать (соединять) хосты, расположенные в разных VLAN. В маршрутизаторе кадры инкапсулируются, т.е. из них извлекаются IP-пакеты, а заголовки канального уровня отбрасываются. Вначале настроим коммутаторы *manage12*, *manage3*, *manage4*. На них нужно настроить trunk порт в сторону маршрутизатора (рис.3):

### **1) Для manage12**

```
manage12 (config)#interface FastEthernet0/24  
manage12 (config-if)#description Marsh1  
manage12 (config-if)# switchport trunk allowed vlan 2-3,101-104  
manage12 (config-if)# switchport mode trunk
```

### **2) Для manage3**

```
manage3 (config)#interface FastEthernet0/24
```

```
manage3 (config-if)# description Marsh1
manage3 (config-if)# switchport trunk allowed vlan 2-3,101-104
manage3 (config-if)# switchport mode trunk
```

### **3) Для manage4**

```
manage4 (config)#interface FastEthernet0/24
manage4 (config-if)# description Marsh1
manage4 (config-if)# switchport trunk allowed vlan 2-3,101-104
manage4 (config-if)# switchport mode trunk
```

Переходим в режим настройки интерфейса маршрутизаторов, обращённых в локальную сеть и включаем их, так как по умолчанию они находятся в состоянии Administratively down (выключено):

#### **1) Для Marsh1**

```
Marsh1(config)#interface FastEthernet 0/0
Marsh1 (config-if)#no shutdown
```

#### **2) Для Marsh2**

```
Marsh2(config)#interface FastEthernet 0/0
Marsh2 (config-if)#no shutdown
```

#### **3) Для Marsh3**

```
Marsh3(config)#interface FastEthernet 0/0
Marsh3 (config-if)#no shutdown
```

Создадим виртуальный интерфейс -sub-interface. Для этого следует указать физический интерфейс, к которому подключена нужная сеть, а после точки нужно поставить некий уникальный идентификатор этого виртуального интерфейса.

***Switch (config)#interface fa0/0.2***

*Примечание. Для удобства, обычно номер сабинтерфейса делают аналогичным номеру VLAN, который он терминирует.*

Следующей командой обозначим, что кадры, исходящие из этого виртуального интерфейса, будут помечены тегом 2-го VLAN. А кадры, входящие на физический интерфейс FastEthernet0/0 с тегом этого VLAN, будут приняты виртуальным интерфейсом FastEthernet0/0.2.

***Switch (config-subif)#encapsulation dot1Q 2***

Определим IP-адрес. Этот адрес будет шлюзом по умолчанию (default gateway) для всех устройств в этом VLAN.

***Switch (config-if)#ip address xxxx. xxxx. xxxx. xxxx. 255.255.255.248***

#### **1) Для Marsh1**

```
Marsh1 (config)#interface fa0/0.2
Marsh1 (config-subif)#description Management
Marsh1 (config-subif)#encapsulation dot1Q 2
Marsh1 (config-if)#ip address 192.168.13.9 255.255.255.248
```

Аналогичным образом настроим VLAN 3,101-103:

```
Marsh1 (config)#interface FastEthernet0/0.101
Marsh1 (config-if)#description PTO
Marsh1 (config-if)#encapsulation dot1Q 101
Marsh1 (config-if)#ip address 192.168.13.9 255.255.255.248
```

```
Marsh1 (config)#interface FastEthernet0/0.3
Marsh1 (config-subif)#description Servers
Marsh1 (config-subif)#encapsulation dot1Q 3
Marsh1 (config-subif)#ip address 192.168.13.1 255.255.255.248
```

```
Marsh1 (config)#interface FastEthernet0/0.101
Marsh1 (config-subif)#description PTO
Marsh1 (config-subif)#encapsulation dot1Q 101
Marsh1 (config-subif)#ip address 192.168.13.33 255.255.255.248
```

```
Marsh1 (config)#interface FastEthernet0/0.102
Marsh1 (config-subif)#description FEO
Marsh1 (config-subif)#encapsulation dot1Q 102
Marsh1 (config-subif)#ip address 192.168.13.49 255.255.255.248
```

```
Marsh1 (config)#interface FastEthernet0/0.103
Marsh1 (config-subif)#description Accounting
Marsh1 (config-subif)#encapsulation dot1Q 103
Marsh1 (config-subif)#ip address 192.168.13.65 255.255.255.248
```

Далее по аналогии настроим маршрутизаторы LAN2 и LAN3:

```
Marsh2 (config)#interface fa0/0.2
Marsh2 (config-subif)#description Management
Marsh2 (config-subif)#encapsulation dot1Q 2
Marsh2 (config-if)#ip address 192.168.13.17 255.255.255.248
```

```
Marsh2 (config)#interface FastEthernet0/0.101
Marsh2 (config-if)#description PTO
Marsh2 (config-if)#encapsulation dot1Q 101
Marsh2 (config-if)#ip address 192.168.13.41 255.255.255.248
```

```
Marsh2 (config)#interface FastEthernet0/0.102
Marsh2 (config-subif)#description FEO
```

*Marsh2 (config- subif)#encapsulation dot1Q 102*  
*Marsh2 (config- subif)#ip address 192.168.13.57 255.255.255.248*

*Marsh2 (config)#interface FastEthernet0/0.103*  
*Marsh2 (config- subif)#description Accounting*  
*Marsh2 (config- subif)#encapsulation dot1Q 103*  
*Marsh2 (config- subif)#ip address 192.168.13.73 255.255.255.248*

*Marsh3 (config)#interface fa0/0.2*  
*Marsh3 (config-subif)#description Management*  
*Marsh3 (config-subif)#encapsulation dot1Q 2*  
*Marsh3 (config-if)#ip address 192.168.13.25 255.255.255.248*

*Marsh3 (config)#interface FastEthernet0/0.103*  
*Marsh3 (config- subif)#description Accounting*  
*Marsh3 (config- subif)#encapsulation dot1Q 103*  
*Marsh3 (config- subif)#ip address 192.168.13.81 255.255.255.248*

*Marsh3 (config)#interface FastEthernet0/0.104*  
*Marsh3 (config- subif)#description Other*  
*Marsh3 (config- subif)#encapsulation dot1Q 104*  
*Marsh3 (config- subif)#ip address 192.168.13.89 255.255.255.248*

### **3.3. Настройка маршрутизации между LAN**

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации. Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введенной администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации.

Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов - это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет. В случае статической маршрутизации администратор вручную определяет маршруты к сетям назначения.

В случае динамической маршрутизации – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором

автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

### 3.3.1. Настройка статической маршрутизации

На Marsh1, Marsh2, Marsh3 используются два интерфейса, к одному (FE0/0) уже подключена наша локальная сеть, а второй (FE0/1) будет использоваться для выхода в интернет и для подключения офисов между собой.

Создадим саб-интерфейсы, выделив для связи 4-ой VLAN, IP-адреса берём из IP-плана (табл.3).

```
1) Marsh1 (config)#interface FastEthernet0/1.4
Marsh1 (config- subif)#description Connection
Marsh1 (config- subif)#encapsulation dot1Q 4
Marsh1 (config- subif)#ip address 192.168.13.98 255.255.255.248
```

```
2) Marsh2 (config)#interface FastEthernet0/1.4
Marsh2 (config- subif)#description Connection
Marsh2 (config- subif)#encapsulation dot1Q 4
Marsh2 (config- subif)#ip address 192.168.13.99 255.255.255.248
```

```
3) Marsh3 (config)#interface FastEthernet0/1.4
Marsh3 (config- subif)#description Connection
Marsh3 (config- subif)#encapsulation dot1Q 4
Marsh3 (config- subif)#ip address 192.168.13.100 255.255.255.248
```

Далее пропишем маршруты статической адресации для маршрутизаторов вручную:

```
1) Marsh1(config)#ip route 192.168.13.88 255.255.255.248 192.168.13.100
Marsh1(config)#ip route 192.168.13.80 255.255.255.248 192.168.13.100
Marsh1(config)#ip route 192.168.13.72 255.255.255.248 192.168.13.99
Marsh1(config)#ip route 192.168.13.40 255.255.255.248 192.168.13.99
Marsh1(config)#ip route 192.168.13.56 255.255.255.248 192.168.13.99
```

```
2) Marsh2(config)#ip route 192.168.13.88 255.255.255.248 192.168.13.100
Marsh2(config)#ip route 192.168.13.80 255.255.255.248 192.168.13.100
Marsh2(config)#ip route 192.168.13.64 255.255.255.248 192.168.13.98
Marsh2(config)#ip route 192.168.13.32 255.255.255.248 192.168.13.98
Marsh2(config)#ip route 192.168.13.48 255.255.255.248 192.168.13.98
Marsh2(config)#ip route 192.168.13.0 255.255.255.248 192.168.13.98
```

```
3) Marsh3(config)#ip route 192.168.13.32 255.255.255.248 192.168.13.98
Marsh3(config)#ip route 192.168.13.48 255.255.255.248 192.168.13.98
```

```
Marsh3(config)#ip route 192.168.13.64 255.255.255.248 192.168.13.98
Marsh3(config)#ip route 192.168.13.0 255.255.255.248 192.168.13.98
Marsh3(config)#ip route 192.168.13.72 255.255.255.248 192.168.13.99
Marsh1(config)#ip route 192.168.13.40 255.255.255.248 192.168.13.99
Marsh1(config)#ip route 192.168.13.56 255.255.255.248 192.168.13.99
```

Проверим доступность между любыми хостами, расположенными в разных локальных сетях, например, между Accounting3 и WEB – сервером. Для этого зададим с PC Accounting3 команду (рис. 10):

*Ping 192.168.13.2*

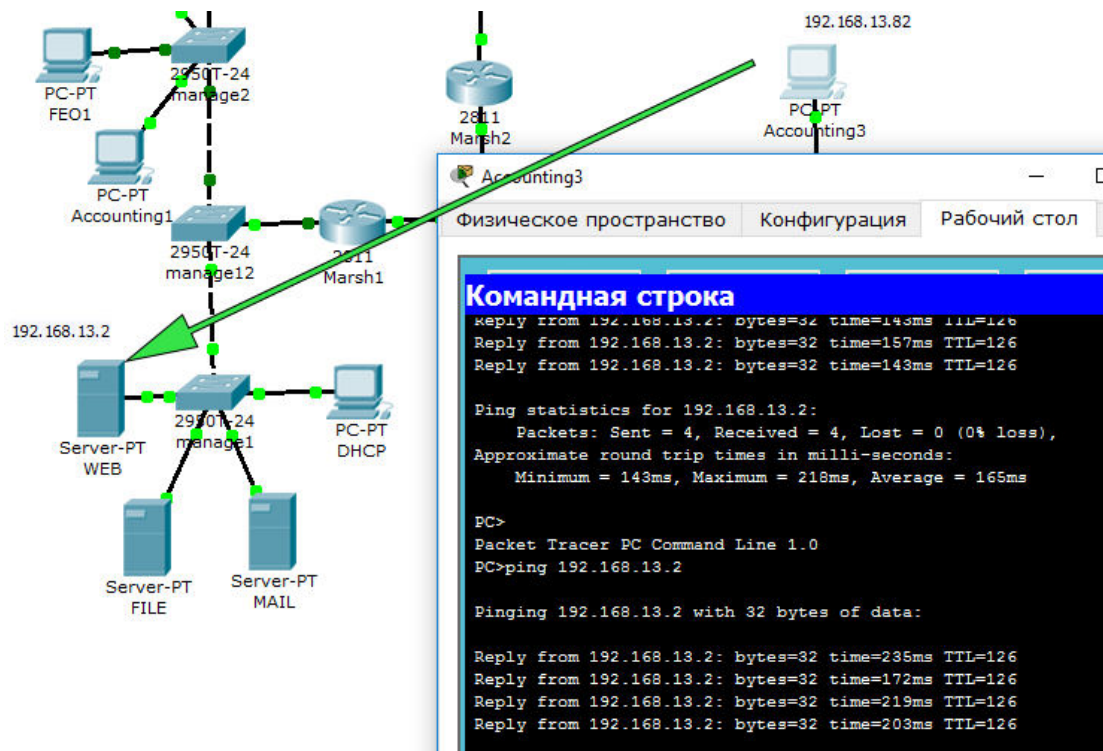


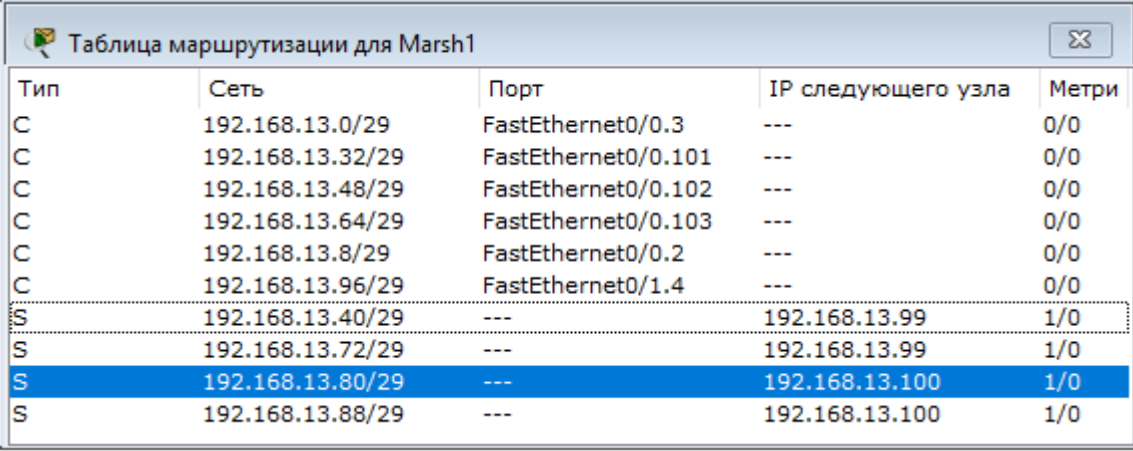
Рис. 10 Проверка наличия связи между Accounting3 и WEB – сервером

Таблица маршрутизации для Marsh3 приведена на рис. 11.

```
192.168.13.0/29 is subnetted, 11 subnets
S    192.168.13.0 [1/0] via 192.168.13.98
C    192.168.13.24 is directly connected, FastEthernet0/0.2
S    192.168.13.32 [1/0] via 192.168.13.98
S    192.168.13.40 [1/0] via 192.168.13.99
S    192.168.13.48 [1/0] via 192.168.13.98
S    192.168.13.56 [1/0] via 192.168.13.99
S    192.168.13.64 [1/0] via 192.168.13.98
S    192.168.13.72 [1/0] via 192.168.13.99
C    192.168.13.80 is directly connected, FastEthernet0/0.103
C    192.168.13.88 is directly connected, FastEthernet0/0.104
C    192.168.13.96 is directly connected, FastEthernet0/1.4
```

Рис. 11 Таблица маршрутизации для Marsh3

Анализ таблицы показывает путь к сети 192.168.13.0/29 (где находится WEB – сервер) прописан с помощью статической маршрутизации и следующим hop (после Marsh3) будет сеть 198.168.13.98 (Marsh1). Аналогично можно проверить обратную связь - Marsh1 → Marsh3 (рис. 12) и все остальные узлы проектируемой сети.



| Тип | Сеть             | Порт                | IP следующего узла | Метри |
|-----|------------------|---------------------|--------------------|-------|
| C   | 192.168.13.0/29  | FastEthernet0/0.3   | ---                | 0/0   |
| C   | 192.168.13.32/29 | FastEthernet0/0.101 | ---                | 0/0   |
| C   | 192.168.13.48/29 | FastEthernet0/0.102 | ---                | 0/0   |
| C   | 192.168.13.64/29 | FastEthernet0/0.103 | ---                | 0/0   |
| C   | 192.168.13.8/29  | FastEthernet0/0.2   | ---                | 0/0   |
| C   | 192.168.13.96/29 | FastEthernet0/1.4   | ---                | 0/0   |
| S   | 192.168.13.40/29 | ---                 | 192.168.13.99      | 1/0   |
| S   | 192.168.13.72/29 | ---                 | 192.168.13.99      | 1/0   |
| S   | 192.168.13.80/29 | ---                 | 192.168.13.100     | 1/0   |
| S   | 192.168.13.88/29 | ---                 | 192.168.13.100     | 1/0   |

Рис. 12. Таблица маршрутизации для Marsh1

### 3.3.2. Настройка динамической маршрутизации

Динамическая маршрутизация - вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP). Каждый протокол маршрутизации использует свою систему оценки маршрутов (метрику). Маршрут к сетям назначения строится на основе следующих критериев:

- количество ретрансляционных переходов;
- пропускная способность канала связи;
- задержки передачи данных;
- и др.

RIP - протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути алгоритм Беллмана-Форда. Алгоритм маршрутизации RIP - один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст адрес. Максимальное количество "хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (метрика 15). Ограничение в 15 хопов не дает применять RIP в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышена безопасность за счет введения дополнительной маршрутной информации.

Принцип дистанционно-векторного протокола: каждый маршрутизатор, использующий протокол RIP периодически широковещательно рассылает

своим соседям специальный пакет-вектор, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. Маршрутизатор получивший такой вектор, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет вектор информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный вектор маршрутизатор рассылает всем своим соседям. Маршрутизатор выбирает из нескольких альтернативных маршрутов маршрут с наименьшим значением метрики, а маршрутизатор, передавший информацию о таком маршруте помечается как следующий (next hop). Протокол непригоден для работы в больших сетях, так как засоряет сеть интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети.

Перед началом работы удалим из маршрутизаторов все настройки статической маршрутизации.

Настроим протокол RIP на маршрутизаторе Marsh3:

*Router (config)#router rip ; Вход в режим конфигурирования протокола RIP*

*Router (config-router)#version 2;*

*Router (config-router)# network 192.168.13.0; Подключение сети к роутеру со стороны Provider.*

Протокол RIPv2 не требует маски подсети, поэтому, прописывая в качестве адреса сети 192.168.13.0, подразумеваются абсолютно все устройства, IP-адрес которых начинается на «192.168.13», то есть вообще все устройства нашей компьютерной сети.

Посмотреть введенные команды можно в маршрутизаторе на вкладке “Config” в меню “RIP” (рис. 13).

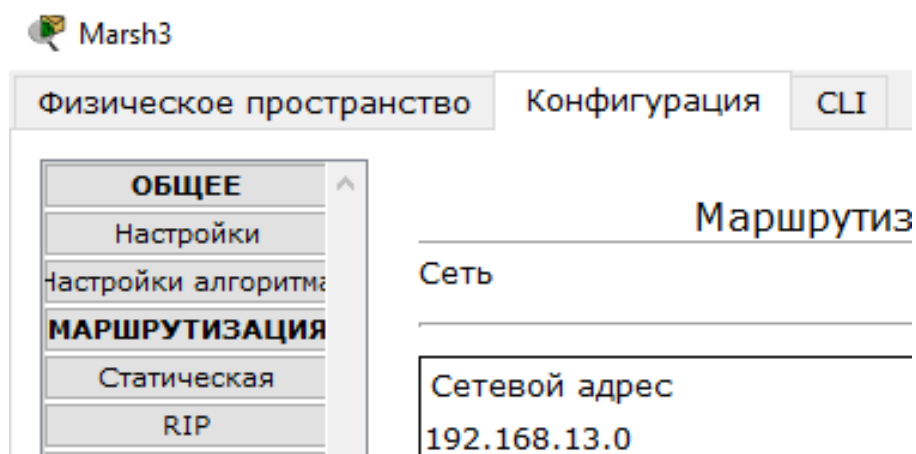


Рис. 13. Результат выполнения введенных команд

Для проверки работы динамической маршрутизации проверим связь между любыми двумя компьютерами, например, между Accounting3 и WEB – сервером (рис.14).

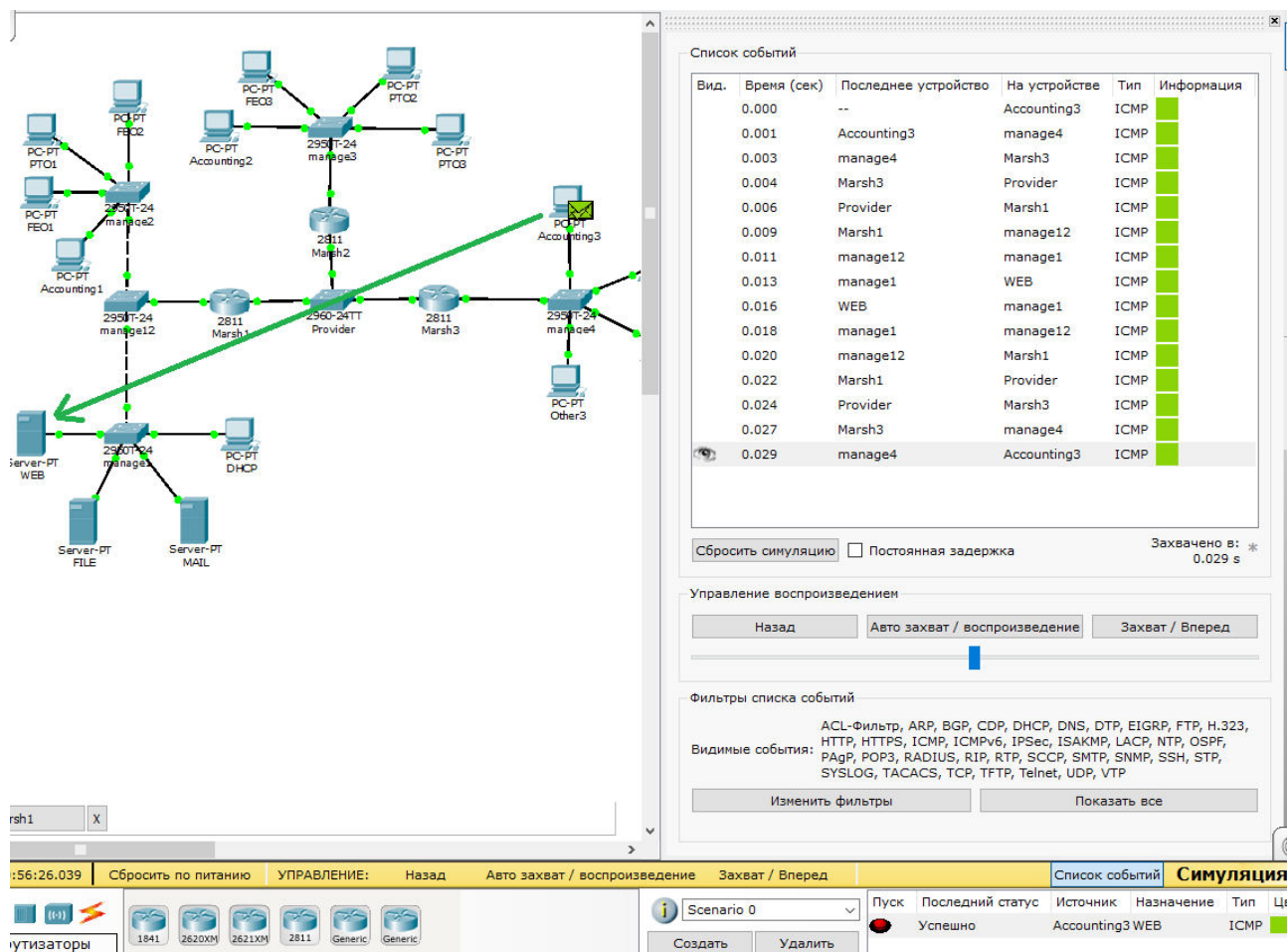


Рис. 14. Проверка работы динамической маршрутизации по протоколу RIP между Accounting3 и WEB – сервером.

Таблица маршрутизации для Marsh3 приведена на рис.15.

| Тип | Сеть             | Порт                | IP следующего узла |
|-----|------------------|---------------------|--------------------|
| C   | 192.168.13.24/29 | FastEthernet0/0.2   | ---                |
| C   | 192.168.13.80/29 | FastEthernet0/0.103 | ---                |
| C   | 192.168.13.88/29 | FastEthernet0/0.104 | ---                |
| C   | 192.168.13.96/29 | FastEthernet0/1.4   | ---                |
| R   | 192.168.13.0/29  | FastEthernet0/1.4   | 192.168.13.98      |
| R   | 192.168.13.16/29 | FastEthernet0/1.4   | 192.168.13.99      |
| R   | 192.168.13.32/29 | FastEthernet0/1.4   | 192.168.13.98      |
| R   | 192.168.13.40/29 | FastEthernet0/1.4   | 192.168.13.99      |
| R   | 192.168.13.48/29 | FastEthernet0/1.4   | 192.168.13.98      |
| R   | 192.168.13.56/29 | FastEthernet0/1.4   | 192.168.13.99      |
| R   | 192.168.13.64/29 | FastEthernet0/1.4   | 192.168.13.98      |
| R   | 192.168.13.72/29 | FastEthernet0/1.4   | 192.168.13.99      |
| R   | 192.168.13.8/29  | FastEthernet0/1.4   | 192.168.13.98      |

Рис. 15. Таблица маршрутизации для Marsh3

Анализ таблицы показывает путь к сети 192.168. 13.0/29 (где находится WEB – сервер) прописан с помощью протокола RIP и следующим hop (после

Marsh3) будет сеть 198.168.13.98 (Marsh1).

### 3.4. Настройка серверов

Как правило, сервер отдает в сеть свои ресурсы, а клиент эти ресурсы использует. Также, на серверах устанавливаются специализированное программное и аппаратное обеспечение. На одном компьютере может работать одновременно несколько программ-серверов. Сервисы серверов часто определяют их название. Серверная ферма для проектируемой компьютерной сети содержит три сервера:

HTTP (WEB) сервер – позволяет создавать простейшие веб-странички и проверять прохождение пакетов на 80-ый порт сервера. Эти серверы предоставляют доступ к веб-страницам и сопутствующим ресурсам, например, картинкам.

DHCP сервер – позволяет организовывать пулы сетевых настроек для автоматического конфигурирования сетевых интерфейсов. Dynamic Host Configuration Protocol обеспечивает автоматическое распределение IP-адресов между компьютерами в сети. Такая технология широко применяется в локальных сетях с общим выходом в Интернет.

FTP – файловый сервер. В его задачи входит хранение файлов и обеспечение доступа к ним клиентских ПК, например, по протоколу FTP. Ресурсы файл-сервера могут быть либо открыты для всех компьютеров в сети, либо защищены системой идентификации и правами доступа.

#### 3.4.1. Настройка Web-сервера.

Для создания HTTP-сервера перейдем на вкладку “Config”, выберем меню “HTTP” и настроим страницу сайта, который будет открываться у пользователей ПК (рис. 16).

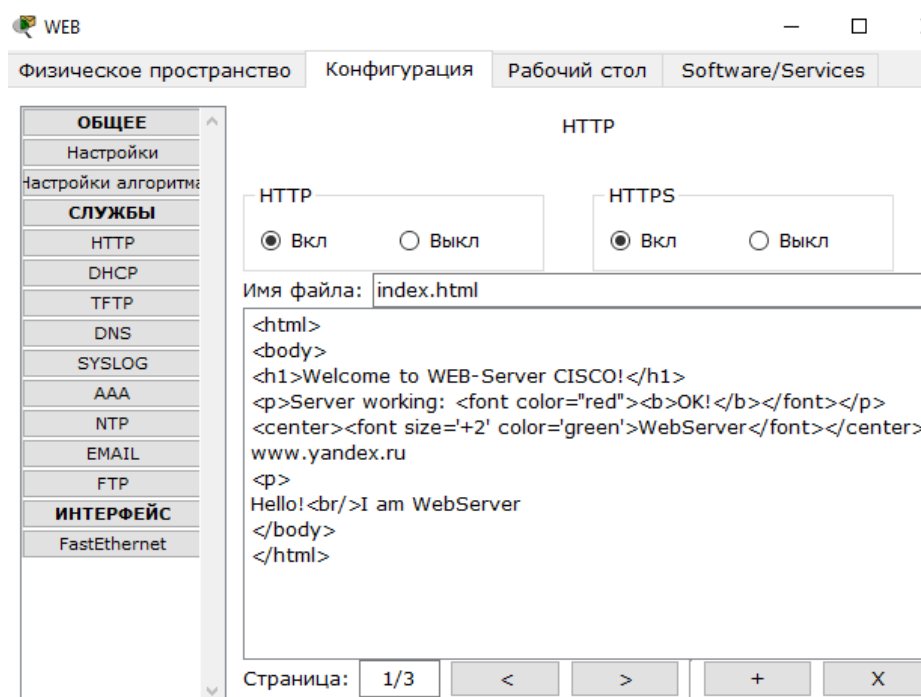


Рис. 16. Настройка HTTP-сервера.

Для того, чтобы бы вместо IP-адреса вводить в браузер название сайта, необходимо обеспечить функции DNS-сервера. Для их настройки переходим в меню “DNS”. Сначала в ресурсной записи типа A Record свяжем доменное имя компьютера webserver с его IP адресом 192.168.19.36, а затем в ресурсной записи типа CNAME свяжем название сайта с сервером (рис. 17).

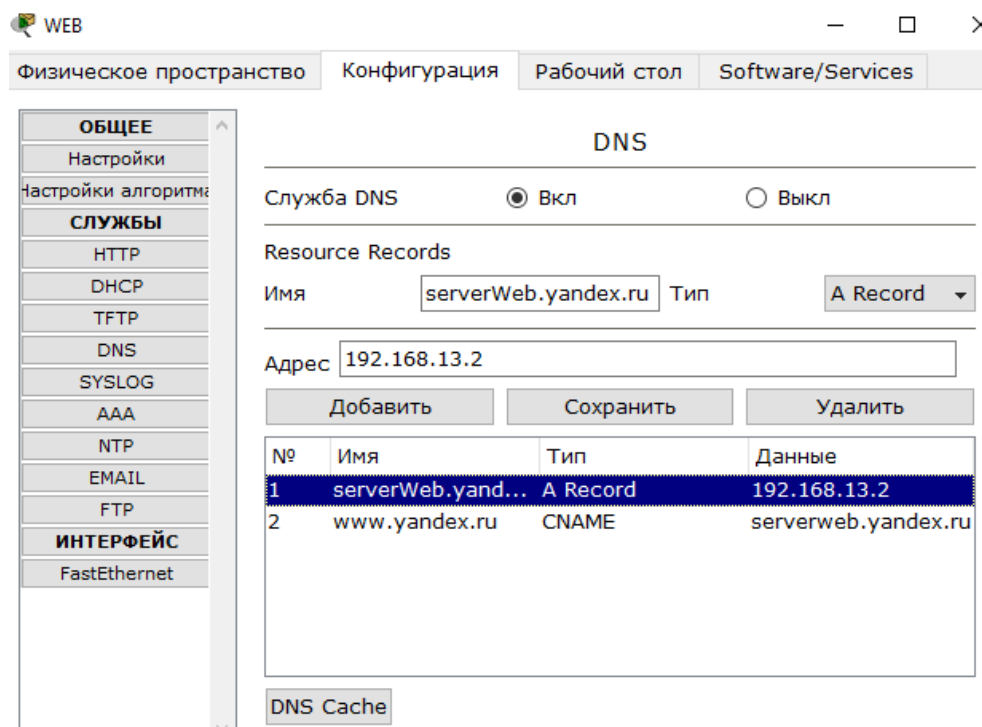


Рис. 17. Настройка функции DNS-сервера.

Для проверки работы Web-сервера в браузере любого ПК введем выбранное имя сайта www.yandex.ru, и если web-страница отображается, то этот сервис работает (рис. 18).

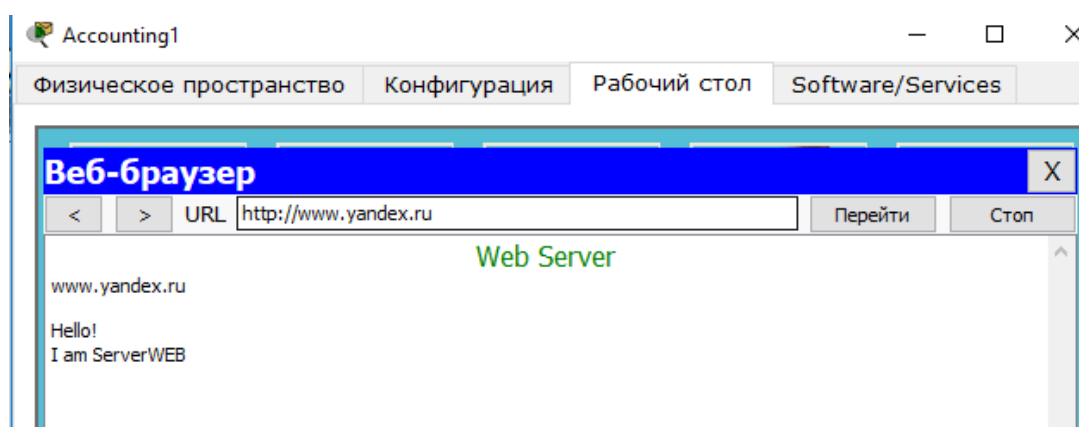


Рис.18.Текст web-страницы

### 3.4.2. Настройка службы DHCP на WEB-сервере

Войдем в конфигурацию и на вкладке DHCP настроим службу. Для этого наберем новые значения пула, установим переключатель On и нажмем на кнопку Save (Сохранить) - рис. 19.

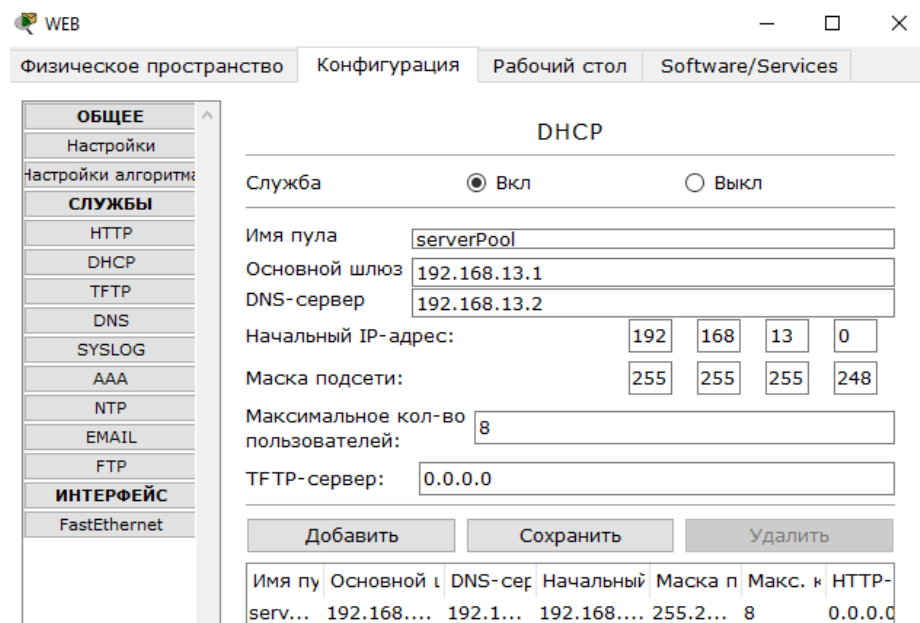


Рис. 19. Настройка DHCP сервера

Для проверки работы клиентов войдем в конфигурацию хоста PC-DHCP и в командной строке сконфигурируем протокол TCP/IP. Для этого командой PC> ipconfig /release сбросим (очистим) старые параметры IP-адреса (рис.20).

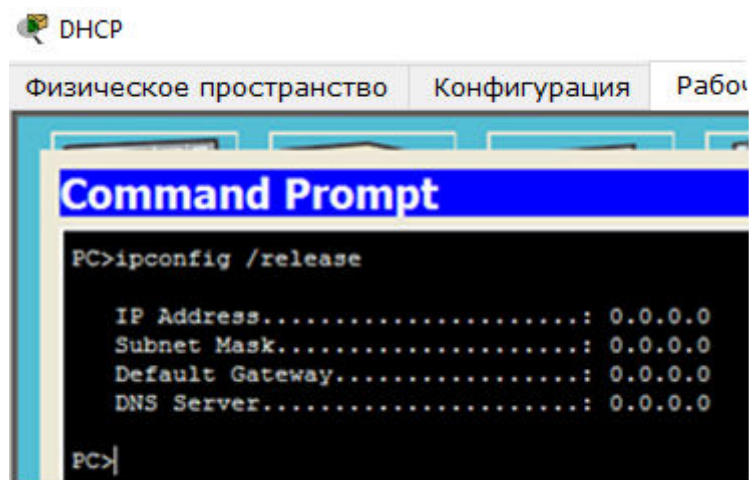


Рис. 20. Удаление конфигурации IP-адресов для всех адаптеров

**Примечание.** Команда *ipconfig /release* отправляет сообщение DHCP RELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан). Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

Теперь командой *ipconfig /renew* получим новые параметры от DHCP сервера (рис. 21).

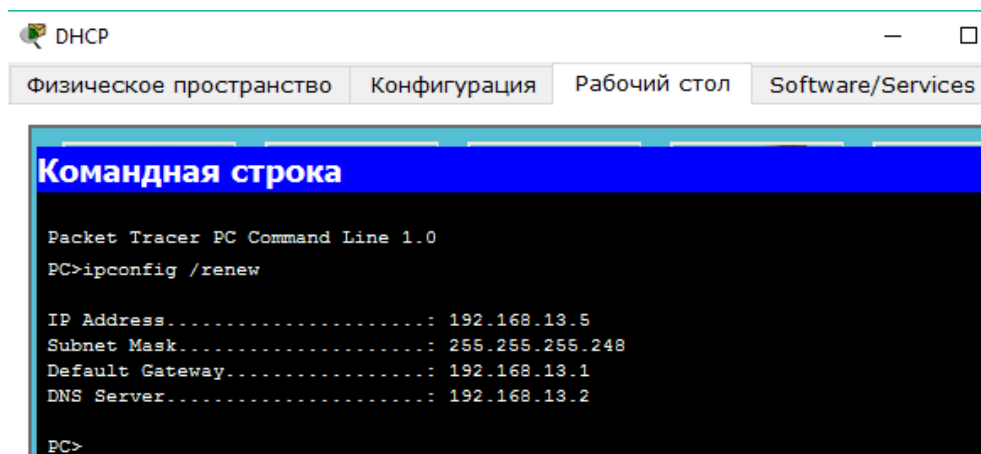


Рис. 21. Конфигурация протокола TCP/IP клиента от DHCP сервера

Теперь проверим работу WEB сервера, открыв сайт в браузере на DHCP (рис. 22) и убедимся, что служба работает.

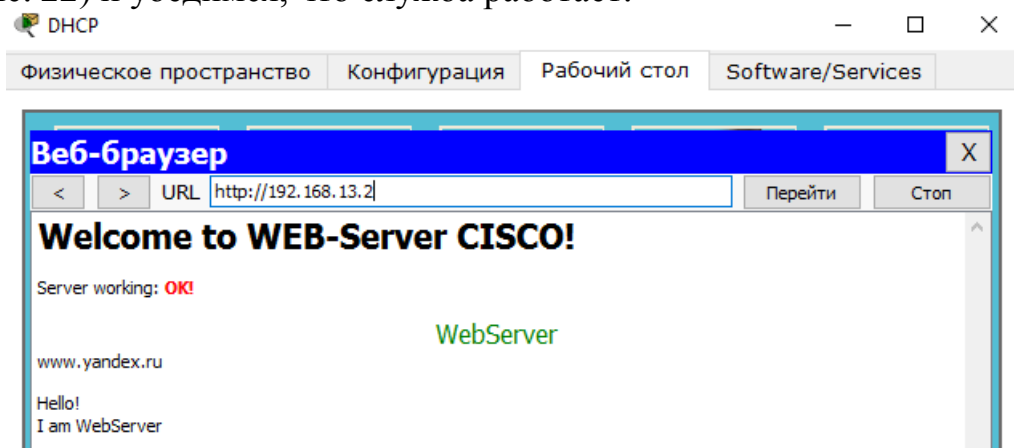


Рис. 22. Проверка работы службы HTTP на DHCP

### 3.5. Настройка списков доступа ACL

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. Маршрутизатор проверяет каждый пакет и на основании критериев, указанных в ACL, определяет, пропустить его или отбросить. Типичными критериями являются:

- адреса отправителя и получателя пакета;
- тип протокола и т.д.

Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Пакет, который не соответствует ни одному из введенных критериев, будет отклонен. Для каждого протокола на интерфейс может быть назначен только один список доступа.

Согласно заданию на курсовую работу, доступ к FTP-серверу должен

иметь лишь один ПК из каждой локальной сети для всех остальных доступ должен быть запрещен. Для обеспечения этого, воспользуемся расширенными списками доступа, так как стандартный список доступа проверяет только адрес отправителя. Поскольку FTP сервер находится в подсети 192.168.13.0/29, список доступа будет применен к интерфейсу fa0/0.3. Однако не стоит забывать, что помимо FTP-сервера, в той же подсети находятся и другие сервера (Web, DHCP и MAIL), к которым должен быть обеспечен доступ со всех устройств сети. Так как порядок команд в списках доступа важен, необходимо сначала разрешить всем устройствам доступ к серверам - Web, DHCP и MAIL, и только потом разрешить доступ к FILE-серверу по протоколу TCP через порты 20 и 21 для трех ПК (пусть этими ПК будут Accounting1, Accounting2, Accounting3), так как в Cisco действует правило, что не разрешено то запрещено. Пропишем ACL в маршрутизатор Marsh1:

```
Marsh1 (config)#ip access-list extended 101
Marsh1 (config-ext-nacl)#permit ip any host 192.168.13.2
Marsh1 (config-ext-nacl)#permit ip any host 192.168.13.4
Marsh1 (config-ext-nacl)#permit ip any host 192.168.13.5
```

Первая команда - создаёт список правил с номером 101, вторая - разрешает прохождение пакетов Web-server по протоколу IP, третья - разрешает прохождение пакетов Mail-server по протоколу IP и последняя - разрешает прохождение пакетов DHCP по протоколу IP.

В список правил с номером 101 добавим 3 разрешающих правила - трём ПК (Accounting1, Accounting2, Accounting3), как указано в задании, для портов сервера 21 и 20 (эти порты служат для авторизации и передачи файлов сервиса FTP):

```
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.66 host 192.168.13.3 eq 20
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.66 host 192.168.13.3 eq 21
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.74 host 192.168.13.3 eq 20
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.74 host 192.168.13.3 eq 21
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.82 host 192.168.13.3 eq 20
Marsh1 (config-ext-nacl)#permit tcp host 192.168.13.82 host 192.168.13.3 eq 21
Marsh1 (config-ext-nacl)#exit
```

Применим список с номером 101 на вход (in) Fa0/0.3 потому, что трафик входит на этот порт роутера со стороны сети:

```
Marsh1 (config)#int fa0/0.3
Marsh1 (config-subif)#ip access-group 101 out
```

Просмотреть списки доступа в маршрутизаторе можно командой  
Prosv-gw1#sh access-lists

На рис. 23 показан результат выполнения команды *sh access-lists*.

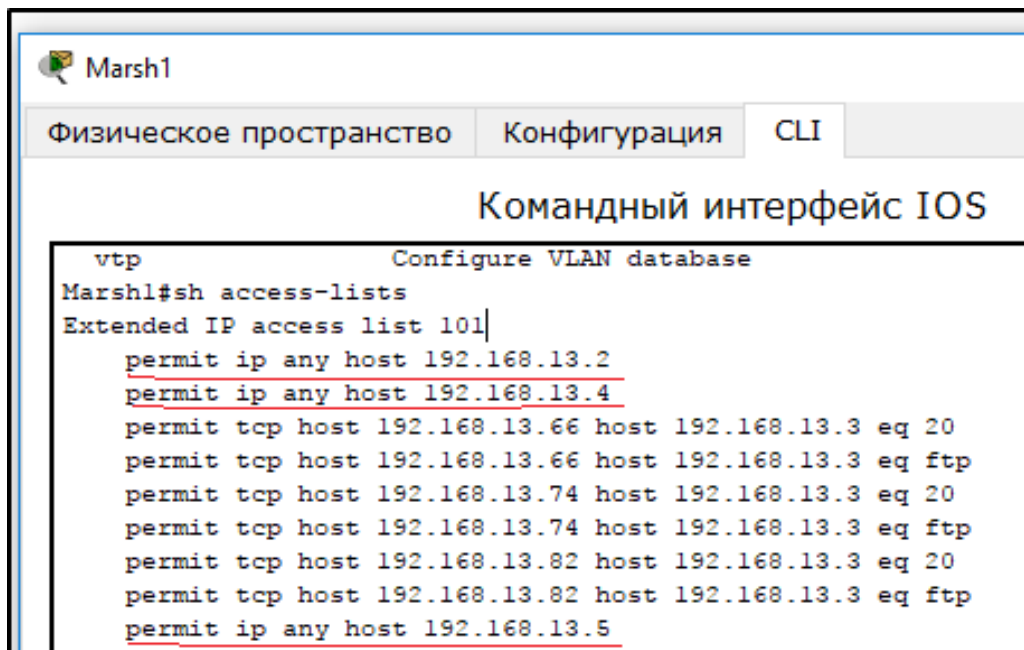


Рис. 23. Результат просмотра списков доступа

Анализ рисунка показывает, что на сервера сети (кроме FTP) разрешен доступ с любого устройства (подчеркнуто красным цветом), а на FTP-сервер лишь с трех вышеперечисленных хостов с IP-адресами – 192.168.13.66, 192.168.13.74 и 192.168.82 относящихся к трем разным подсетям (табл. 3).

Для того, чтобы окончательно убедиться, что введенные правила работают проверим доступ с хостов Accounting2 и РТОЗ (рис.24).

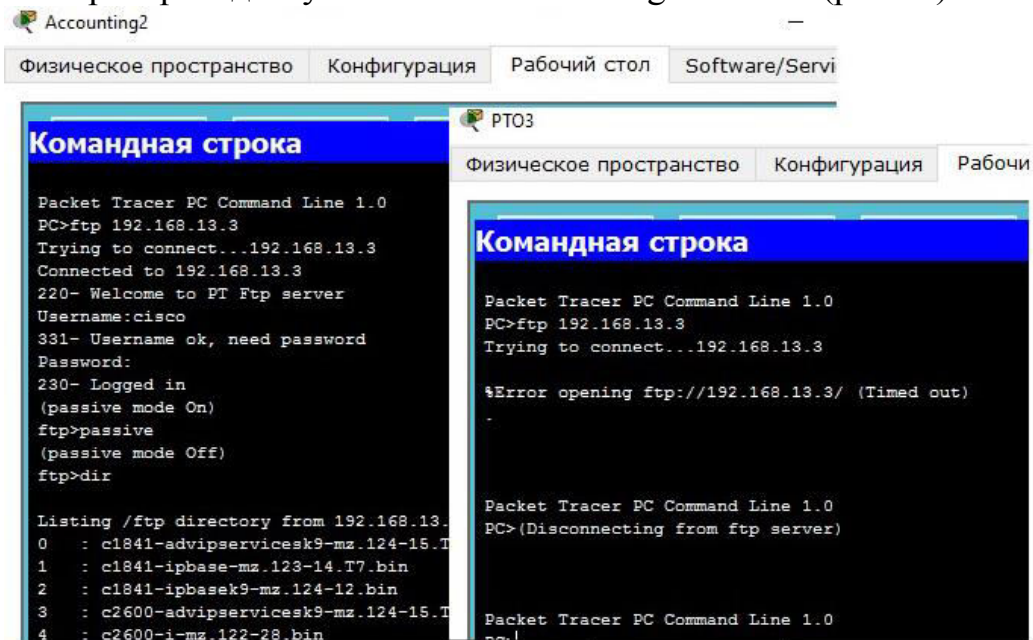


Рис.24. Проверка доступа к файл-серверу с Accounting2 и РТОЗ

Из рис. 24 видно, что обращение от хоста Accounting2 проходит, а от узла РТОЗ – нет. Это и является доказательством работы ACL для спроектированной компьютерной сети и при необходимости можно аналогично проверить все остальные устройства.

### **Заключение**

В рамках данной работы были разработаны методические указания выполнения курсовой работы по дисциплине «Администрирование информационных систем» с помощью симулятора Cisco Packet Tracer. В ходе разработки были выполнены следующие этапы:

- представлено описание программного интерфейса симулятора Packet Tracer;
- даны рекомендации по структуре курсовой работы;
- представлен вариант выполнения курсовой работы.

### **Библиографический список**

Таненбаум Э., Уэзеролл Д. Компьютерные сети – СПб., 2012. - 960 с.  
Олифер В.Г., Олифер И.А. Компьютерные сети – СПб., 2016. - 992 с.  
Хабракен Дж. Как работать с маршрутизаторами Cisco – М.: Изд-во «ДМК Пресс», 2005. - 320 с.

## Оглавление

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Введение .....                                                      | 3  |
| 1. Описание пакета программ Cisco Packet Tracer .....               | 4  |
| 2. Задание и структура курсовой работы .....                        | 5  |
| 3. Пример выполнения курсовой работы .....                          | 8  |
| 3.1. Подготовка структурной схемы сети и задание IP-адресов .....   | 9  |
| 3.1.1. Разработка структурной схемы сети .....                      | 9  |
| 3.1.2 Создание теоретической схемы сетей уровня L-1, L-2, L-3 ..... | 9  |
| 3.1.3 Разработка плана подключения оборудования .....               | 11 |
| 3.2. Настройка VLAN, access и trunk-портов проектируемой сети ..... | 14 |
| 3.2.1. Настройка каналов коммутации между VLAN .....                | 15 |
| 3.2.2. Настройка портов доступа (access) .....                      | 18 |
| 3.2.3. Настройка trunk-портов .....                                 | 20 |
| 3.2.4. Настройка каналов коммутации между VLAN .....                | 22 |
| 3.3. Настройка маршрутизации между LAN .....                        | 25 |
| 3.3.1. Настройка статической маршрутизации .....                    | 26 |
| 3.3.2. Настройка динамической маршрутизации .....                   | 28 |
| 3.4. Настройка серверов .....                                       | 30 |
| 3.4.1. Настройка Web-сервера .....                                  | 31 |
| 3.4.2. Настройка службы DHCP на WEB-сервере .....                   | 32 |
| 3.5. Настройка списков доступа ACL .....                            | 34 |
| Заключение .....                                                    | 37 |
| Библиографический список .....                                      | 37 |