Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
Высшая школа технологии и энергетики
Кафедра прикладной математики и информатики

СЕТЕВЫЕ ТЕХНОЛОГИИ

Выполнение курсовой работы

Методические указания для студентов всех форм обучения
по направлению подготовки
01.03.02 — Прикладная математика и информатика

Составители:
С. В. Тихов
А. И. Кушнеров

Санкт-Петербург
2023

Утверждено
на заседании кафедры ПМИ
26.04.2023 г., протокол № 1

Рецензент П. Е. Антонюк

Методические указания соответствуют программам и учебным планам дисциплины «Сетевые технологии» для студентов, обучающихся по направлению подготовки 01.03.02 «Прикладная математика и информатика». В указаниях представлен порядок выполнения и оформления курсовой работы.

Методические указания предназначены для бакалавров очной формы обучения.

Утверждено Редакционно-издательским советом ВШТЭ СПбГУПТД в качестве методических указаний

Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=202016, по паролю.
- Загл. с экрана.
Дата подписания к использованию 29.12.2023 г. Рег.№ 5120/22

Высшая школа технологии и энергетики СПб ГУПТД
198095, СПб., ул. Ивана Черных, 4.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1. Краткое описание пакета программ «Cisco Packet Tracer» 5
2. Задание и структура курсовой работы 9
3. Пример выполнения курсовой работы 12
3.1. Подготовка структурной схемы сети и задание IP-адресов 13
3.1.1. Разработка структурной схемы сети 13
3.1.2. Создание теоретической схемы сетей уровня L-1, L-2, L-3 14
3.1.3. Разработка плана подключения оборудования 15
3.1.4. Составление IP-плана 17
3.2. Настройка VLAN, access- и trunk-портов проектируемой сети 19
3.2.1. Создание VLAN и настройка каналов коммутации между хостами 22
3.2.2. Создание VLAN с помощью протокола VTP 23
3.2.3. Настройка каналов коммутации между VLAN. 26
3.3. Настройка маршрутизации между сетями и настройка серверов 30
3.3.1. Настройка статической маршрутизации 31
3.3.2. Настройка серверов 33
3.3.2.1. Настройка WEB-сервера 33
3.3.2.2. Настройка службы DHCP на WEB-сервере 34
ЗАКЛЮЧЕНИЕ 37
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 38

ВВЕДЕНИЕ

Цель дисциплины «Сетевые технологии» – 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 «Сетевые технологии» 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. КРАТКОЕ ОПИСАНИЕ ПАКЕТА ПРОГРАММ «CISCO PACKET TRACER»

Cisco является всемирно известным разработчиком и производителем сетевого оборудования. Эта американская компания стремится представить полный спектр сетевого оборудования, и таким образом предоставить клиенту возможность закупить абсолютно всё необходимое сетевое оборудование исключительно у Cisco Systems.

Cisco Packet Tracer – это эмулятор сети, созданный компанией Cisco. Программа позволяет строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. В ней вы получаете возможность изучать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д.

На рисунке 1 представлен интерфейс (главное окно) программы Cisco Packet Tracer.

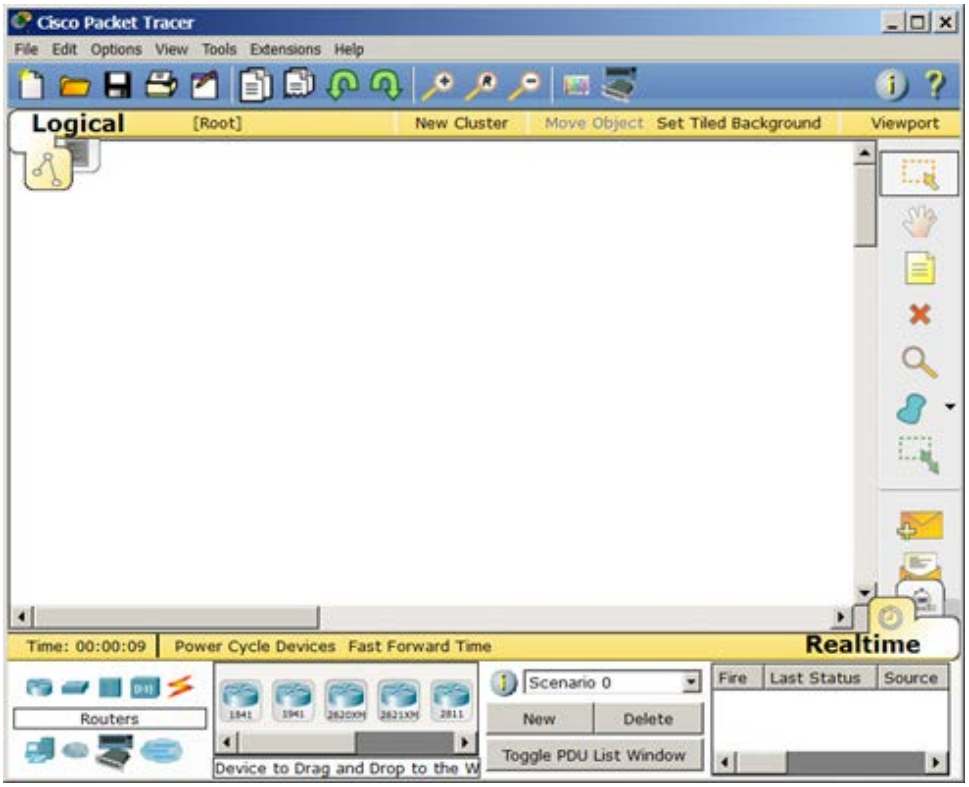


Рисунок 1 – Интерфейс программы Cisco Packet Tracer (CPT)

Снизу под рабочей областью расположена панель оборудования. Данная панель содержит в своей левой части типы (классы) устройств, а в правой части – их наименование (модели). Чтобы поместить устройство на рабочую область программы, его необходимо перетащить мышкой. При наведении курсора на каждое из устройств в прямоугольнике, находящемся в центре между ними, будет отображаться его тип. Типы оборудования представлены на рисунке 2.

Рисунок 2 – Панель оборудования Packet Tracer (Основные типы оборудования)

Маршрутизаторы (роутеры) используются для поиска оптимального маршрута передачи данных на основании алгоритмов маршрутизации. **Коммутаторы** - устройства, предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментов сети. Коммутатор (свитч) передаёт пакеты информации на основании таблицы коммутации, поэтому трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах, как на концентраторе (хабе).

Беспроводные устройства в программе представлены беспроводным маршрутизатором и тремя точками доступа.

Оконечное оборудование - ПК, ноутбук, сервер, принтер, телефоны и так далее.

Тип соединения позволяет выбрать линию связи.

С помощью линий связи создаются соединения узлов сети в единую топологию, и при этом каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов устройств (рис. 3).

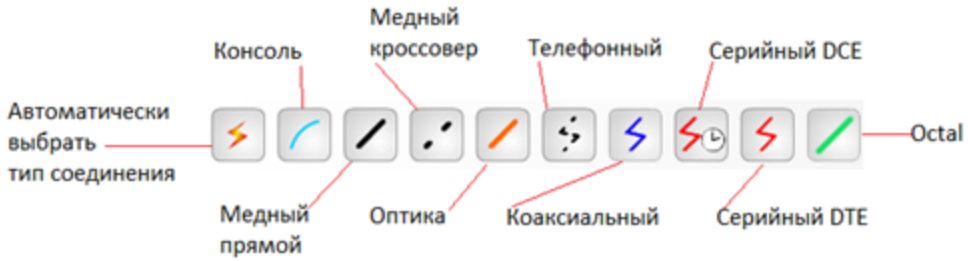


Рисунок 3 – Типы линий связи

Автоматический тип – при данном типе соединения Packet Tracer автоматически выбирает наиболее предпочтительные типы соединения для выбранных устройств.

Консоль – консольное соединение. Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами.

Медь прямой – соединение медным кабелем типа «витая пара», оба конца кабеля обжаты в одинаковой раскладке.

Медь кроссовер – соединение медным кабелем типа «витая пара», концы кабеля обжаты как кроссовер.

Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств, имеющих оптические интерфейсы.

Телефонный кабель – кабель для подключения телефонных аппаратов. Соединение через телефонную линию может быть осуществлено между устройствами, имеющими модемные порты. Пример - ПК, дозванивающийся в сетевое облако.

Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля. Используется для соединения между кабельным модемом и облаком.

Серийный DCE и серийный DTE - соединения через последовательные порты для связей Интернет. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Сторону DCE можно определить по маленькой иконке "часов" рядом с портом.

В программе возможно физическое представление оборудования в виде его физической конфигурации (рис. 4). Для этого необходимо дважды щелкнуть мышью по устройству и перейти на вкладку “**Physical**”.

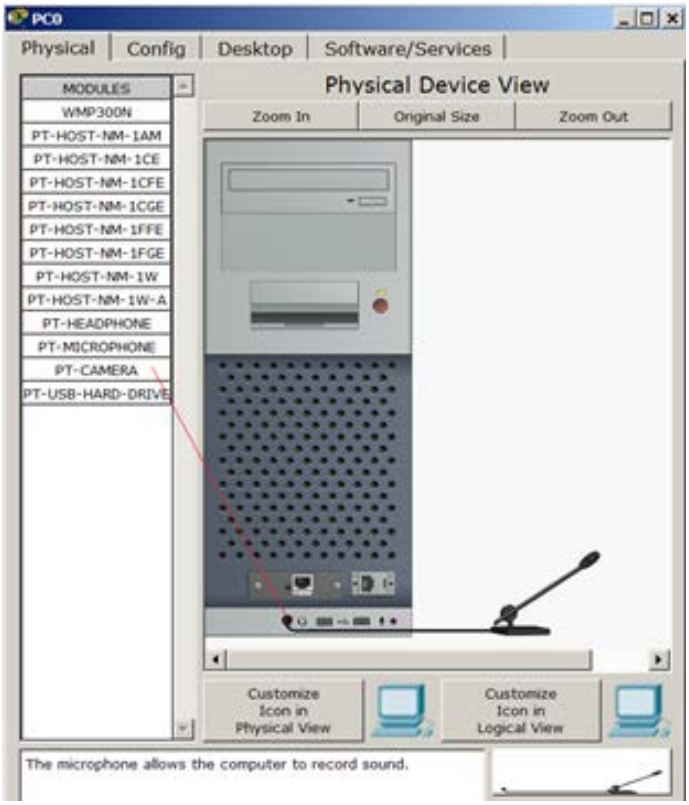


Рисунок 4 – Физическая конфигурация ПК

На вкладке “**Config**” можно изменять конфигурацию программного обеспечения устройства (рис. 5):

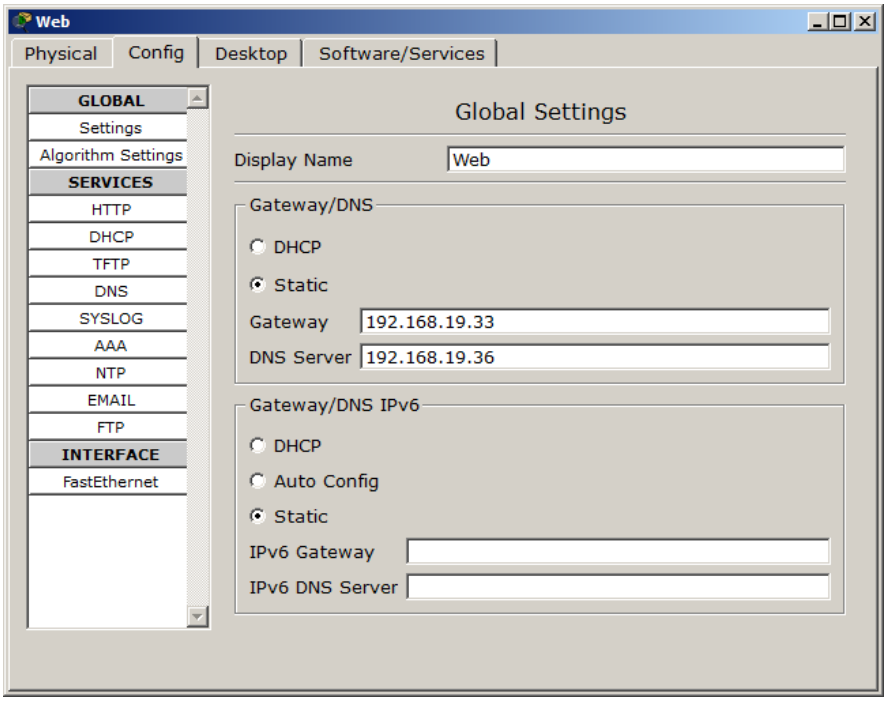


Рисунок 5 – Конфигурация ПО Web-сервера

На вкладке “**Desktop**” можно зайти на рабочий стол устройства (рис. 6):

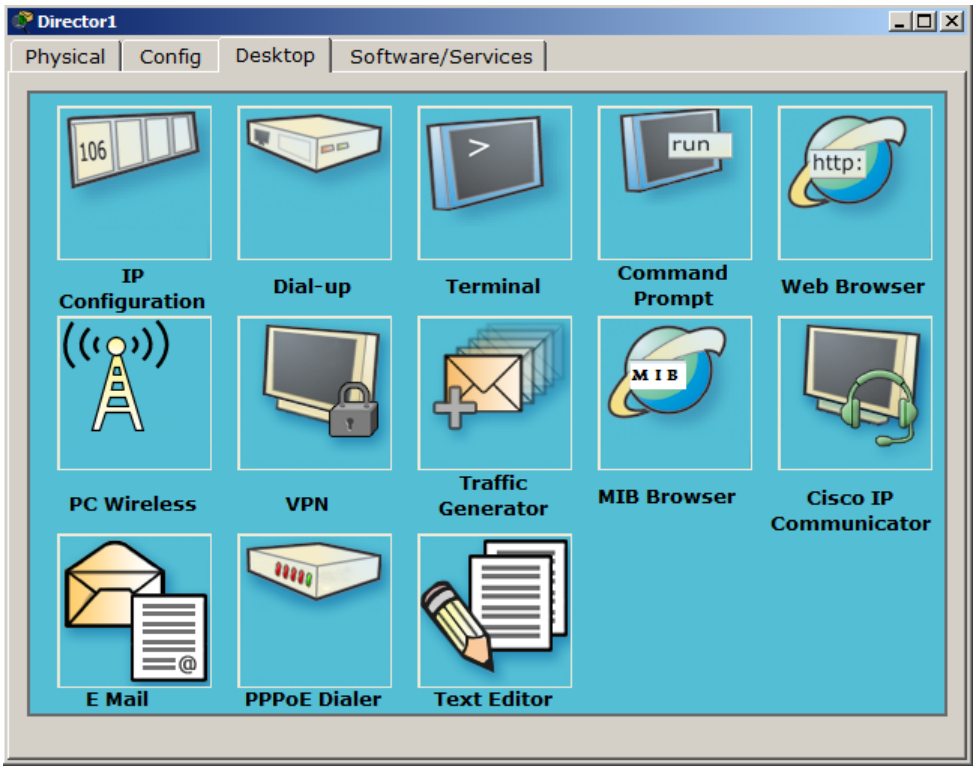


Рисунок 6 – Рабочий стол ПК

Во вкладке “**CLI**” можно открыть командную строку устройства (рис. 7):

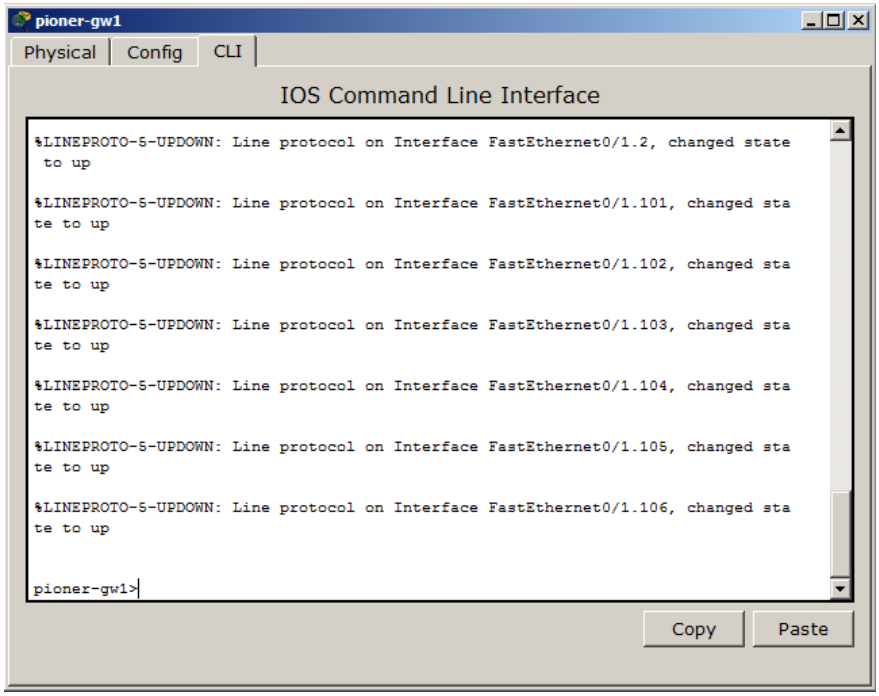


Рисунок 7 – Командная строка маршрутизатора

2. ЗАДАНИЕ И СТРУКТУРА КУРСОВОЙ РАБОТЫ

Целью курсовой работы является приобретение навыков по базовому конфигурированию компьютерной сети, что 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) и сведения о преподавателе (руководителе) (ФИО, подпись);
- наименование места и год 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 рисунке 8.

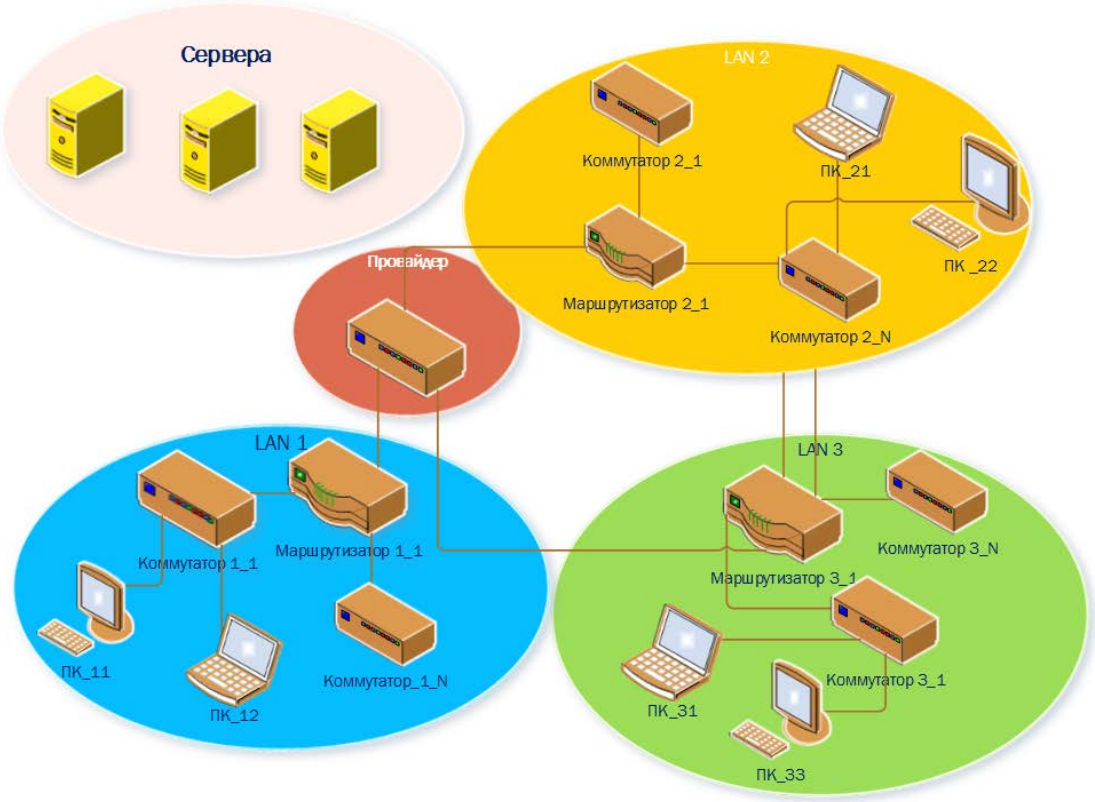


Рисунок 8 – Общая схема сети

Исходные данные для проектирования выбираются студентом из приведенных ниже данных (табл.1.) самостоятельно с учетом своего шифра (порядкового номера в ведомости). Минимальное количество подключаемых маршрутизаторов – три.

Таблица 1 – Варианты задания

№ варианта	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**10**	**12**	**13**	**14**	**15**	**16**
Количество подсетей (VLAN)	8	6	8	7	6	7	9	7	6	7	6	7	6	7	9	9
Минимальное количество ПК в каждой VLAN	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. 192.168.20.0 255.255.255.0

Хост(min): 192.168.20.1
Хост(max): 192.168.20.254

2. 192.168.21.0 255.255.255.0

Хост(min): 192.168.21.1
Хост(max):192.168.21.254

3. 192.168.22.0 255.255.255.0

Хост(min): 192.168.22.1
Хост(max):192.168.22.254

4. 192.168.23.0 255.255.255.0

Хост(min): 192.168.23.1
Хост(max):192.168.23.254

5. 192.168.24.0 255.255.255.0

Хост(min): 192.168.24.1
Хост(max):192.168.24.254

6. 192.168.25.0 255.255.255.0

Хост(min): 192.168.25.1
Хост(max):192.168.25.254

7. 192.168.26.0 255.255.255.0

Хост(min): 192.168.26.1
Хост(max):192.168.26.254

8. 192.168.27 .0 255.255.255.0

Хост(min): 192.168.2 7.1
Хост(max):192.168.27.254

9. 192.168.28.0 255.255.255.0

Хост(min): 192.168.28.1
Хост(max):192.168.28.254

10. 192.168.29.0 255.255.255.0

Хост(min): 192.168.29.1
Хост(max):192.168.29.254

11. 192.168.30.0 255.255.255.0

Хост(min): 192.168.30.1
Хост(max):192.168.30.254

12. 192.168.31.0 255.255.255.0

Хост(min): 192.168.31.1
Хост(max):192.168.31.254

13. 192.168.32.0 255.255.255.0

Хост(min): 192.168.32.1
Хост(max):192.168.32.254

14. 192.168.33.0 255.255.255.0

Хост(min): 192.168.33.1
Хост(max):192.168.33.254

15. 192.168.34.0 255.255.255.0

Хост(min): 192.168.34.1
Хост(max):192.168.34.254

16. 192.168.35.0 255.255.255.0

Хост(min): 192.168.35.1
Хост(max):192.168.35.254

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 хостами, расположенными в разных сетях (все хосты должны быть доступны).

6. Настроить сервера: WEB, DHCP.

3. ПРИМЕР ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Исходные данные вариант 0:

- Количество VLAN: 6;
- Минимальное количество ПК в каждой VLAN: 3;
- Минимальное количество маршрутизаторов: 6.

Начальный IP адрес и маска для проектируемой сети:

192.168.19.0 255.255.255.0
Хост(min): 192.168.19.0
Хост(max): 192.168.19.255

3.1. Подготовка структурной схемы сети и задание IP-адресов

3.1.1. Разработка структурной схемы сети

Для выполнения курсовой работы первым делом необходимо создать компьютерную сеть в модели Cisco Packet Tracer. Рекомендуется предварительно обсудить детали задания и построить теоретическую схему, а не сразу приступать к практике.

Согласно общей схеме сети, представленной на рисунке 8, необходимо создать три локальные сети, подключенные к одному и тому же провайдеру.

Локальная сеть (LAN) — это компьютерная сеть, позволяющая нескольким компьютерам подключаться к Интернету через единую точку доступа. Такой точкой доступа в нашем случае будут выступать маршрутизаторы. Далее, согласно заданию, необходимо создать шесть подсетей (VLAN), в каждой из которых будут находиться минимум шесть ПК. Для удобства поместим в каждую локальную сеть одинаковое количество ПК, то есть двенадцать штук. Помимо этого, к одной из локальных сетей будет подключена серверная ферма, состоящая из трех серверов: Web-сервера, DHCP-сервера и FTP-сервера.

Подключение ПК и серверов к маршрутизаторам будет реализовано через коммутаторы. Еще один коммутатор будет являться симулятором провайдера. Коммутаторы, подключенные к компьютерам и/или серверам, являются устройствами доступа Access switches (ASW), так как к ним подключены конечные пользователи. Таким образом, получим структурную схему сети (рис. 9).

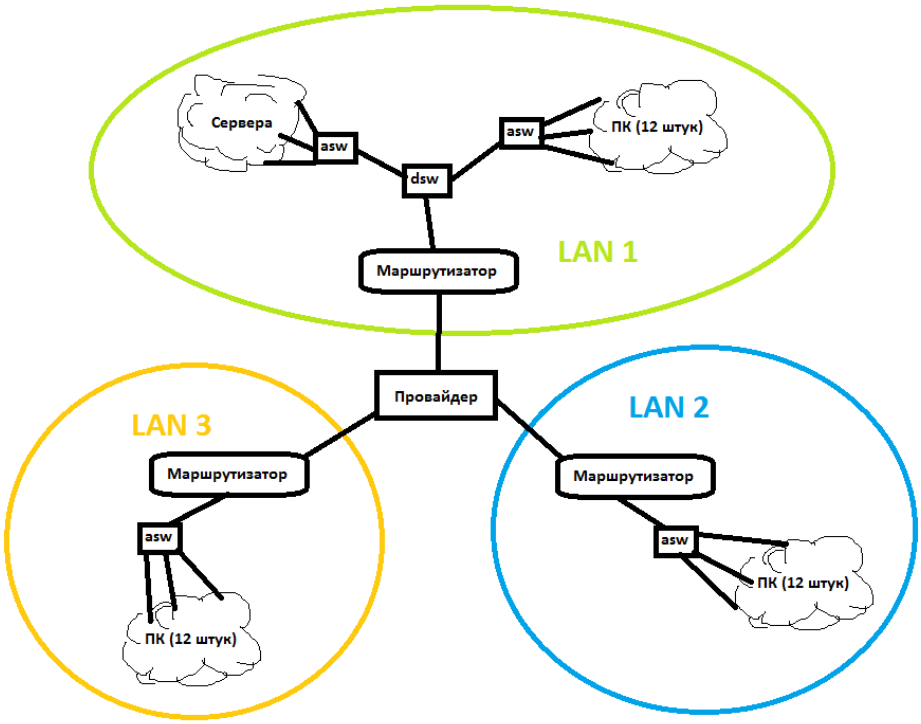


Рисунок 9 – Структурная схема проектируемой сети

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

На схеме L1 (рис. 10) изображены физические устройства сети с номерами портов. Подключение устройств по VLAN показано на схеме L2 (рис. 11), а на рисунке 12 – схема взаимодействия устройств сети на третьем уровне.

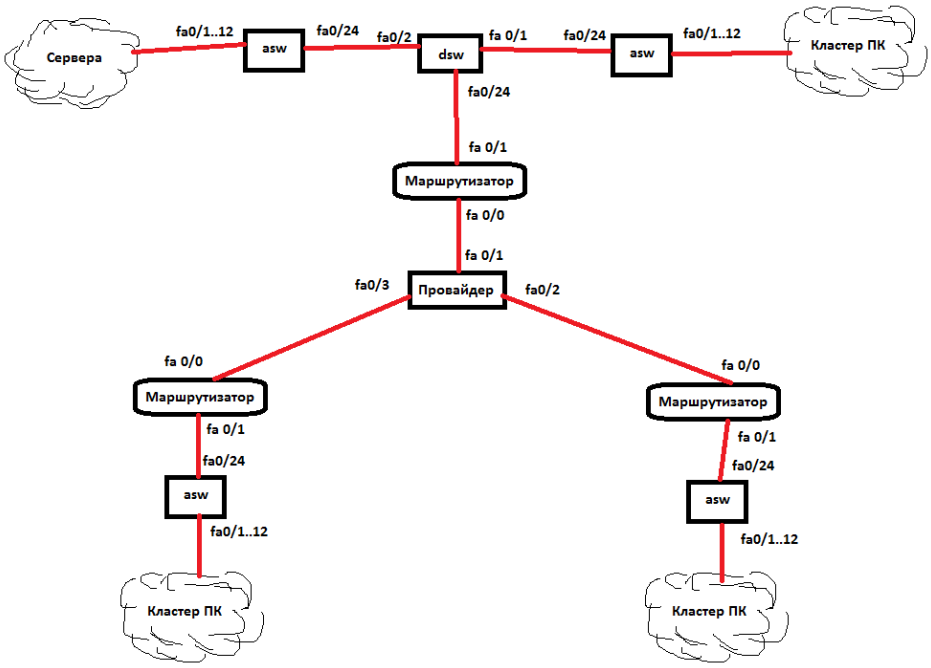


Рисунок 10 – Схема уровня сети L-1

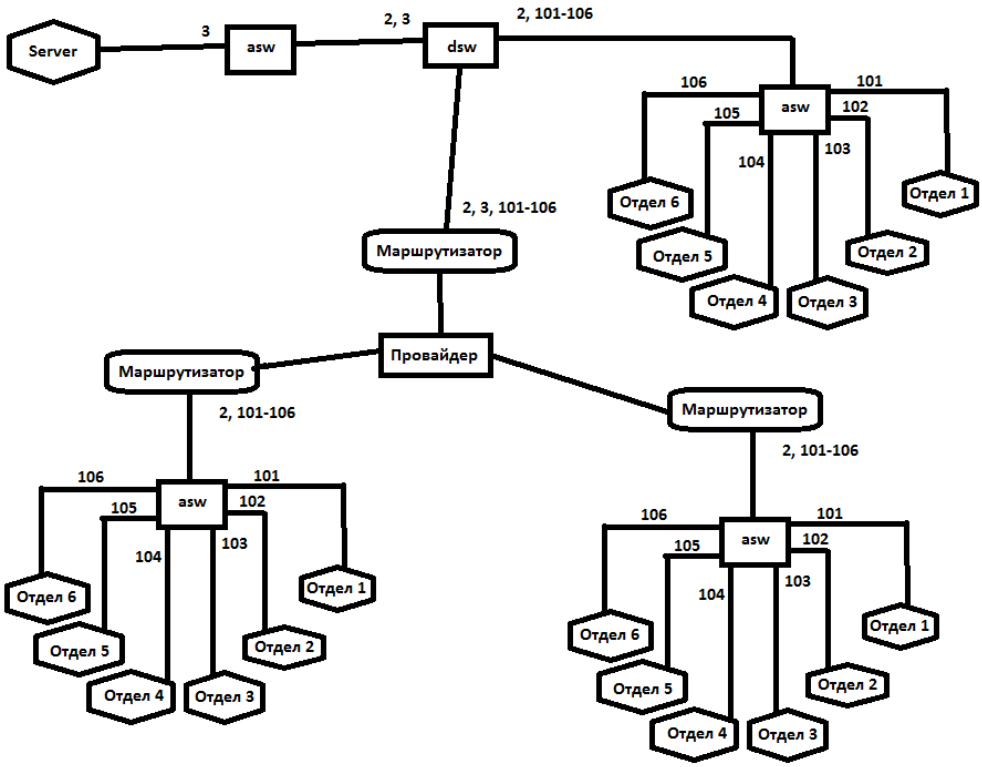


Рисунок 11 – Схема уровня сети L-2

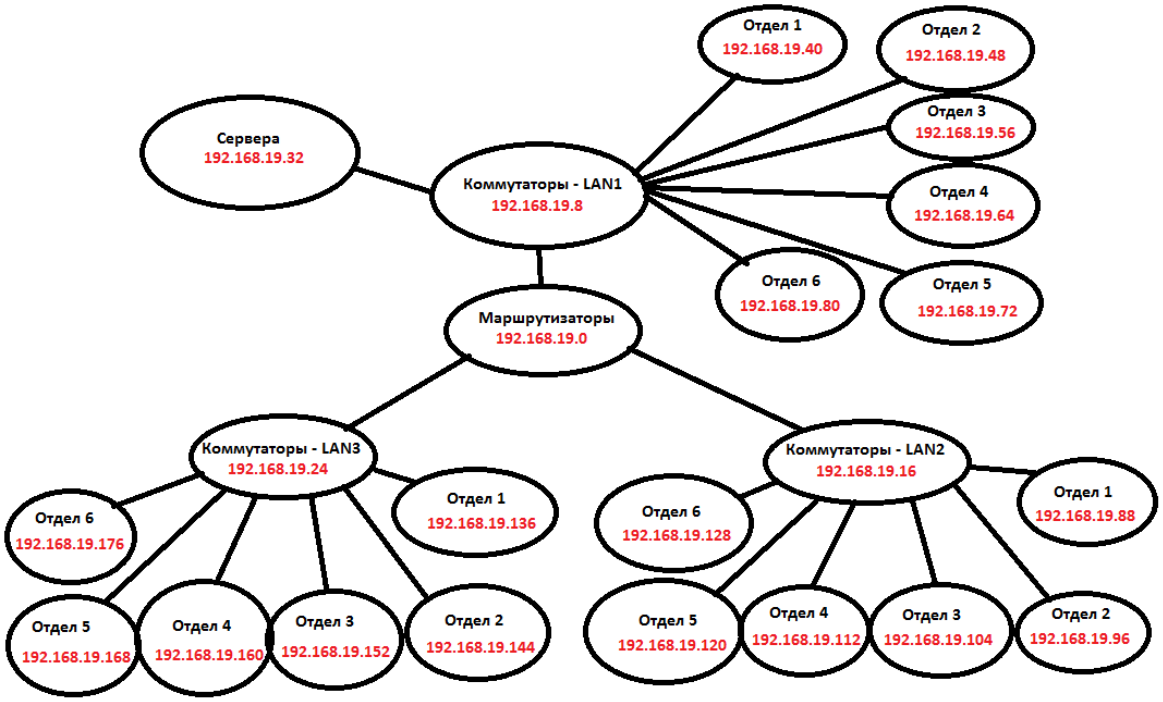


Рисунок 12 – Схема уровня сети L-3

3.1.3. Разработка плана подключения оборудования

Теперь можно приступать непосредственно к практике и созданию компьютерной сети.

1. Необходимо создать на рабочем пространстве программы Cisco Packet Tracer все устройства, количество и расположение которых уже оговорено выше.

2. Все маршрутизаторы будут модели 2811, коммутаторы – доступа (asw) и коммутатор-симулятор провайдера – модели 2950-24, а коммутатор распространения (dsw) – модели 2950-24T, так как эта модель имеет два порта GigabitEthernet.

3. Необходимо дать названия всем устройствам сети. Для удобства представим, что каждая локальная сеть принадлежит какому-нибудь офису, расположенному недалеко от одной из станций метрополитена города Санкт-Петербурга, и назовем локальные сети соответствующе этим станциям. Пусть первая локальная сеть находится в офисе недалеко от метро «Проспект Просвещения», вторая – около «Пионерской» и третья – около «Комендантского Проспекта». Назовем коммутаторы и маршрутизаторы в локальных сетях соответствующе. Для этого заходим в режим командной строки устройства и вводим:

Router>enable
Router#config
Router(config) #hostname prosv-gw1

В названии маршрутизатора “gw” означает “gateway”, или “шлюз”. Названия конечных устройств можно менять на вкладке “Config”, в поле “Display name”. Имена серверов меняем согласно их предназначению (рис. 13).

4. Каждый офис имеет отделы. Пусть одна подсеть VLAN относится к одному отделу. Согласно заданию курсовой работы, необходимо создать шесть VLAN и, соответственно, шесть отделов в каждом офисе. Пусть этими отделами будут: Директора и их заместители (Directors), ПТО (PTO), ФЭО (FEO), Бухгалтерия (Accounting), Охрана (Security) и Другие Пользователи (Other). Даем названия всем ПК в соответствии с отделом, к которому они принадлежат и переходим к соединению узлов сети в единую топологию.

5. Подключение конечных устройств к коммутаторам, а также коммутаторов к маршрутизаторам осуществляется за счёт медных кабелей с обычным обжимом, подключенных к портам устройств и соединяющих их. Для соединения двух коммутаторов требуется медный кабель с кроссоверным обжимом. Таблица подключения по портам представлена на рисунке 13.

Имя устройства	Имя порта	Подключенное устройство
Provider	fa 0/1	prosv-gw1
	fa0/2	pioner-gw1
	fa0/3	komend-gw1
prosv-gw1	fa0/0	Provider
	fa0/1	prosv-dsw1
pioner-gw1	fa0/0	Provider
	fa0/1	pioner-asw1
komend-gw1	fa0/0	Provider
	fa0/1	komend-asw1
prosv-dsw1	fa0/24	prosv-gw1
	gig1/1	prosv-asw1
	gig1/2	prosv-asw2
prosv-asw2	fa0/1	FTP
	fa0/2	DHCP
	fa0/3	Web
	fa0/24	prosv-dsw1
	fa0/4	DHCP CHECK
prosv-asw1	fa0/1..2	Director1/2
	fa0/3..4	FEO1/2
	fa0/5..6	PTO1/2
	fa0/7..8	Accounting1/2
	fa0/9..10	Security1/2
	fa0/11..12	Other1/2
	fa0/24	prosv-dsw1
pioner-asw1	fa0/1..2	Director3/4
	fa0/3..4	FEO3/4
	fa0/5..6	PTO3/4
	fa0/7..8	Accounting3/4
	fa0/9..10	Security3/4
	fa0/11..12	Other3/4
	fa0/24	pioner-gw1
komend-asw1	fa0/1..2	Director5/6
	fa0/3..4	FEO5/6
	fa0/5..6	PTO5/6
	fa0/7..8	Accounting5/6
	fa0/9..10	Security5/6
	fa0/11..12	Other5/6
	fa0/24	komend-gw1

Рисунок 13 – Таблица подключения по портам

Получившаяся в программе CISCO Packet Tracer схема сети представлена на рисунке 14.

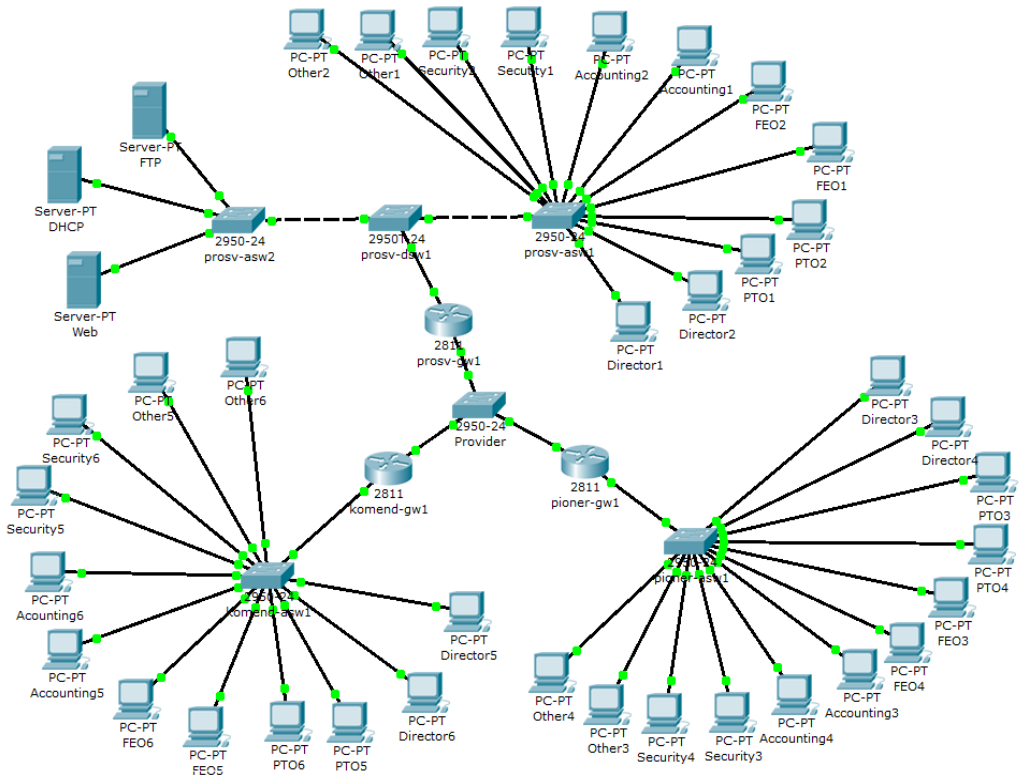


Рисунок 14 – Схема компьютерной сети в программе Cisco Packet Tracer.

3.1.4. Составление IP-плана

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. 15).

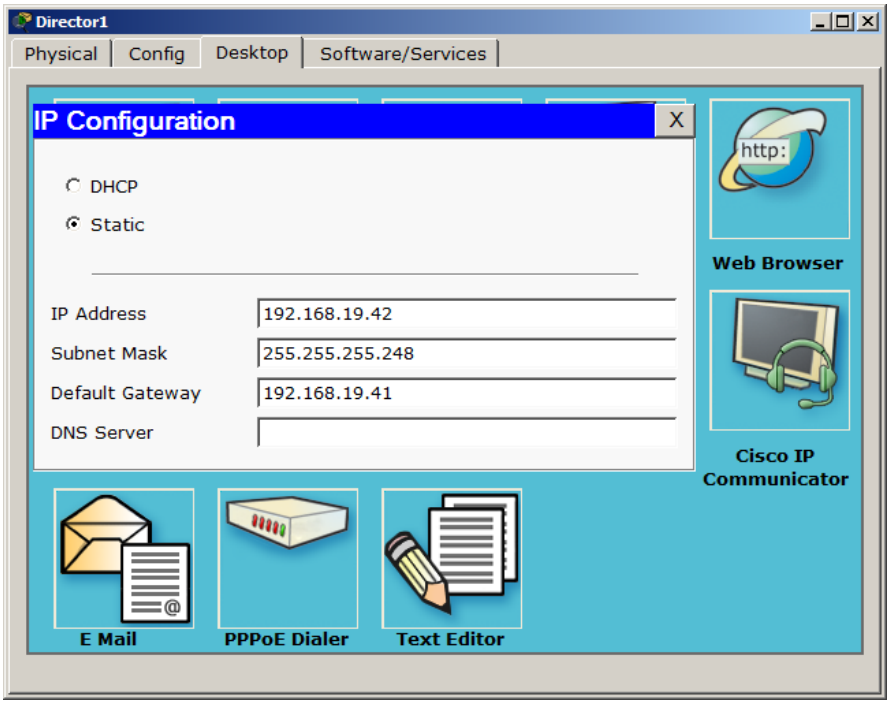


Рисунок 15 – Настройка IP-адреса, маски подсети и шлюза для ПК

Составляем IP-план, по которому назначим IP-адреса каждому узлу сети. План включает в себя название устройства, его адрес, номер подсети и шлюз подсети. Рассчитать номера подсетей можно вручную, а можно с помощью IP-калькулятора. Можно использовать калькулятор, размещенный на Интернет-ресурсе http://ip-calculator.ru/.

Получившийся IP-план представлен на рисунке 16, где 192.168.19.0/24 – адрес проектируемой сети (вариант 0).

	192.168.19.2	prosv-gw1	192.168.19.1	192.168.19.0
	192.168.19.3	pioner-gw1		
	192.168.19.4	komend-gw1		
	192.168.19.10	prosv-dsw1	192.168.19.9	192.168.19.8
	192.168.19.11	prosv-asw1		
	192.168.19.12	prosv-asw2		
	192.168.19.18	pioner-asw1	192.168.19.17	192.168.19.16
	192.168.19.26	komend-asw1	192.168.19.25	192.168.19.24
	192.168.19.34	FTP server	192.168.19.33	192.168.19.32
	192.168.19.35	DHCP server		
	192.168.19.36	Web server		
ПРОСВЕЩЕНИЯ	192.168.19.42/43	Director1/2	192.168.19.41	192.168.19.40
	192.168.19.50/51	PTO1/2	192.168.19.49	192.168.19.48
	192.168.19.58/59	FEO1/2	192.168.19.57	192.168.19.56
	192.168.19.66/67	Acc1/2	192.168.19.65	192.168.19.64
	192.168.19.74/75	Sec1/2	192.168.19.73	192.168.19.72
	192.168.19.82/83	Oth1/2	192.168.19.81	192.168.19.80
ПИОНЕРСКАЯ	192.168.19.90/91	DIr3/4	192.168.19.89	192.168.19.88
	192.168.19.98/99	PTO3/4	192.168.19.97	192.168.19.96
	192.168.19.106/107	FEO3/4	192.168.19.105	192.168.19.104
	192.168.19.114/115	Acc3/4	192.168.19.113	192.168.19.112
	192.168.19.122/123	Sec3/4	192.168.19.121	192.168.19.120
	192.168.19.130/131	Oth3/4	192.168.19.129	192.168.19.128
КОМЕНДАНТСКИЙ	192.168.19.137/138	Dir5/6	192.168.19.137	192.168.19.136
	192.168.19.146/147	PTO5/6	192.168.19.145	192.168.19.144
	192.168.19.154/155	FEO5/6	192.168.19.153	192.168.19.152
	192.168.19.162/163	Acc5/6	192.168.19.161	192.168.19.160
	192.168.19.170/171	Sec5/6	192.168.19.169	192.168.19.168
	192.168.19.178/179	Oth5/6	192.168.19.177	192.168.19.176

Рисунок 16 – IP-план проектируемой сети

Теперь можно перейти к созданию и настройке VLAN access и trunk-портов проектируемой сети.

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, 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.

В Cisco используется следующая терминология портов:

- Access port – порт, принадлежащий одному VLAN и передающий нетегированный трафик. По спецификации Cisco, access порт может принадлежать только одному VLAN, по умолчанию это первый (нетегированный) VLAN. Любой кадр, который проходит через access порт, помечается номером, принадлежащим этому VLAN.
- Trunk port – порт, передающий тегированный трафик одного или нескольких VLAN. Этот порт, наоборот, не изменяет тег, а лишь пропускает кадры с тегами, которые разрешены на этом порту
- Порты, в которые подключены конечные устройства, следует настроить как access-порты, а остальные – как trunk.

Пусть VLAN под номером 2 будет VLAN’ом управления, в который будут входить маршрутизаторы и коммутаторы. VLAN 3 отведем под серверную ферму. Шести отделам офисов отведем VLAN’ы со 101 номера по 106 соответственно. Номера с 4 по 100 оставим как резерв. В связи с этим, дополним нашу таблицу подключения оборудования по портам номерами VLAN и типами портов – access или trunk (рис. 17).

Имя устройства	Имя порта	Подключенное устройство	Mode	VLAN
Provider	fa 0/1	prosv-gw1	Trunk	2
	fa0/2	pioner-gw1	Trunk	2
	fa0/3	komend-gw1	Trunk	2
prosv-gw1	fa0/0	Provider	Trunk	2
	fa0/1	prosv-dsw1	Trunk	2
pioner-gw1	fa0/0	Provider	Trunk	2
	fa0/1	pioner-asw1	Trunk	2
komend-gw1	fa0/0	Provider	Trunk	2
	fa0/1	komend-asw1	Trunk	2
prosv-dsw1	fa0/24	prosv-gw1	Trunk	2
	gig1/1	prosv-asw1	Trunk	2
	gig1/2	prosv-asw2	Trunk	2
prosv-asw2	fa0/1	FTP	Access	3
	fa0/2	DHCP	Access	3
	fa0/3	Web	Access	3
	fa0/24	prosv-dsw1	Trunk	2
	fa0/4	DHCP CHECK	Access	3
prosv-asw1	fa0/1..2	Director1/2	Access	101
	fa0/3..4	FEO1/2	Access	102
	fa0/5..6	PTO1/2	Access	103
	fa0/7..8	Accounting1/2	Access	104
	fa0/9..10	Security1/2	Access	105
	fa0/11..12	Other1/2	Access	106
	fa0/24	prosv-dsw1	Trunk	2
pioner-asw1	fa0/1..2	Director3/4	Access	101
	fa0/3..4	FEO3/4	Access	102
	fa0/5..6	PTO3/4	Access	103
	fa0/7..8	Accounting3/4	Access	104
	fa0/9..10	Security3/4	Access	105
	fa0/11..12	Other3/4	Access	106
	fa0/24	pioner-gw1	Trunk	2
komend-asw1	fa0/1..2	Director5/6	Access	101
	fa0/3..4	FEO5/6	Access	102
	fa0/5..6	PTO5/6	Access	103
	fa0/7..8	Accounting5/6	Access	104
	fa0/9..10	Security5/6	Access	105
	fa0/11..12	Other5/6	Access	106
	fa0/24	komend-gw1	Trunk	2

Рисунок 17 – Таблица подключения по портам с учетом VLAN

Создать VLAN можно в любом роутере или коммутаторе в консоли, с помощью команд

Prosv-asw1>enable

Prosv-asw1#vlan database

Prosv-asw1(vlan)#vlan 2 name Management

Созданные VLAN можно просмотреть на вкладке “Config” в меню “VLAN Database” (рис. 18).

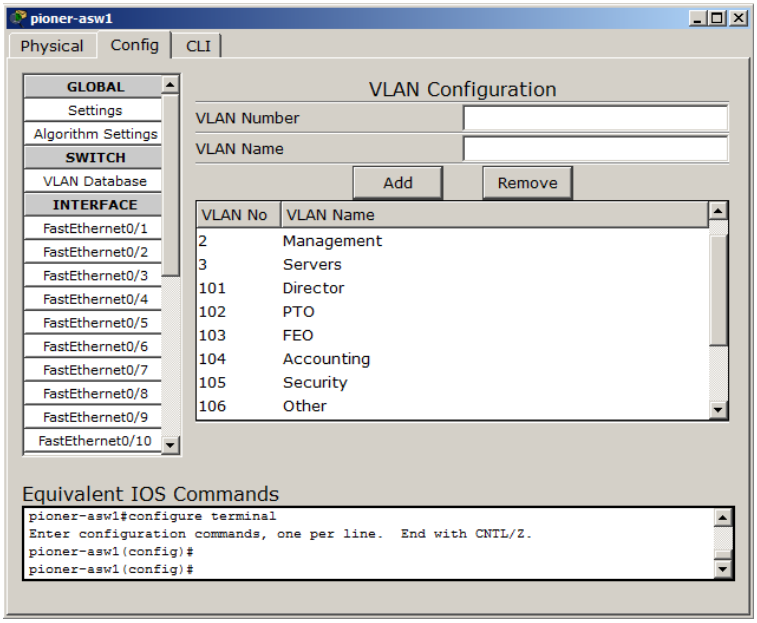


Рисунок 18 – База данных VLAN в коммутаторе pioner-asw1

3.2.1. Создание VLAN и настройка каналов коммутации между хостами

Для упорядочивания хода работы разберём, что необходимо выполнить при настройке каналов коммутации:

1) Настроить hostname. Это поможет в будущем на реальной сети быстро сориентироваться, где вы находитесь:

Switch(config)#hostname HOSTNAME

2) Создать все VLAN и дать им название:

Switch(config)#vlan VLAN-NUMBER
Switch(config-vlan)#name NAME-OF-VLAN

3) Настроить все access-порты и задать им имя:

Switch(config-if)#description DESCRIPTION-OF-INTERFACE
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan VLAN-NUMBER

Удобно иногда бывает настраивать интерфейсы сразу одной командой:

msk-arbat-asw3(config)#interface range FastEthernet 0/6 – 10
msk-arbat-asw3(config-if-range)#description FEO
msk-arbat-asw3(config-if-range)#switchport mode access
msk-arbat-asw3(config-if-range)#switchport access vlan 102

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

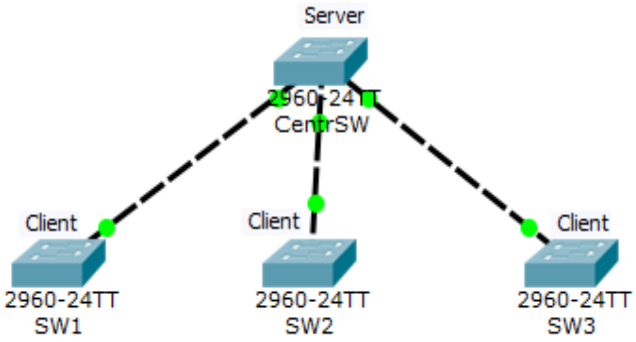
В соответствии с принятой последовательностью создадим все VLAN, в соответствии с командами и таблицей на рисунке 17. Необходимо, чтобы каждый

маршрутизатор и коммутатор “знал” созданные нами VLAN, поэтому такую базу данных придется создать в каждом маршрутизаторе и коммутаторе. После создания баз данных необходимо настроить маршрутизацию между VLAN.

3.2.2. Создание VLAN с помощью протокола VTP

Для упрощения и сокращения времени при создании VLAN можно использовать протокол VTP. **Протокол VTP (англ. VLAN Trunking Protocol)** – проприетарный протокол компании Cisco, служащий для обмена информацией о VLAN-ах. Для настройки **VLAN,** достаточно прописать их на одном коммутаторе, а все остальные будут синхронизированы с его базой.

Пример. Рассмотрим схему, представленную на рисунке 19, состоящую из 4 коммутаторов (один из них является VTP-сервером, а 3 остальных клиентами).



Рисунке 19 – Настраиваемая конфигурация

VLAN, которые будут созданы на сервере, автоматически синхронизируются на клиентах. VTP может создавать, изменять и удалять VLAN. Каждое такое действие влечет к тому, что увеличивается номер ревизии (каждое действие увеличивает номер на +1). Клиенты, получившие это объявление, сравнивают свой номер ревизии с пришедшим. И если пришедший номер выше, они синхронизируют свою базу с ней. В противном случае объявление игнорируется.

VTP может задавать следующие режимы работы;

- VTP Server. Может создавать, изменять и удалять VLAN. Если получает объявления, в которых ревизия старше его, то синхронизируется. Постоянно рассылает объявления и ретранслирует от соседей.
- VTP Client. Создавать, изменять и удалять VLAN нельзя, вся информация получается и синхронизируется от сервера. Периодически сообщает соседям о своей базе VLAN.
- VTP Transparent – эта независимый режим. Может создавать, изменять и удалять VLAN только в своей базе.

По умолчанию все коммутаторы работают в режиме сервера.

Последовательность действий:

1. Проверить, что центральный коммутатор в режиме находится в режиме Server. Введем команду show vtp status (рис. 20):

```
CentrSW#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Рисунок 20 – Выполнение команды show vtp status

Видим, что VTP Operating Mode: Server, ревизия нулевая.

2. Настроим коммутаторы SW1, SW2, SW3:

SW1(config)#vtp mode client
*Setting device to VTP **CLIENT** mode*

Устройство перешло в клиентский режим. Остальные настраиваются точно также. Чтобы устройства смогли обмениваться объявлениями, они должны находиться в одном домене. Если устройство (в режиме Server или Client) не состоит ни в одном домене, то при первом полученном объявлении, оно перейдет в объявленный домен. Если же клиент состоит в каком-то домене, то принимать объявления от других доменов не будет. Откроем SW1 и убедимся, что он не состоит ни в одном домене (рис. 21):

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Рисунок 21 – Выполнение команды Status

3. Переведем центральный коммутатор в домен cisadmin.ru:

CentrSW(config)#vtp domain cisadmin.ru
Changing VTP domain name from NULL to cisadmin.ru

Имя домена изменилось (рис. 22).

```
CentrSW#sh
CentrSW#show vtp s
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : cisadmin.ru
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA4 0xF7 0xDE 0x24 0x07 0x3D 0x91 0xD2
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Рисунок 22 – Перевод центрального коммутатора в домен cisadmin.ru

Обратите внимание, что номер ревизии пока что нулевой. Он изменится, как только мы создадим на нем VLAN. Но перед созданием надо перевести симулятор в режим simulation, чтобы посмотреть, как он сгенерирует объявления.

4. Создадим 20-ый VLAN и увеличим номер ревизии (рис. 23)

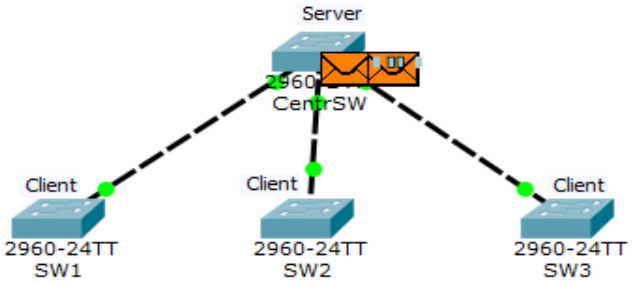


Рисунок 23 – Генерация объявлений

Как только создан VLAN и увеличился номер ревизии, сервер генерирует объявления. У него их два. Сначала откроем то, что находится левее. Это объявление называется «Summary Advertisement» или на русском «сводное объявление» (рис. 24). Это объявление, в котором рассказывается об имени домена и текущей ревизии, генерируется коммутатором раз в 5 минут.

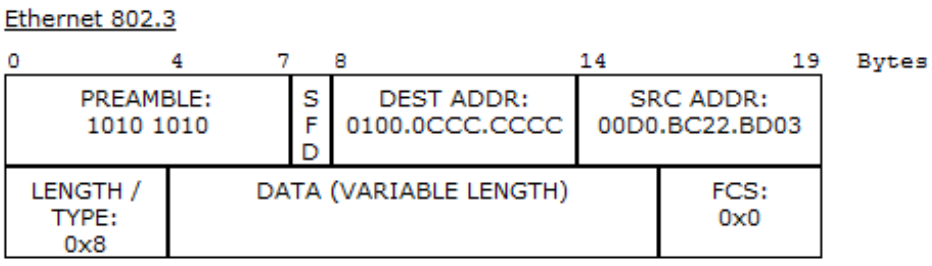


Рисунок 24 – Объявление «Summary Advertisement»

Теперь посмотрим на следующее генерируемое сообщение. Оно называется «Subset Advertisement» или «подробное объявление». Это подробная информация о каждом передаваемом VLAN (рис. 25).

Предусмотрен отдельный заголовок для каждого типа VLAN. Список

настолько длинный, что не поместился в экран. Клиенты видят, что номер ревизии выше, чем у них, и синхронизируют базу. И отправляют сообщение серверу о том, что база VLAN изменилась.

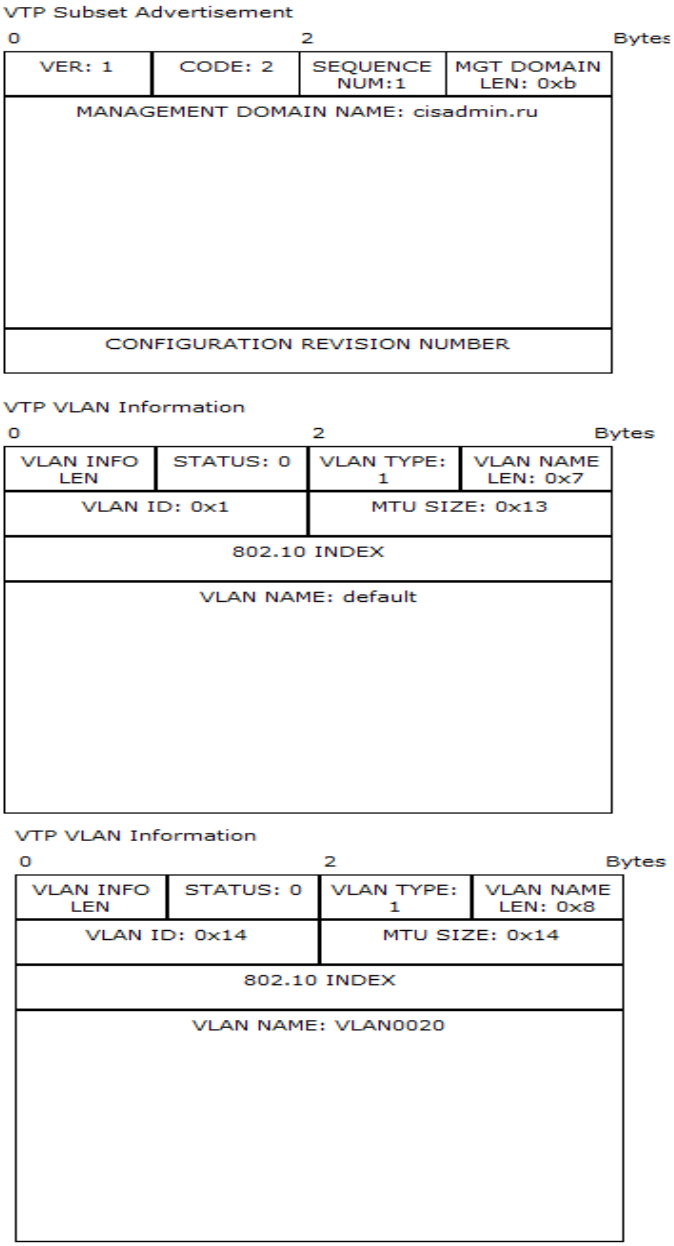


Рисунок 25 – Объявление Subset Advertisement»

3.2.3. Настройка каналов коммутации между VLAN

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.

Итак, мы создали множество VLAN, но ни одно устройство пока что не относится ни к одному из них. Для того чтобы отнести конечные устройства к определенному VLAN, необходимо настроить acces-порты коммутаторов.

Сделать это можно в консоли коммутатора с помощью команд

Prosv-asw1(config)#int range fa0/1-2
Prosv-asw1(config-if-range)#switchport mode access
Prosv-asw1(config-if-range)#switchport access vlan 101

После настройки access-портов согласно таблице на рисунке 17 при наведении курсора мышкой на коммутатор мы увидим номера VLAN напротив каждого настроенного порта (рис. 26).

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	101	--	0009.7C52.3101
FastEthernet0/2	Up	101	--	0009.7C52.3102
FastEthernet0/3	Up	102	--	0009.7C52.3103
FastEthernet0/4	Up	102	--	0009.7C52.3104
FastEthernet0/5	Up	103	--	0009.7C52.3105
FastEthernet0/6	Up	103	--	0009.7C52.3106
FastEthernet0/7	Up	104	--	0009.7C52.3107
FastEthernet0/8	Up	104	--	0009.7C52.3108
FastEthernet0/9	Up	105	--	0009.7C52.3109
FastEthernet0/10	Up	105	--	0009.7C52.310A
FastEthernet0/11	Up	106	--	0009.7C52.310B
FastEthernet0/12	Up	106	--	0009.7C52.310C
FastEthernet0/13	Down	1	--	0009.7C52.310D
FastEthernet0/14	Down	1	--	0009.7C52.310E

Рисунок 26 – Информация о access-портах, полученная при наведении курсора мышкой на коммутатор prosv-asw1

Настройка trunk-портов похожа на настройку access-портов, с тем лишь различием, что мы можем выбрать множество VLAN, трафик которых будет способен пройти по этому порту. Trunk-порты коммутаторов prosv-asw1, pioner-asw1 и komend-asw1 должны пропускать VLAN 2, 101, 102, 103, 104, 105 и 106. В trunk-портах коммутатора prosv-dsw1 к этим VLAN добавляется еще и 3-й, так как в этой локальной сети также присутствует серверная ферма. Коммутатор prosv-asw2, расположенный в серверной ферме, должен пропускать только VLAN 2 и 3. Настроить trunk-порты можно в консоли коммутатора с помощью команд:

Prosv-dsw1(config)#int fa0/24
Prosv-dsw1(config-if)#switchport mode trunk
Prosv-dsw1(config-if)#switchport trunk allowed vlan 2,3,101-106

В IP-плане (рис. 16) мы также задали IP-адреса для коммутаторов и маршрутизаторов. Все коммутаторы мы определили в VLAN 2, и именно в этом интерфейсе прописывается IP-адрес, с помощью командной строки:

Prosv-asw1(config)#interface vlan 2
Prosv-asw1(config-if)# ip address 192.168.19.11 255.255.255.248

Под IP-адресами для маршрутизаторов подразумевалась выделенная сеть для связи Point-to-Point, то есть те адреса, по которым маршрутизаторы могли бы обращаться друг к другу. Так как единственная линия связи, соединяющая два маршрутизатора, обязательно проходит через симулятор провайдера, IP-адреса сети для связи Point-to-Point прописываем в портах, соединяющих маршрутизатор с коммутатором “Provider”. Однако мы также указали, что все

маршрутизаторы и коммутаторы принадлежат второму VLAN, поэтому IP-адрес необходимо писать в сабинтерфейсе порта, в котором командой encapsulation можно указать, какой именно трафик будет принимать этот сабинтерфейс:

Prosv-gw1(config)#interface fa 0/0.2

Prosv-gw1(config-subif)#encapsulation dot1q 2

Prosv-gw1(sonfig-subif)#description Management

Prosv-gw1(config-subif)#ip address 192.168.19.2 255.255.255.248

Настраиваем все порты симулятора провайдера как trunk, пропускающие только трафик VLAN 2, проверяем связь между любыми двумя маршрутизаторами в режиме симуляции (рис. 27). Сообщение “Succesfull” говорит о том, что связь есть.

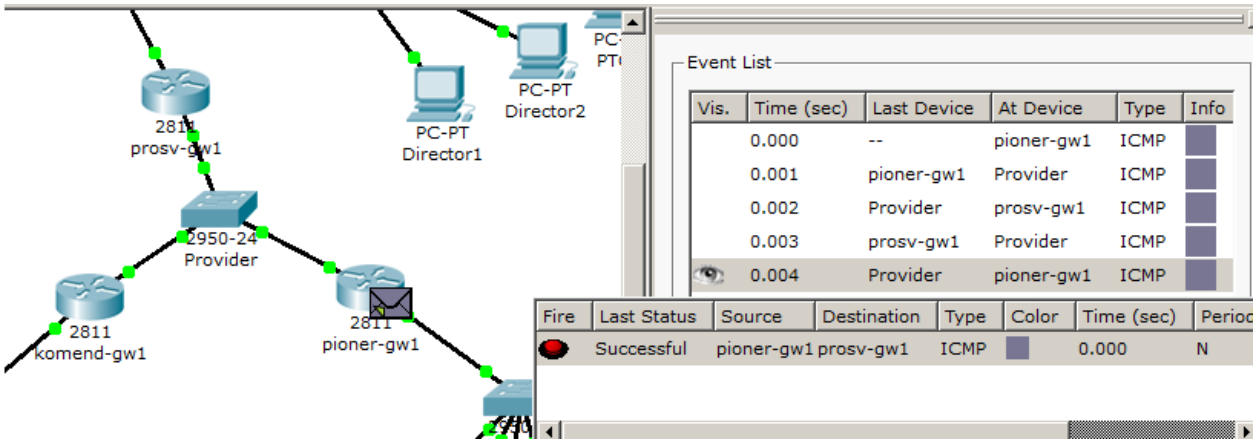


Рисунок 27 – Проверка связи pioner-gw1 с prosv-gw1

Последним штрихом настройки маршрутизаций внутри локальных сетей является настройка сабинтерфейсов портов маршрутизаторов внутри локальных сетей. В качестве IP-адресов этих сабинтерфейсов должны выступать шлюзы соответствующих подсетей. Эти же самые шлюзы мы присваивали конечным устройствам:

Prosv-gw1(config)#interface fa 0/1.101

Prosv-gw1(config-subif)#encapsulation dot1q 101

Prosv-gw1(sonfig-subif)#description Directors

Prosv-gw1(config-subif)#ip address 192.168.19.41 255.255.255.248

После настройки сабинтерфейсов, их можно просмотреть, наведя мышку на маршрутизатор (рис. 28).

```
Port                Link   VLAN   IP Address         IPv6 Address                              MAC Address
FastEthernet0/0     Up     --     <not set>          <not set>                                 0090.21E8.E401
FastEthernet0/0.2   Up     --     192.168.19.2/29    <not set>                                 0090.21E8.E401
FastEthernet0/1     Up     --     <not set>          <not set>                                 0090.21E8.E402
FastEthernet0/1.2   Up     --     192.168.19.9/29    <not set>                                 0090.21E8.E402
FastEthernet0/1.3   Up     --     192.168.19.33/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.101 Up     --     192.168.19.41/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.102 Up     --     192.168.19.49/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.103 Up     --     192.168.19.57/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.104 Up     --     192.168.19.65/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.105 Up     --     192.168.19.73/29   <not set>                                 0090.21E8.E402
FastEthernet0/1.106 Up     --     192.168.19.81/29   <not set>                                 0090.21E8.E402
Vlan1               Down   1      <not set>          <not set>                                 0001.9624.A399
Hostname: prosv-gw1

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 28 – Сабинтерфейсы маршрутизатора prosv-gw1

Проверим связь любых двух ПК в одной локальной сети (рис. 29).

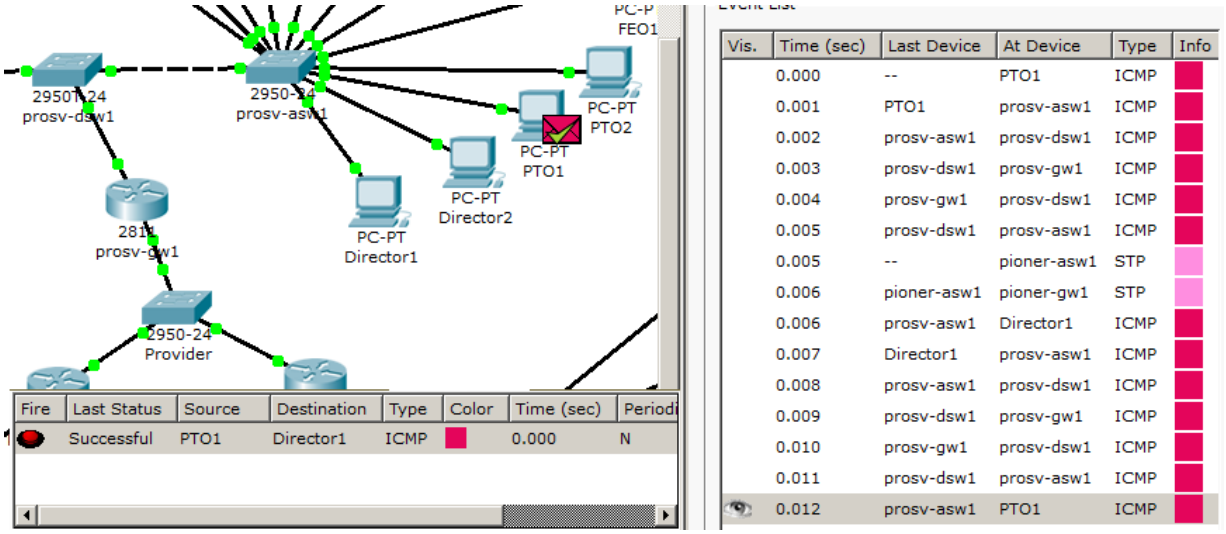


Рисунок 29 – Проверка связи между ПК PTO1 и Director1

И коммутатора с маршрутизатором (рис. 30).

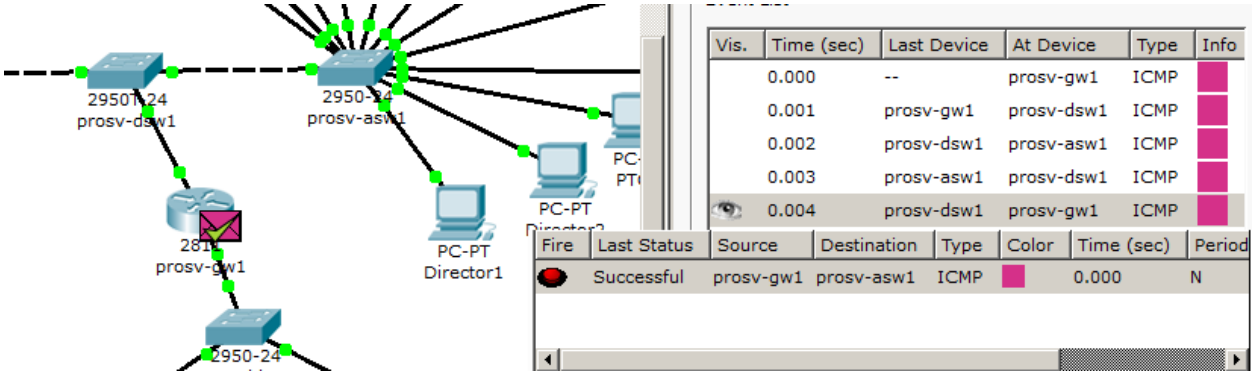


Рисунок 30 – Проверка связи между маршрутизатором prosv-gw1 и коммутатором prosv-asw1

Получив положительные результаты внутри каждой из локальных сетей, можно приступать к настройке маршрутизации между разными локальными сетями.

3.3. Настройка маршрутизации между сетями и настройка серверов

Маршруты к удаленным сетям могут быть сконфигурированы для каждого маршрутизатора вручную администратором (**статическая маршрутизация**) или созданы с помощью маршрутизирующих протоколов (**динамическая маршрутизация**).

Статические маршруты полностью определены администратором, поэтому они более **безопасны**, требуют **меньше вычислительных ресурсов** и **более узкую полосу пропускания,** по сравнению с динамическими маршрутами. Статические маршруты, по сравнению с динамическими, характеризуются более высоким приоритетом, поскольку административное расстояние **AD = 1**.

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, введённой 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 выборе 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.

Чтобы сконфигурировать статическую маршрутизацию, администратор должен задать маршруты ко всем возможным сетям назначения, которые не присоединены непосредственно к данному маршрутизатору. Для конфигурирования статической маршрутизации используется команда *ip route,* которая содержит три параметра:

- **адрес сети назначения**,
- **сетевую маску**,
- **адрес входного интерфейса следующего маршрутизатора** на пути к адресату (**next hop**) или **идентификатор выходного интерфейса**.

Адрес входного интерфейса следующего маршрутизатора (следующего перехода) на пути к адресату иногда называют шлюзом.

3.3.1. Настройка статической маршрутизации

В предыдущих разделах была произведена настройка связи внутри каждой из локальных сетей, однако связь между двумя разными LAN пока отсутствует. Происходит это, потому что маршрутизаторы, получив пакет, предназначенный для другой локальной сети, не знают, куда его посылать. Известные маршрутизатору адреса (таблицу маршрутизации) можно посмотреть командой

Prosv-gw1#sh ip route

Для примера настроим связь между ПК Director5, находящемся в офисе на «Комендантском» с ПК Other4, который находится в офисе на «Пионерской». Необходимые для настройки статической маршрутизации между этими двумя ПК данными представлены на рисунке 31.

IP адреса	Принадлежат	Шлюз	Номер подсети
192.168.19.3	pioner-gw1	192.168.19.1	192.168.19.0
192.168.19.4	komend-gw1		
192.168.19.131	Other4	192.168.19.129	192.168.19.128
192.168.19.138	Director5	192.168.19.137	192.168.19.136

Рисунок 31 – Данные для статической маршрутизации между Director5 и Other4

Пакет с ПК Director5 должен дойти до маршрутизатора komend-gw1, после чего быть отправлен в маршрутизатор pioneer-gw1, который направит его к ПК Other4, и вернуться по тому же маршруту обратно к ПК Director5.

Смысл прост – заставить маршрутизатор komend-gw1 переслать трафик, предназначенный для сети с адресом 192.168.19.128 (в этой сети находится ПК Other4) через маршрутизатор pioner-gw1, которому мы прописали «внешний» IP-адрес 192.168.19.3. После чего по аналогии настроить маршрутизатор pioner-gw1, который должен отправить трафик, предназначенный для сети с адресом 192.168.19.136 на «внешний» порт маршрутизатора komend-gw1, имеющий адрес 192.168.19.4.

Для реализации этого в консоли роутера прописывают команду

Router(config)#ip route [Network] [Mask] [Next hop]

Поле Network предназначено для адреса сети, Mask – для маски подсети, а Next hop – для адреса, на который маршрутизатору следует отправить трафик, предназначенный для сети с адресом, указанным в поле Network. В нашем случае, команды будут выглядеть так:

Pioner-gw1(config)#ip route 192.168.19.137 255.255.255.248 192.168.19.4
Komend-gw1(config)#ip route 192.168.19.128 255.255.255.248 192.168.19.3

Посмотреть настройки статической маршрутизации можно во вкладке “Config” в меню “Static” (рис. 32) или с помощью команды: *show ip route.*

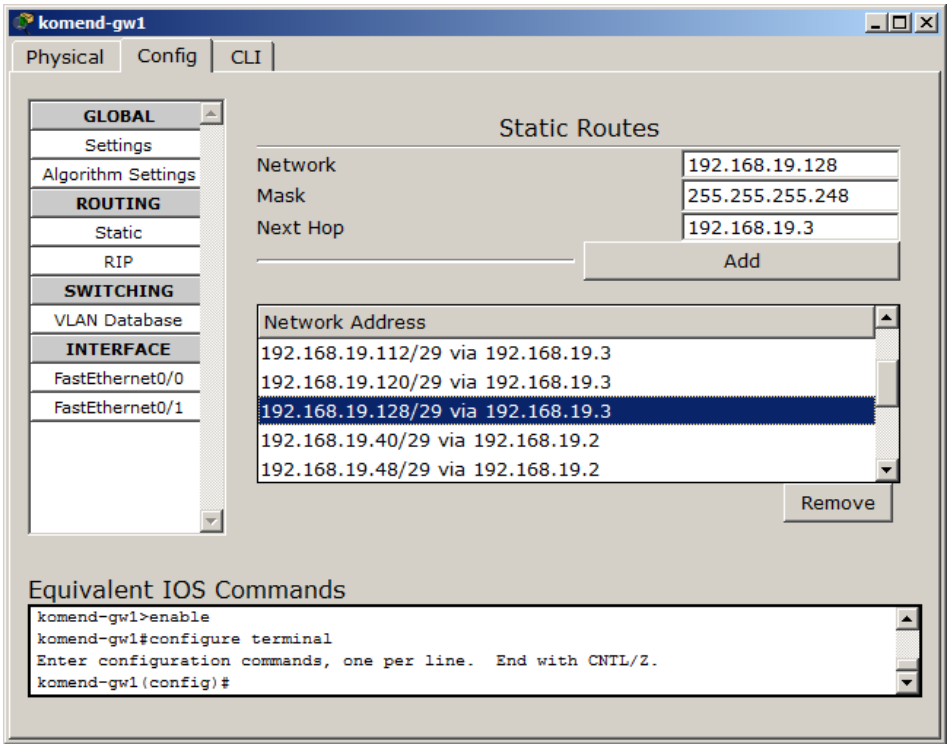


Рисунок 32 – Настройка статической маршрутизации в komend-gw1

После настройки проверим связь между ПК Director5 и Other4 (рис. 33) и по аналогии настроим статическую маршрутизацию между всеми остальными узлами сети.

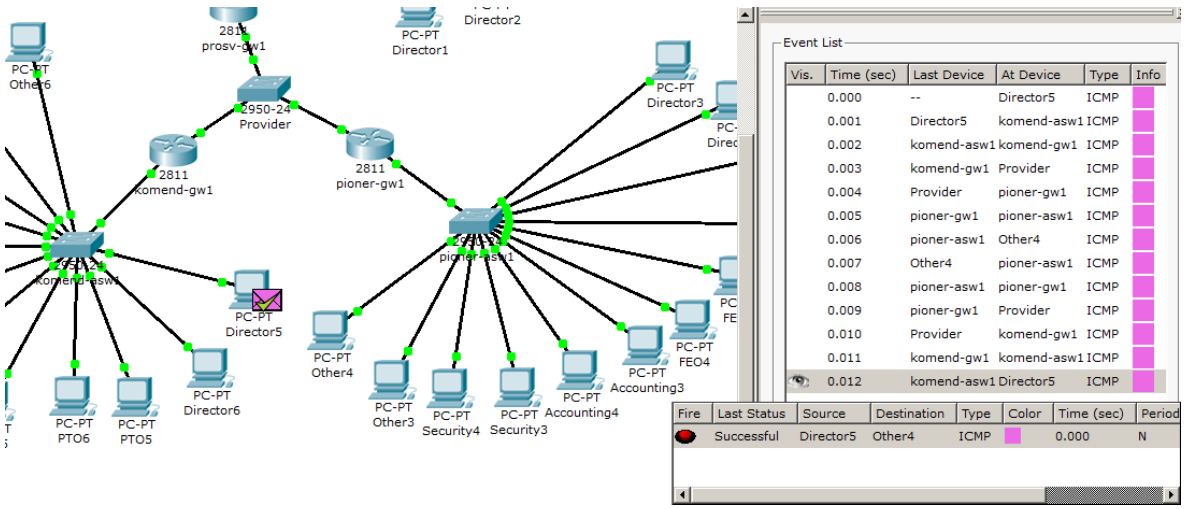


Рисунок 33 – Проверка связи между ПК Director5 и Other4

Настройка статической маршрутизации занимает много времени и создает гигантское пространство для ошибок, однако уменьшает количество трафика по сравнению с динамической маршрутизацией.

3.3.2. 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.

3.3.2.1. Настройка WEB-сервера

Для создания HTTP-сервера перейдём на вкладку “Config”, выберем меню “HTTP” и настроим страницу сайта, который будет открываться у пользователей ПК (рис. 34).

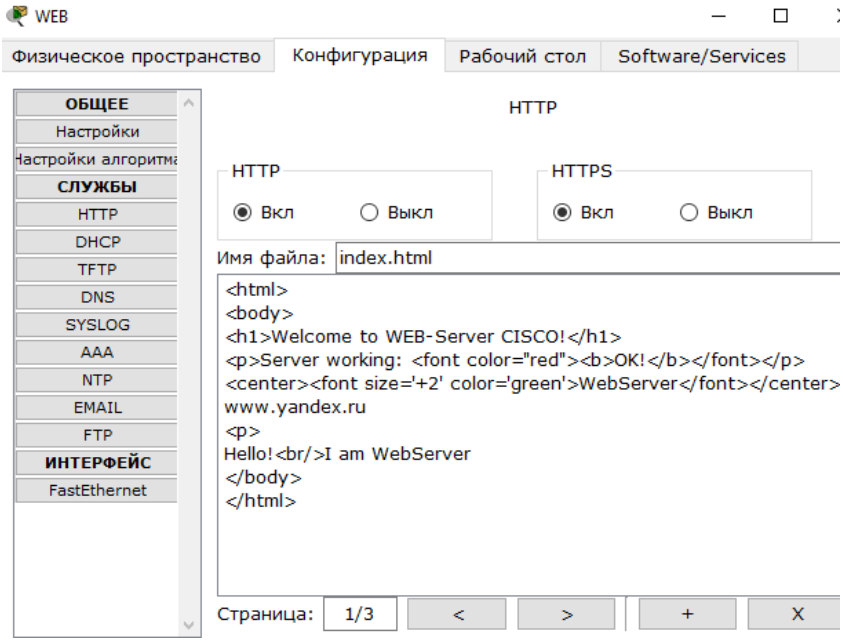


Рисунок 34 – Настройка HTTP-сервера

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. 35).

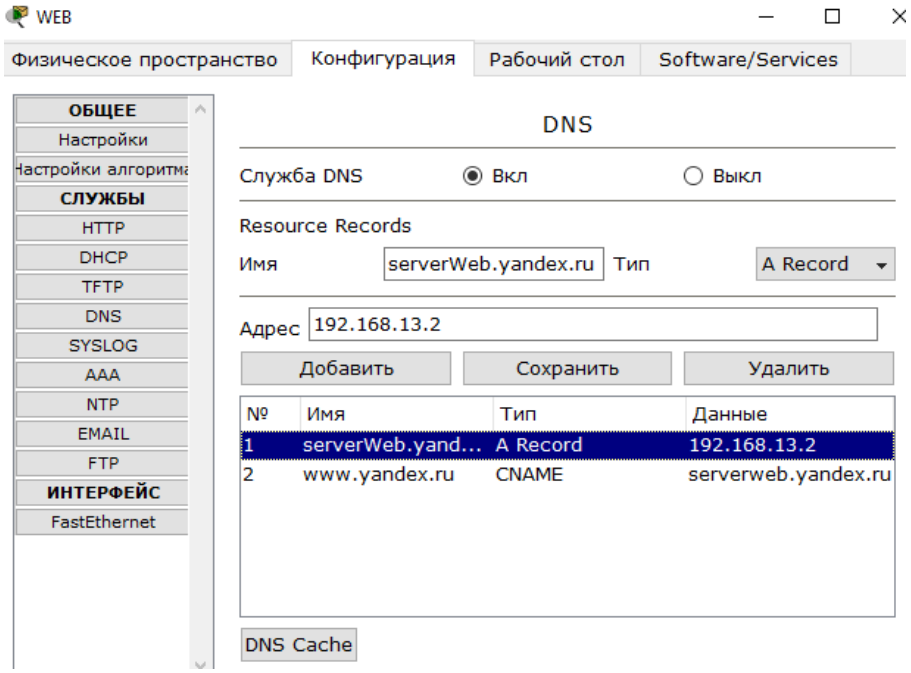


Рисунок 35 – Настройка функции DNS-сервера

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. 36).

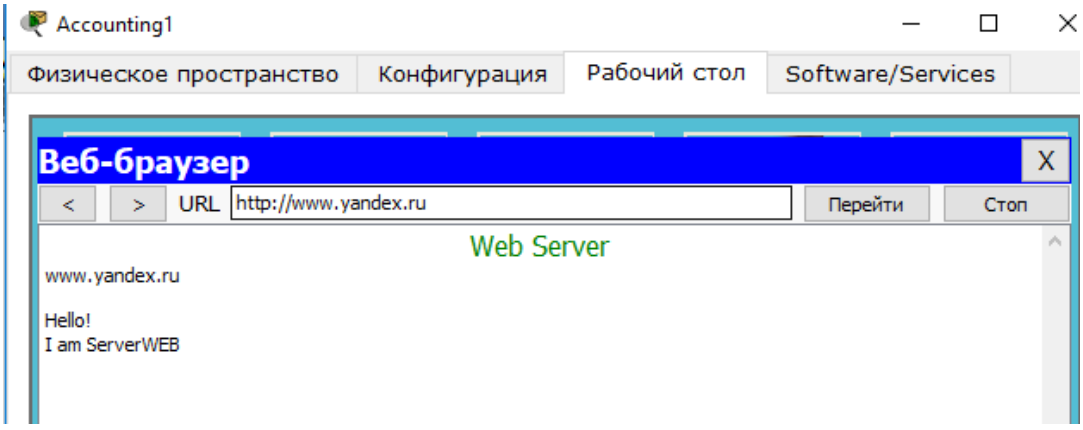


Рисунок 36 – Текст web-страницы

3.3.2.2. Настройка службы DHCP на WEB-сервере

Войдем в конфигурацию и на вкладке DHCP настроем службу. Для этого наберем новые значения пула, установим переключатель On и нажмем на кнопку Save (Сохранить) – рисунок 37.

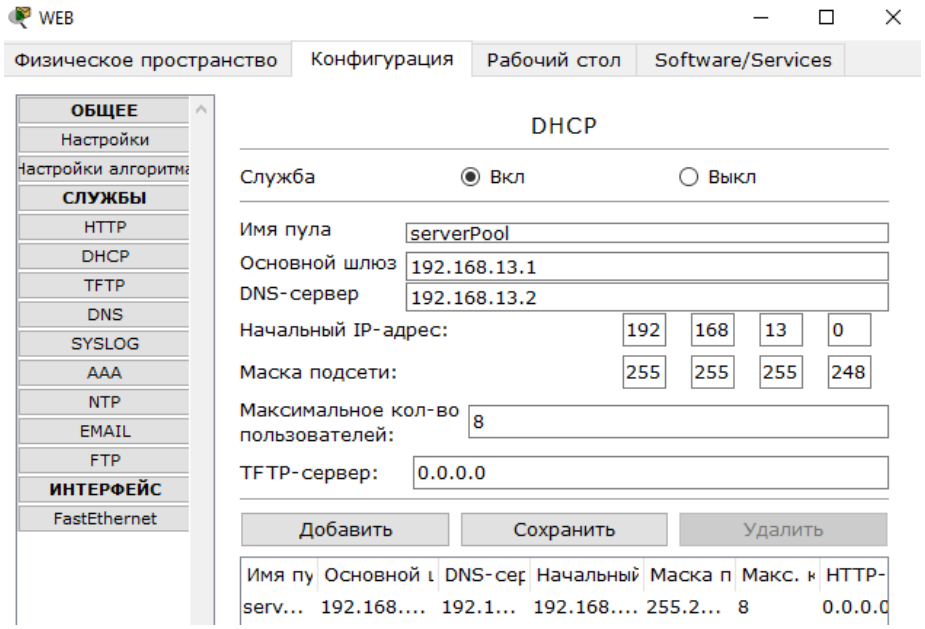


Рисунок 37 – Настройка DHCP-сервера

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. 38).

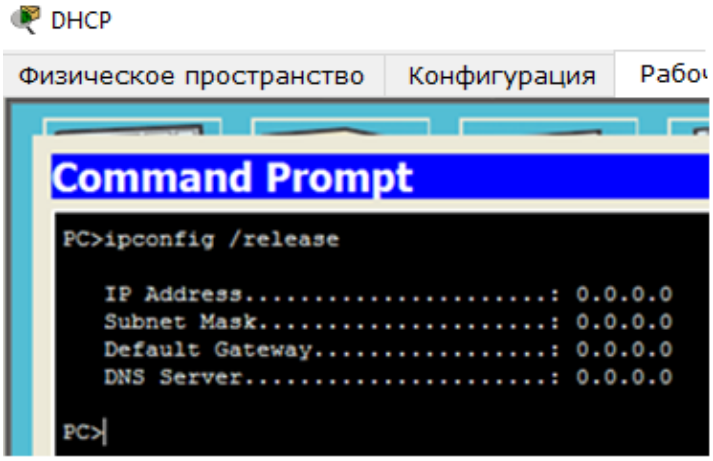


Рисунок 38 – Удаление конфигурации IP-адресов для всех адаптеров

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. 39).

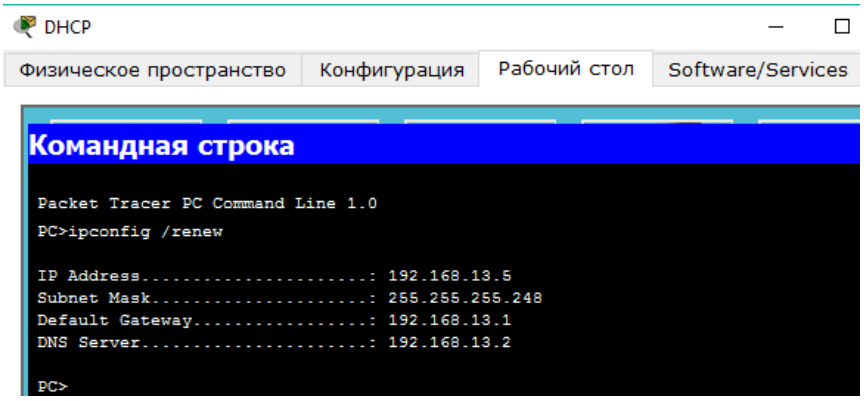


Рисунок 39 – Конфигурация протокола TCP/IP клиента от DHCP сервера

Теперь проверим работу WEB-сервера, открыв сайт в браузере на DHCP (рис. 40) и убедимся, что служба работает.

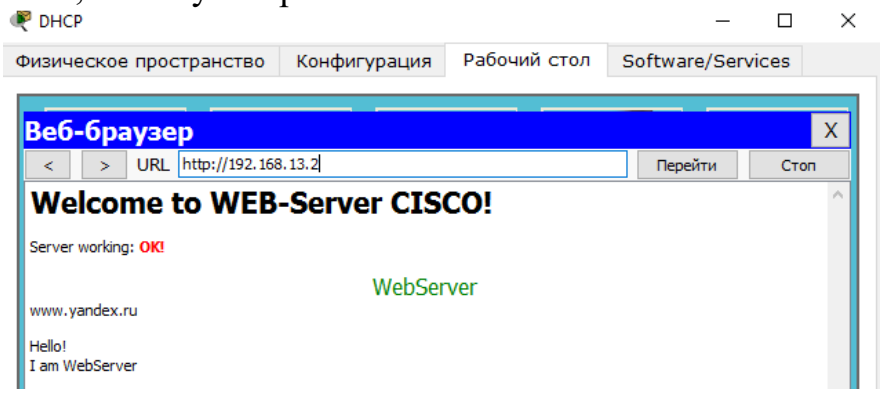


Рисунок 40 – Проверка работы службы HTTP на DHCP

ЗАКЛЮЧЕНИЕ

В рамках данной работы были подготовлены методические указания для выполнения курсового проекта по дисциплине «Сетевые технологии» 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

1. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – СПб., 2019. – 960 с. – Текст: непосредственный.
2. Олифер, В. Г. Компьютерные сети / В. Г. Олифер, И. А. Олифер. – СПб., 2020. – 992 с. – Текст: непосредственный.