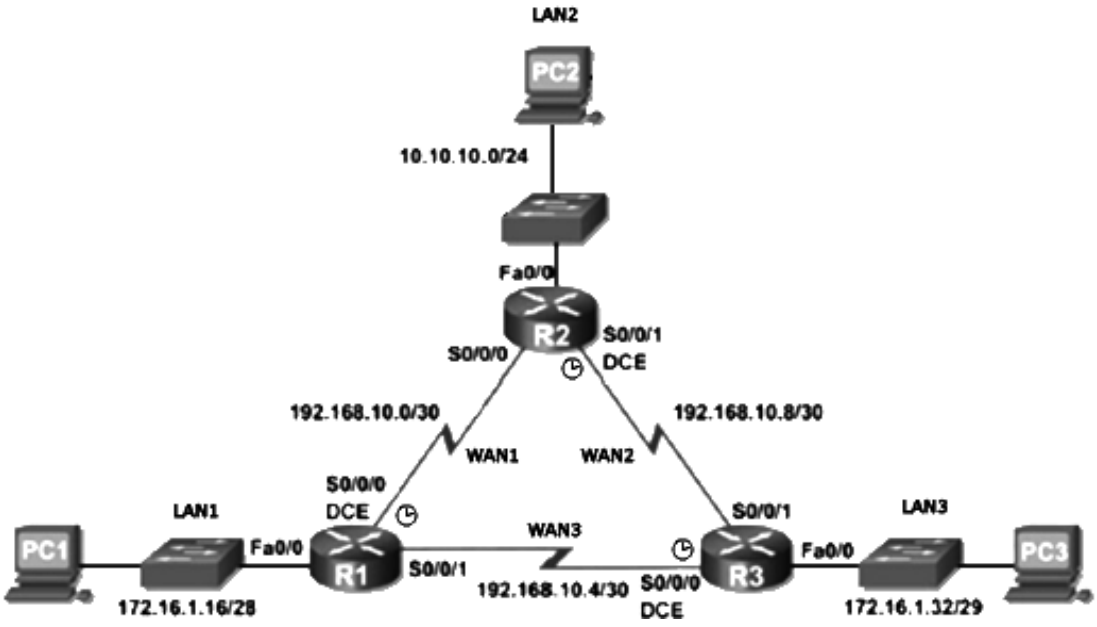
УНИВЕРСИТЕТ ИТМО

М.А. Плоткин, И.А. Шарков, И.Г. Дейнека

МЕТОДИЧЕСКОЕ РУКОВОДСТВО ДЛЯ ПРОВЕДЕНИЯ ЦИКЛА ЛАБОРАТОРНЫХ РАБОТ ПО КУРСУ «СЕТИ СВЯЗИ И СИСТЕМЫ КОММУТАЦИИ»



Санкт-Петербург
2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

М.А. Плоткин, И.А.Шарков, И.Г. Дейнека

МЕТОДИЧЕСКОЕ РУКОВОДСТВО ДЛЯ ПРОВЕДЕНИЯ ЦИКЛА ЛАБОРАТОРНЫХ РАБОТ ПО КУРСУ «СЕТИ СВЯЗИ И СИСТЕМЫ КОММУТАЦИИ»

Учебно-методическое пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2016

Плоткин М.А., Шарков И.А., Дейнека И.Г. Методическое руководство для проведения цикла лабораторных работ по курсу сети связи и системы коммутации. Учебно-методическое пособие – СПб: Университет ИТМО, 2016. – 90с.

Учебно-методическое пособие разработано в соответствии с программой курса «Сети связи и системы коммутации» Федерального государственного образовательного стандарта высшего образования для магистрантов по направлению подготовки 11.04.02. Инфокоммуникационные технологии и системы связи. В настоящее издание вошли практические работы, посвященные применению на практике знаний по настройке сетевого оборудования. Содержание работ включает в себя теоретическую и экспериментальную части.

Рекомендовано к печати Ученым советом факультета инфокоммуникационных технологий 22 апреля 2016 года, протокол №4/16.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Предисловие

Дисциплина «Сети связи и системы коммутации» была включена в учебный план Университета в 2002 году. В исходной программе курса основное внимание уделялось телефонной сети общего применения (ТФОП), использующей для передачи, в основном, волоконно-оптические линии связи (ВОЛС) и системы синхронной цифровой иерархии (СЦИ), а для коммутации – цифровые электронные АТС с коммутацией каналов (ЭАТС).

В 80-90х годах прошлого века наряду с предоставлением услуг телефонной связи, ТФОП служила основой для организации сетей для передачи различных видов дискретных (данные, телеграф) и аналоговых (телевидение, радиовещание) сигналов.

Созданные в то время стационарные и мобильные сети связи позволили принципиально решить важные задачи глобализации и персонализации телефонных услуг.

Наиболее перспективным направлением развития как телефонной, так и других сетей связи считалось создание «Интеллектуальной Сети» (ИС), позволяющей постоянно расширять набор сервисных возможностей, в основном, путем совершенствования программного обеспечения сетевых узлов. При этом более консервативные функции передачи сигналов и коммутации каналов должны были обеспечиваться оборудованием транспортной сети, использующей традиционный набор ВОЛС, СЦИ и ЭАТС.

Бурное развитие Интернета, первоначально скромно предложенного в качестве корпоративной цифровой сети для связи нескольких вычислительных центров, успехи полупроводниковой электроники и вычислительной техники, развитие информационных технологий, наконец, рост прогизводительности персональных компьютеров и повышение возможностей абонентских устройств мобильных сетей, – все это радикально изменило структуру современных сетей связи и пути их дальнейшего совершенствования.

В течение одного десятилетия задачи традиционных транспортных сетей трансформировались в исполнение функций только нижнего физического уровня модели взаимодействия открытых систем (OSI[1]). В современных сетях функции канального и сетевого уровней модели OSI обеспечиваются коммуникационными устройствами Интернета (коммутаторами и маршрутизаторами), а функции более высоких уровней, реализующих быстро изменяющиеся программно-информационные приложения, выполняются интеллектуальным оборудованием конечных пользователей сети, как правило, персональными компьютерами.

Практически все основные системные характеристики современной многофункциональной сети связи определяются параметрами устройств Интернета.

Принципиальные решения Интернета – передача всех видов сигналов в форме цифровых пакетов, единая глобальная система адресации, совмещающаяся с автономным управлением отдельными подсетями, распределенная маршрутизация и возможность организации альтернативных маршрутов, обеспечение гарантированного качества обслуживания (QoS[2]), соответствующего специфике передаваемого сигнала – все это значительно повысило надежность, пропускную способность и функциональность действующих сетей связи.

---

[1] Сетевая модель OSI (англ. open systems interconnection basic reference model — базовая эталонная модель взаимодействия открытых систем) — сетевая модель стека сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99).

[2] QoS (англ. quality of service — качество обслуживания) — этим термином в области компьютерных сетей называют вероятность того, что сеть связи соответствует заданному соглашению о трафике, или же, в ряде случаев, неформальное обозначение вероятности прохождения пакета между двумя точками сети.

Отметим, что в сети связи, построенной на основе интернет-технологий, произошло отделение транспортной инфраструктуры сети связи от программно-управляемых аппаратных комплексов, как это предполагалось в интеллектуальной сети. Однако в интернет-сетях основные сервисные возможности определяются программным обеспечением оконечных станций (серверов и ПК пользователей), а не сетевых узлов.

Радикальные преобразования принципов организации современных телекоммуникационных сетей нашли отражение в изменении содержания курса «Сети связи и системы коммутации».

Начиная с 2012 года, основное внимание было направлено на изучение принципов построения локальных и глобальных компьютерных сетей, характеристик и особенностей работы различных типов коммуникационных сетевых устройств, методов организации глобальной многофункциональной телекоммуникационной сети на базе технологии Интернет.

Многоплановость содержания исходного курса ограничивала возможности организации практических занятий, которые сводились к выполнению индивидуальных расчетных заданий.

Проведенная консолидация тематики курса позволила в пределах учебного плана, наряду с выполнением определенного объема расчетных задач, организовать цикл лабораторных работ по современным сетям связи, основывающихся на Интернет-технологиях.

В данном учебном пособии представлены методические руководства по проведению шести лабораторных работ.

Выполнение каждой работы предполагает решение комплекса задач в ходе аудиторных занятий, подготовку домашнего задания, составление и защиту отчета.

Проведение цикла лабораторных работ должно помочь слушателям закрепить теоретические знания принципов организации корпоративных и глобальных сетей связи, приобрести практические навыки по построению компьютерных сетей и познакомиться с особенностями функционирования и эксплуатации современного коммуникационного сетевого оборудования.

Лабораторная работа №1.
Исследование пропускной способности локальных компьютерных сетей с различной логической структурой

1. Введение

Наиболее распространенной современной сетевой технологией для организации локальных вычислительных сетей (ЛВС или LAN – Local Area Network) является Ethernet, обеспечивающая наибольшую простоту протоколов работы и управления сетью, низкую стоимость коммуникационных устройств и широкие возможности оперативного наращивания числа рабочих станций.

Принципиальной особенностью данной технологии является случайный доступ к общей разделяемой среде. Такой метод доступа обеспечивает предельную простоту алгоритма работы сети, однако при повышении нагрузки на сеть возрастает количество возникающих коллизий, вызывающих необходимость повторной передачи кадров, что в итоге приводит к увеличению задержки передаваемых сигналов и ограничивает величину передаваемого сетевого трафика до (30-40)% от номинальной пропускной способности.

Единая разделяемая среда, соответствующая логической «общей шине», формируется в сети, сегменты которой объединяются повторителями или мультиплексорами. При этом в

сети одновременно могут передаваться сигналы лишь одной рабочей станции, то есть образуется ***общесетевой домен коллизий***. Это не адекватно условиям работы разветвленных локальных сетей, состоящих из нескольких сегментов, у которых значительная часть генерируемого трафика, как правило, замыкается внутри собственного сегмента.

Пропускная способность сети может быть повышена с помощью логической структуризации, разделяющей всю сеть на несколько доменов коллизий при помощи мостов, коммутаторов или маршрутизаторов.

В данной работе исследуется передача трафика в локальной вычислительной сети с единой разделяемой средой и в сети с логической структуризацией.

Исследование проводится с помощью пакета программ Cisco Packet Tracer, позволяющего эмулировать процессы, происходящие в компьютерных сетях при передаче информационного трафика.

2. Эмулятор компьютерных сетей Cisco Packet Tracer

Cisco Packet Tracer (CPT) - это пакет программ для эмуляции работы компьютерных сетей, разработанный компанией Cisco. 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 Cisco серии 2950, 2960, 3650, маршрутизаторов 1800, 2600, 2800, серверов DHCP, HTTP, TFTP, FTP, рабочих станций, предоставляет возможности установки различных модулей расширения в компьютеры, коммутаторы и маршрутизаторы.

Пакет программ позволяет создавать макеты компьютерных сетей довольно сложных топологий, проверять работоспособность и проводить исследования сетей.

2.1. Основные возможности Cisco Packet Tracer

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 (коммутаторы, маршрутизаторы, точки доступа), оконечные устройства (сервера, рабочие станции, телефонные аппараты) и линии связи (оптоволоконный кабель, витая пара, коаксиальный кабель, радиолинии).
- Настройка активного оборудования через консоль (клавиатуру) по интерфейсу командной строки CLI (Command Line Interface) 3 - методом, реально используемым 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.

[3] Интерфейс командной строки (Command Line Interface или CLI) – средство взаимодействия с компьютерной программой, когда пользователь формирует команды в форме текстовых строк (команд).

- Эмуляция включения и настройки различных сервисов в рабочих станциях (почта, веб, 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);

Для более полного представления о возможностях эмулятора необходимо подробней изучить функционал Cisco Packet Tracer.

2.2. Графический интерфейс Cisco Packet Tracer

Запустите эмулятор Cisco Packet Tracer.

Основная работа выполняется в главном окне программы, представляющей весьма удобный графический интерфейс (рис. 1.1).

Наименования и функции для основных полей главного окна Cisco Packet Tracer, соответствующие нумерации рис.1.1, приведены ниже.

1. Главное меню содержит стандартные для многих программ пункты: Файл, Правка, Настройки, Вид, Инструменты, Расширения, Помощь. Особого внимания заслуживает пункт «Расширения», содержащий мастер проектов, многопользовательский режим и ряд других дополнительных возможностей, которые с помощью CPT могут сформировать целую лабораторию.
2. Панель инструментов, часть которых просто дублирует пункты главного меню.
3. Переключатель логической и физической организации рабочего пространства.
4. Панель инструментов, содержащая средства выделения, удаления, перемещения, масштабирования объектов, а также формирования и передачи пакетов данных (PDU[4]) между устройствами.
5. Переключатель режима реального времени (Realtime) и режима имитации (Simulation Mode).
6. Панель выбора группы коммуникационных устройств, оконечных станций и линий связи.
7. Панель, содержащая конкретные типы коммуникационных устройств (маршрутизаторов, коммутаторов, концентраторов), оконечных устройств и линий связи. Содержимое этой панели зависит от выбранной группы устройств в пункте выше. Используя символические обозначения конкретных устройств, можно, как из кубиков LEGO, собрать логическую схему сети, перенося символ методом Drag and Drop в рабочее пространство.
8. Панель создания пользовательских сценариев.
9. Рабочее пространство.

[4] Protocol Data Unit (PDU) — обобщённое название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент и т. д. Примеры названий некоторых пакетов: LACPDU, OAMPDU, BPDU,OSSPDU.

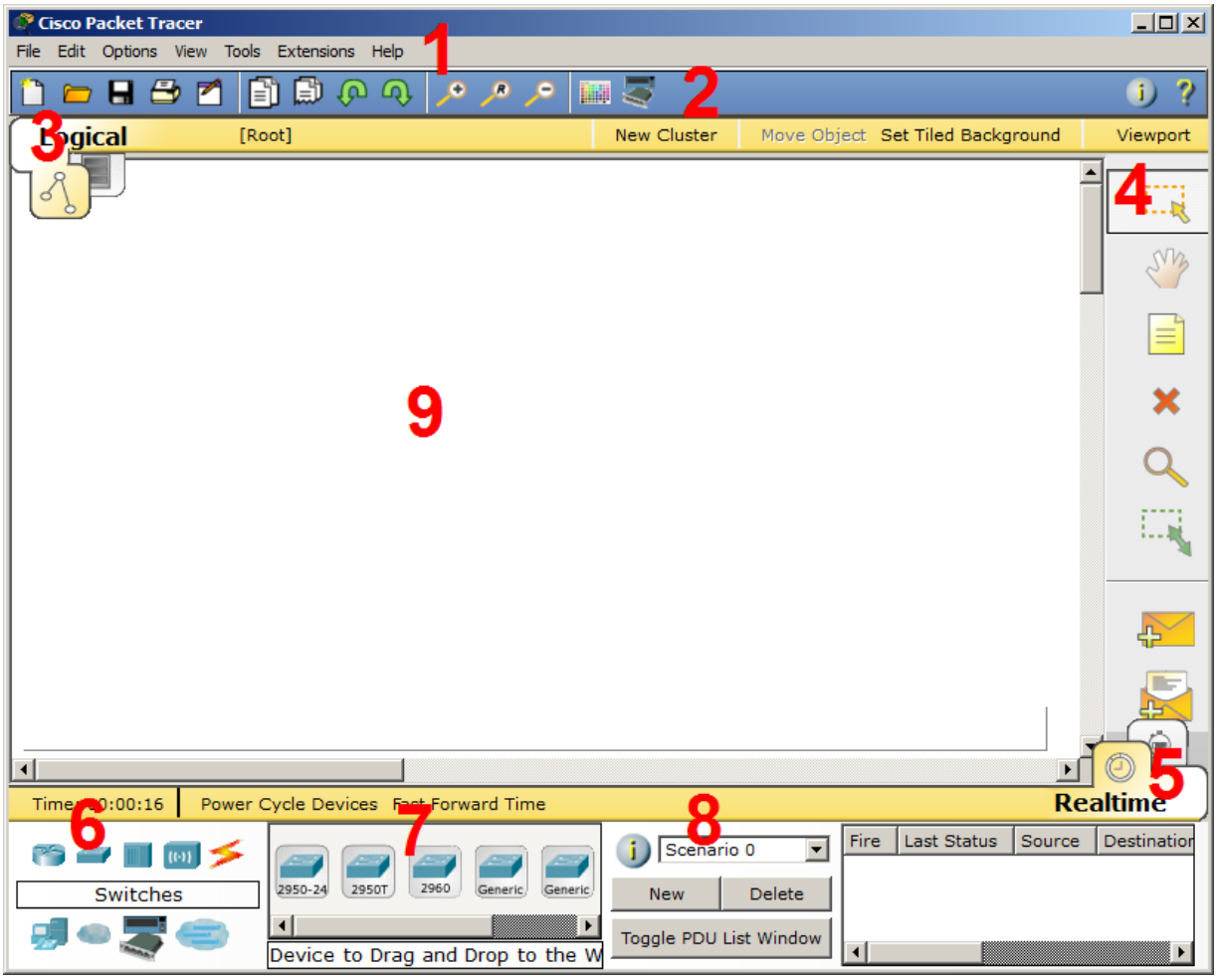


Рис. 1.1. Главное окно программы Cisco Packet Tracer

Дополнительные возможности Cisco Packet Tracer будет представлены в ходе решения практических задач.

2.3. Создание сети с общей разделяемой средой в Cisco Packet Tracer

В качестве исходной структуры построим сеть с общим доступом, объединяющую восемь оконечных станций при помощи четырех абонентских и одного корневого концентратора.

2.4. Выбор коммуникационных устройств и настройка аппаратной конфигурации

В панели «Выбор группы устройств» [6] выберите группу «Концентраторы» (Рис. 2).

Рис. 1.2. Панель выбора устройств – концентраторы

В панели «Выбор конкретных устройств» [7] выберите устройство Hub-PT и переместите его с панели устройств на рабочую область (Рис. 1.3).

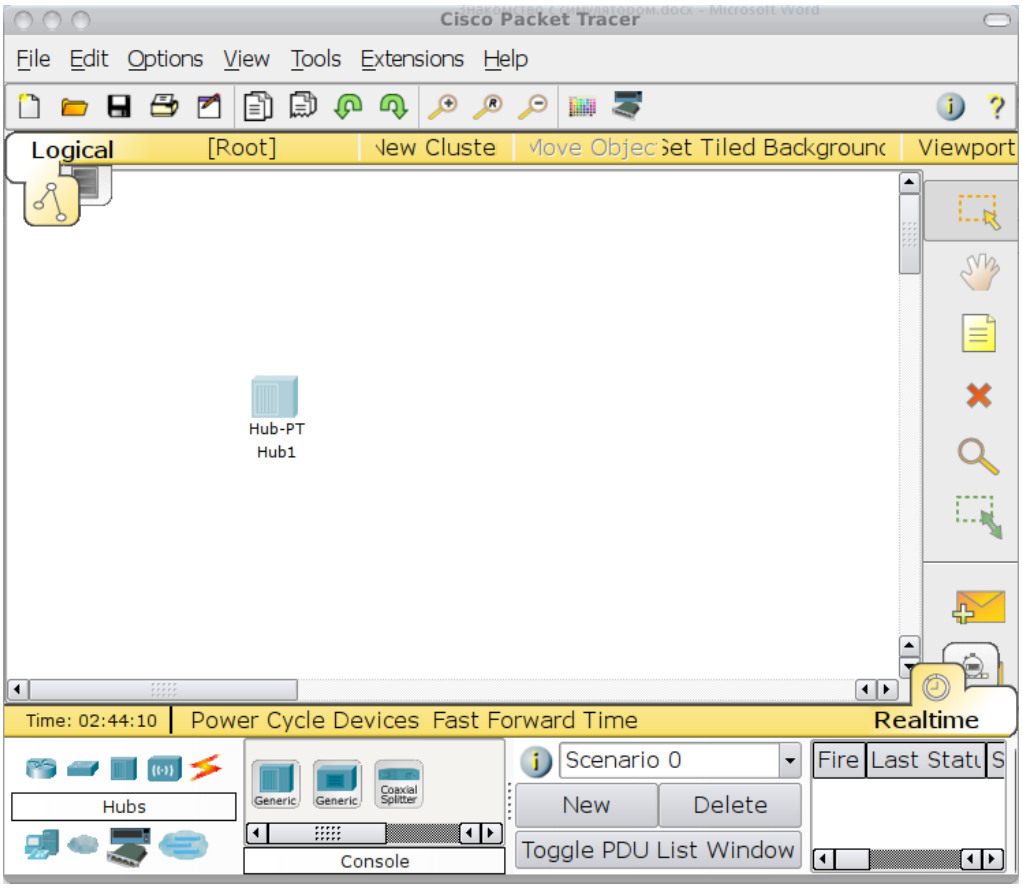


Рис. 1.3. Концентратор, размещенный в логическом рабочем пространстве

Одинарным щелчком мыши на пиктограмме концентратора откройте окно настройки выбранного оборудования (Рис. 1.4).

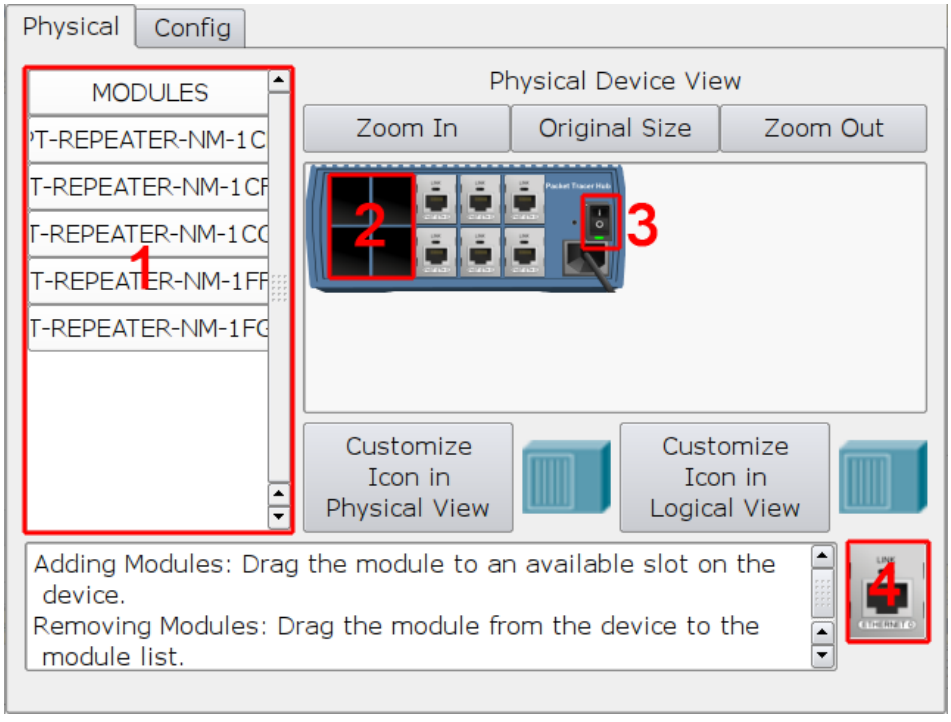


Рис. 1.4. Окно комплектации оборудования

Вкладка “Physical” позволяет управлять аппаратной конфигурацией выбранного устройства и показывает его внешний вид. Слева расположен список модулей [1], которыми можно укомплектовать данный концентратор. При выборе модуля из списка внизу экрана появляется краткое описание модуля и его изображение [4]. Эти модули можно установить в четыре свободных порта [2]. Разумеется, как и в настоящем оборудовании, установка новых модулей должна производиться при выключенном питании. Выключите устройство, нажав на тумблер питания [3].

Слева в списке выберите PT-REPEATER-NM-1CFE (второй в списке). Модуль PT-REPEATER-NM-1CFE обеспечивает один интерфейс Fast Ethernet для работы по медным парам. Переместите его название в один из свободных портов. Включите питание концентратора [3].

Аналогичным образом разместите еще четыре концентратора в логическом рабочем пространстве (рис. 1.5).

> Т.к. в Cisco Packet Tracer используются не реальные сетевые устройства, а их упрощенные модели, полученные в данной работе результаты могут значительно отличаться от реальных. Для того, чтобы данные моделирования были более корректными, необходимо, чтобы Cisco Packet Tracer учитывал длину линий связи. Для этого в главном меню приложения выберите Options->Preferences. В открывшемся окне поставьте галочку напротив пункта “Enable Cable Length Effects”.

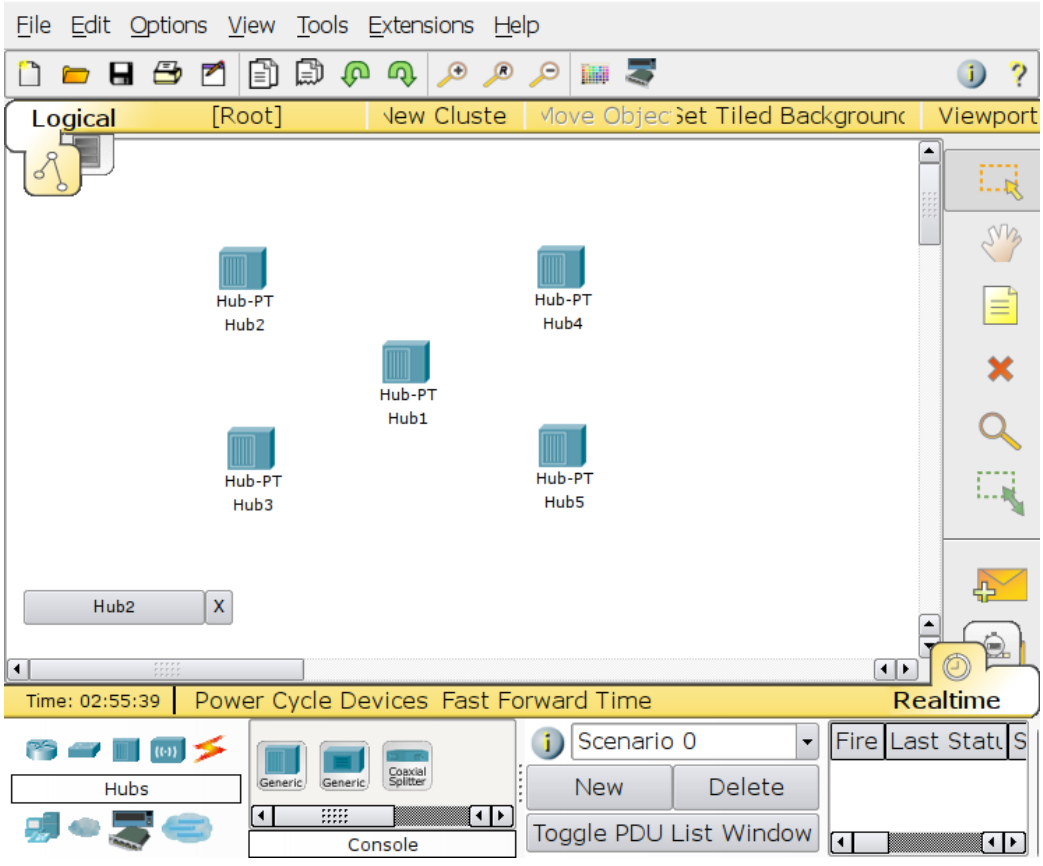


Рис. 1.5. Размещение концентраторов в рабочей области CPT

2.5. Соединение коммуникационных устройств линиями связи

Перейдите в группу “линии связи”. Выберите перекрёстный кабель (Copper Cross-Over) и соедините концентраторы между собой. При соединении Cisco Packet Tracer попросит указать порты, к которым этот кабель будет подключен (Рис. 1.6).

При подключении друг к другу коммуникационных устройств (концентраторы, коммутаторы, маршрутизаторы) принято использовать, по возможности, свободные порты с как можно большими номерами (Port9, Port8, … , Port0), а при подключении абонентских устройств (компьютеры, IP-телефоны и т.д.) – порты с меньшими номерами (Port0, Port1, …).

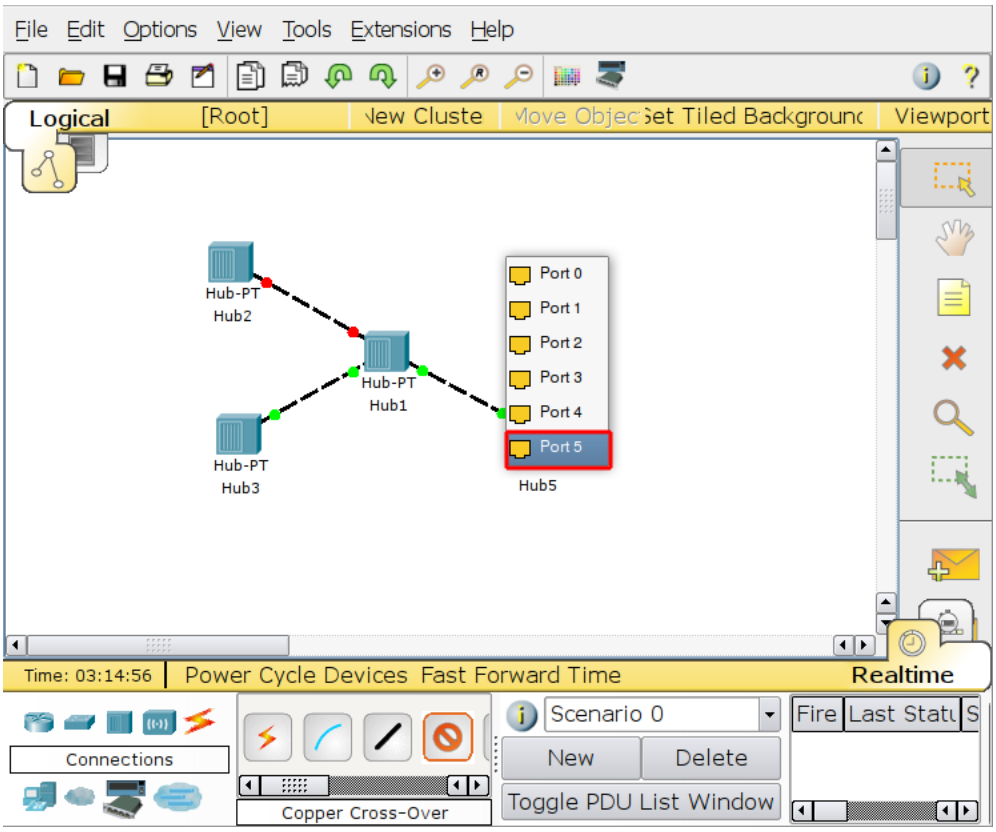


Рис. 1.6. Соединение концентраторов линиями связи

После подключения соединительного кабеля к концентраторам производится определение статуса порта (физический уровень) и состояния соединения (канальный уровень).

Изменение статуса порта и соединения обычно сопровождается изменением светового индикатора (цветовая индикация зависит от производителя и типа оборудования).

В СТР для отображения статуса порта и состояния соединения используются круглые маркеры, расположенные на концах линий связи. Маркеры могут иметь несколько состояний, обозначаемых различными цветами (Таблица 1.1).

Таблица 1.1

Красный	Порт находится в состоянии Down (отключено). На физическом уровне не обнаружено каких-либо сигналов, обладающих признаками используемого протокола.
Зеленый	Порт находится в состоянии Up (подключено), т.е. на физическом уровне обнаружен используемый протокол. Но это состояние ничего не говорит о статусе канального уровня.
Мигающий зеленый	Активность на канальном уровне. Частота мигания зависит от количества пакетов, передаваемых в единицу времени.

Оранжевый	Порт находится в режиме блокировки канального уровня, идет процесс обнаружения возможных сетевых петель. Данное состояние может наблюдаться только на коммутаторах.

Убедитесь, что все используемые порты концентраторов находятся в состоянии “Up”.

2.5.1. Выбор и настройка оконечных устройств

Перейдите в группу “Оконечные устройства” и перетащите в область рабочего пространства компьютер. Для удобства дальнейшей работы переименуйте компьютер PC0 в PC1. Для этого щелкните мышкой на названии компьютера и введите новое название.

Установите семь компьютеров PC2, PC3,….PC8.

Соедините порты концентраторов Port 0 и Port 1 прямым кабелем (copper straight-through) с портами Fast Ethernet компьютеров, как показано на рис. 1.7. Для этого для каждого компьютера проделайте следующие операции:

- выберите прямой патчкорд;
- наведите курсор на пиктограмму компьютера и выберите порт “Fast Ethernet”;
- доведите кабель до соответствующего концентратора и выберите Port 0 или Port 1.

Убедитесь, что все соединения компьютеров и концентраторов находятся в активном состоянии “Up”.

Войдите в раздел Options главного меню и в группе Preferences активизируйте режим имитации длины соединительных кабелей (Enable Cable Length Effects).

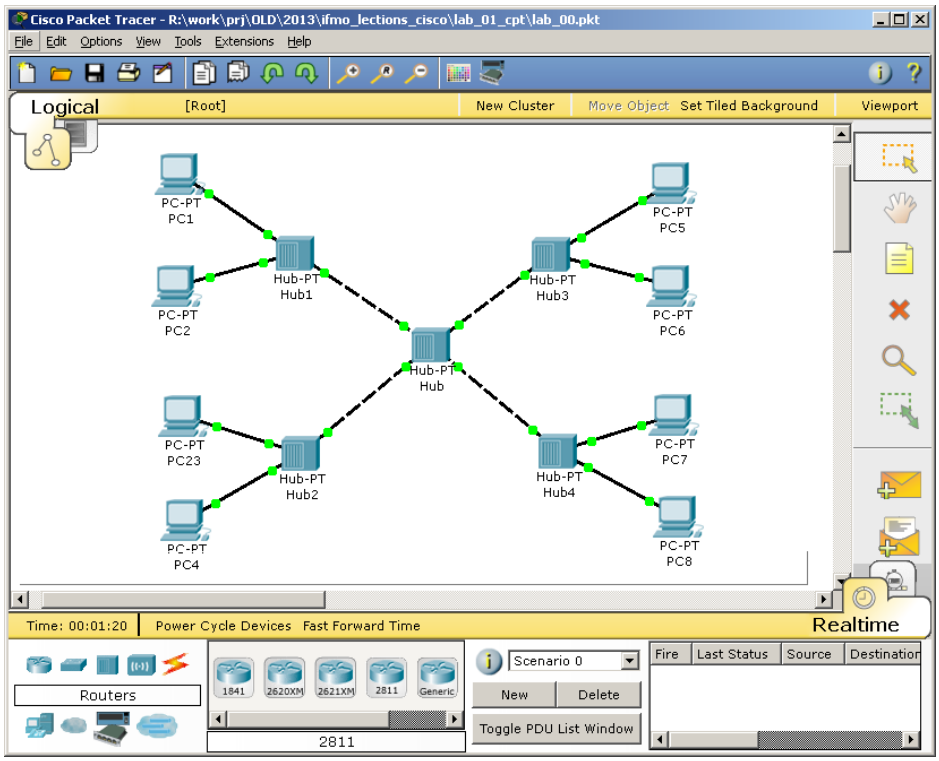


Рис. 1.7. Топология сети с одним доменом коллизий

2.5.2. Присвоение сетевых адресов рабочим станциям

Выберите PC1 и щелкните по его пиктограмме. В открывшемся окне настроек устройства перейдите во вкладку “Desktop”. Выберите пункт ”IP Configuration”. Укажите следующие настройки (рис.1.8):

IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

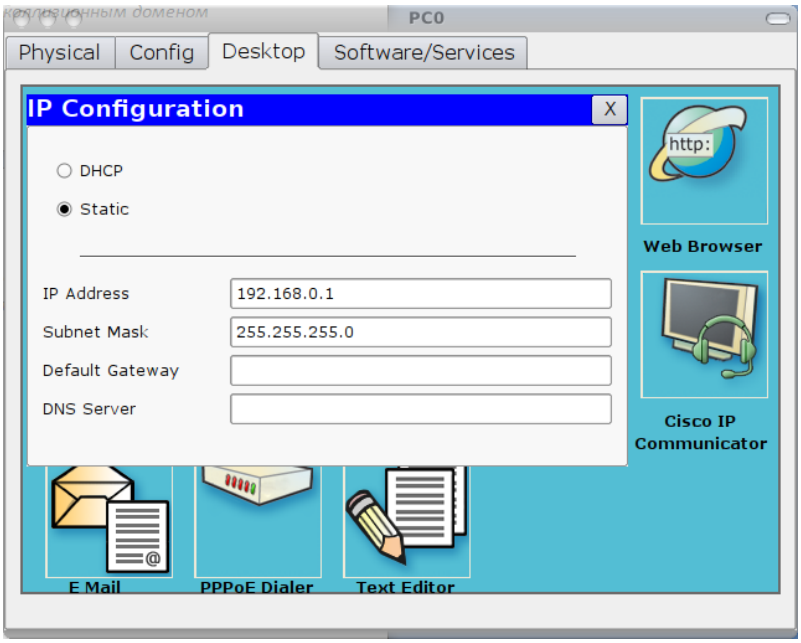


Рис. 1.8. Настройка сетевого адреса компьютера

Аналогичным образом проведите настройку остальных компьютеров, используя данные таблицы.

Таблица 1.2

Имя узла	IP-адрес	Маска подсети
PC1	192.168.0.1	255.255.255.0
PC2	192.168.0.2	255.255.255.0
PC3	192.168.0.3	255.255.255.0
PC4	192.168.0.4	255.255.255.0
PC5	192.168.0.5	255.255.255.0
PC6	192.168.0.6	255.255.255.0
PC7	192.168.0.7	255.255.255.0
PC8	192.168.0.8	255.255.255.0

Проверьте правильность проведенной настройки компьютеров.

Откройте окно настроек PC1. На вкладке “Desktop” выберите приложение “Command prompt” – аналог интерфейса командной строки windows. В открывшемся окошке после приглашения **PC>** наберите команду **ipconfig /all** и убедитесь в правильности введенных на прошлом шаге настроек сетевого подключения (рис. 1.9). Повторите процедуру проверки на других компьютерах.

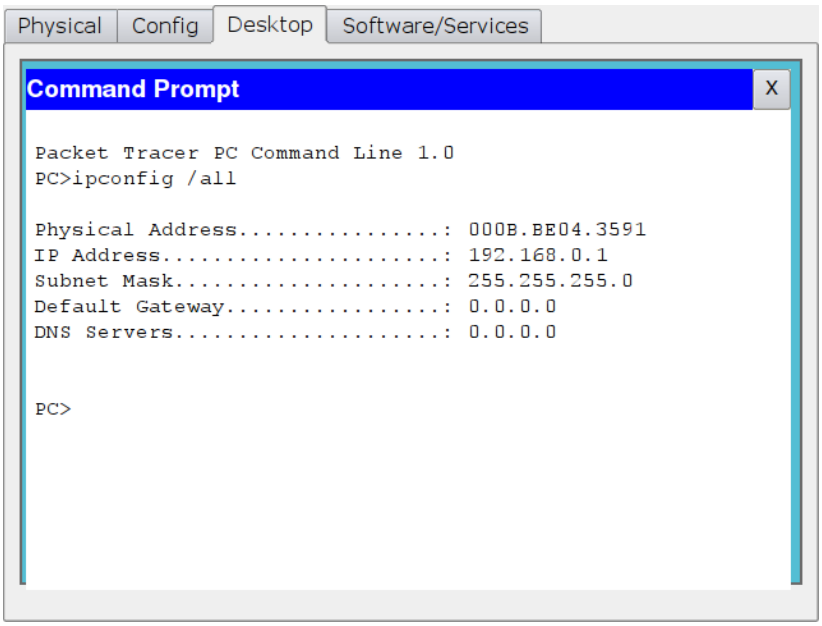


Рис. 1.9. Проверка настроек сетевого интерфейса

Интерфейс командной строки активно используется сетевыми администраторами и разработчиками оборудования для оперативного администрирования сети – конфигурирования и управления рабочими станциями, коммутаторами и маршрутизаторами. Доступ к командной строке зависит от типа операционной системы. В системе WindowsXP для доступа к командной строке проделайте следующие действия: Пуск->Выполнить и в открывшемся окне набрать cmd (Рис. 1.10).

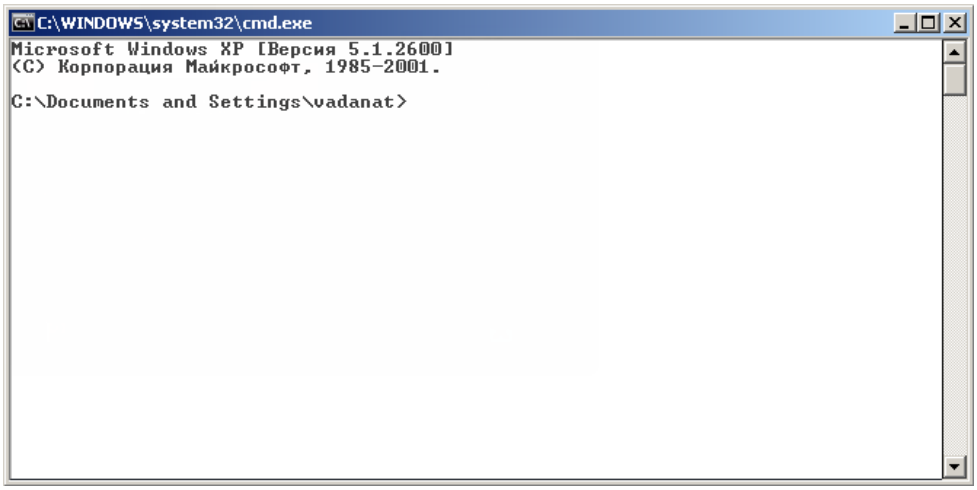


Рис. 1.10. Интерфейс командной строки в Windows XP

2.5.3. Проверка доступности рабочих станций в сети

Доступность компьютера проверяется при помощи посылки контрольного диагностического сообщения по протоколу ICMP (Internet Control Message Protocol), по которому любая оконечная станция должна выдать эхо-ответ узлу, отправившему такое сообщение.

В сетях на основе TCP/IP для проверки соединений обычно используется утилита ping. Эта программа отправляет запросы (ICMP Echo-Request) протокола ICMP узлу сети с указанным IP-адресом. Получив этот запрос, исследуемый узел должен послать пакет с ответом (ICMP Echo-Reply). Отправляющий узел фиксирует поступающие ответы. Время

между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно оценить загруженность каналов передачи данных и промежуточных устройств.

Часто ping-ом называют не только утилиту, но и сам запрос.

Проверим доступность узла PC2 с узла PC1. Для этого вернитесь на PC1. Запустите интерфейс командной строки “Command prompt” и выполните команду **ping 192.168.0.2**. В случае правильной конфигурации сети и компьютеров (PC1, PC2) на все отправленные эхо-запросы будут получены эхо-ответы (рис.1.11), о чем свидетельствует запись «потеряно 0%». При наличии ошибок в подключениях или настройках узлов будет получено сообщение о потере пакетов (рис 1.12).

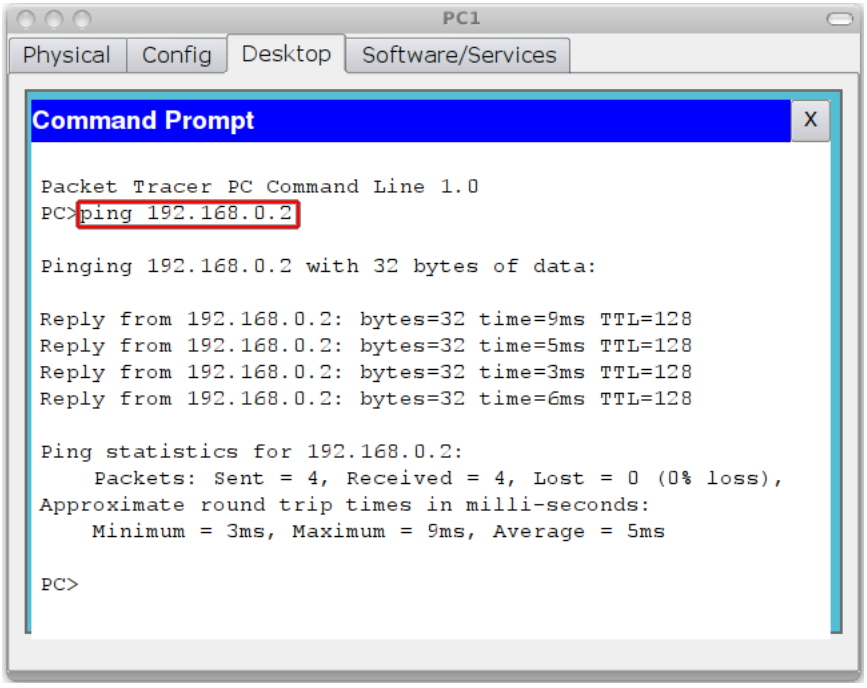


Рис. 1.11. Сообщение об успешной проверке доступности узла 192.168.0.2

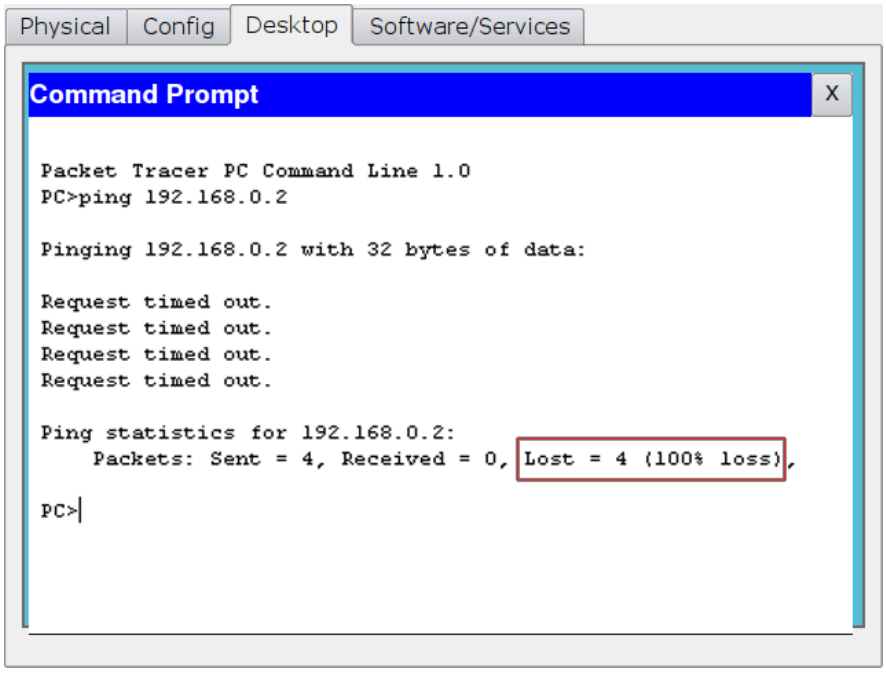


Рис. 1.12. Сообщение о потере пакетов

Проверьте доступность других компьютеров сети, выполнив команду **ping <IP_address>** для всех компьютеров в сети.

3. Исследование качества передачи трафика по сети с общей разделяемой средой

3.1. Формирование нагрузочного трафика в Cisco Packet Tracer

«Пингование» является универсальным средством тестирования сетей TCP/IP. Если увеличить размер пакета и отправлять запросы с коротким интервалом, не ожидая ответа от удаленного узла, то можно создать достаточную сетевую нагрузку.

Воспользуемся этим методом. При помощи протокола ICMP сформируем трафик между компьютерами PC3 и PC7. Штатная утилита ping не позволяет отправлять эхо-запрос (ICMP Echo-Request) без получения эхо-ответа (ICMP Echo-Reply) на предыдущий запрос или до истечения времени ожидания. Поэтому для организации трафика используем приложение Traffic Generator. В окне управления PC3 во вкладке Desktop выберите приложение Traffic Generator.

Укажите следующие настройки (рис.1.13):

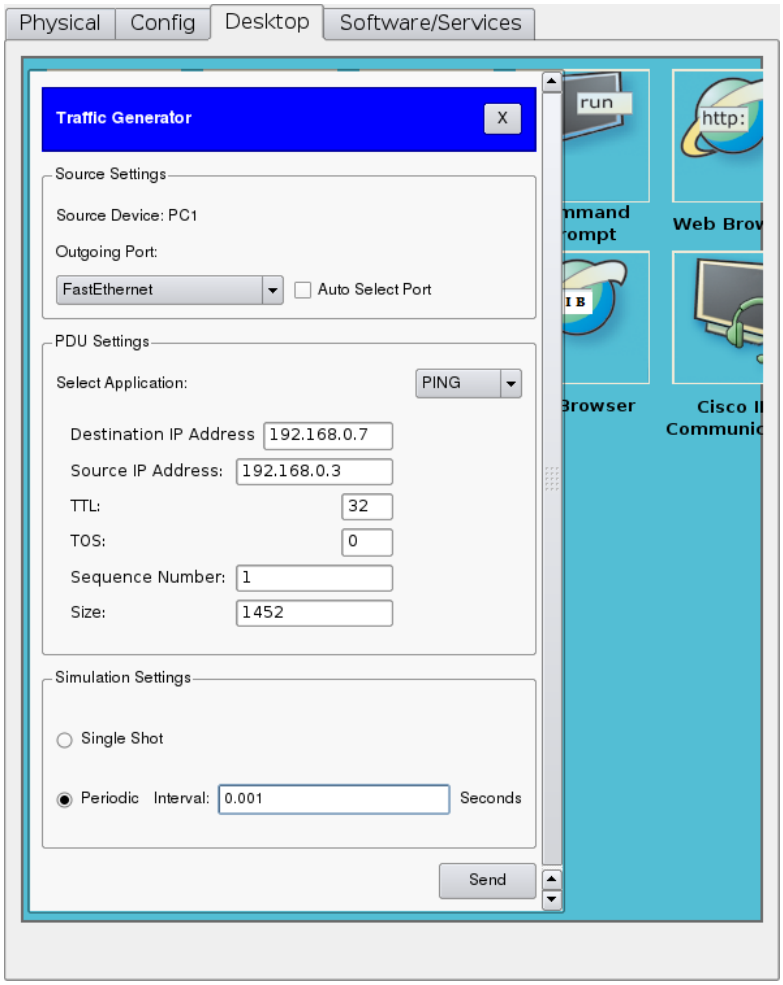


Рис. 1.13. Настройка генератора трафика

В разделе Source Settings (настройки источника) выберите FastEthernet.

В разделе PDU Settings (настройки IP-пакета):

Select application:	PING (т.е. использовать будем утилиту ping, протокол ICMP);
Destination:	IP Address: 192.168.0.7 (адрес получателя);
Source IP Address:	192.168.0.3 (адрес отправителя, указываем свой адрес);
TTL:	32(время жизни пакета; определяет максимальное число маршрутизаторов, которое пакет может пройти при продвижении по сети);
TOS:	0 (Type of Service - тип обслуживания, «0» - обычный, без приоритета);
Sequence Number:	1 (начальное значение счетчика пакетов);
Size:	1452 (размер поля данных пакета в байтах);

В разделе Simulations Settings (настройки имитации):

Periodic Interval:	0.001 Seconds (период повторения пакетов)

После нажатия кнопки Send между PC3 и PC7 начнется активный обмен данными. Не закрывайте окна настройки, чтобы не прервать поток трафика!

Обратите внимание на изменившуюся активность сетевых интерфейсов (мигание зеленых маркеров на линиях связи).

3.2. Визуализация передачи пакетов по сети в Cisco Packet Tracer

CPT позволяет наглядно представить прохождение пакетов по сети, используя режим “Simulation” (Имитация). Для перехода в этот режим нажмите на пиктограмму секундомера в панели выбора режима (рис. 1.14).

Справа появится панель управления для режима “Simulation” (рис. 1.14). Последовательно *многократно н*ажимая на кнопку «Capture / Forward» [5], *проследите,* как происходит пошаговое распространение пакетов по сети [2]. Перемещения пакетов синхронно регистрируются в списке событий (Event List [1]).

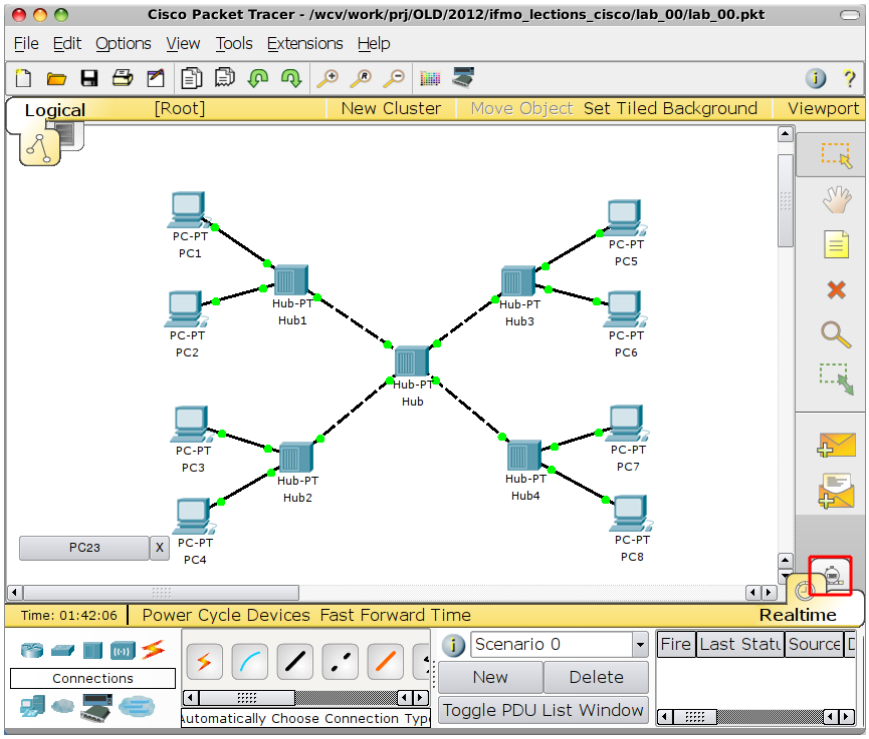


Рис. 1.15. Выбор режима симуляции в Cisco Packet Tracer.

В неструктурированной сети пакеты, передаваемые от PC3, распространяются по всей сети и поступают на входы всех конечных пользователей. При этом на всех компьютерах, кроме компьютера назначения PC7, полученные сообщения помечаются красными крестиками.

Изучите поведение пакетов при отправке эхо-запроса от PC3 к PC7 и эхо-ответа, передаваемого от PC7 к PC3. Визуализация процесса передачи пакетов по сети может быть осуществлена в автоматическом режиме. Для этого необходимо нажать кнопку «Auto Capture / Play».

Чтобы выйти из режима “Simulation”, нажмите кнопку «Realtime», находящуюся рядом с кнопкой “Simulation”.

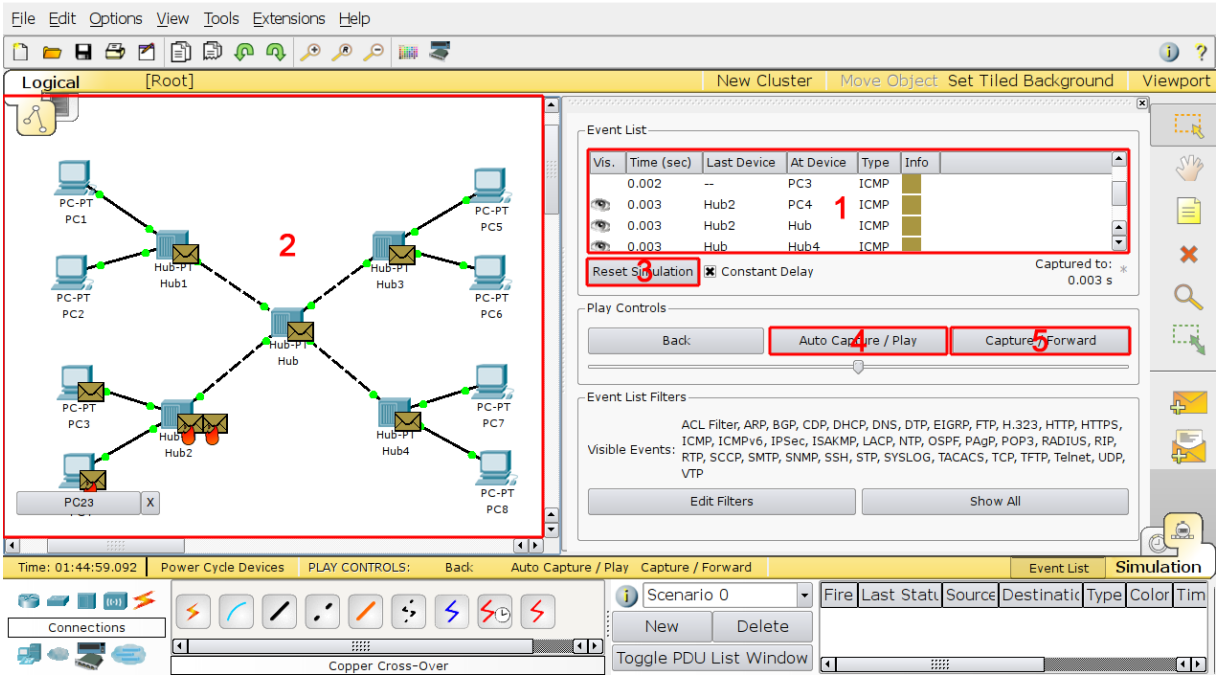


Рис 1.16. Режим имитации (Simulation)

3.3. Исследование качества передачи в сети с общей разделяемой средой

Вернитесь в режим «Realtime», нажав на значок часов в нижнем правом углу рабочего поля.

Для оценки качества работы сети передадим контрольный поток пакетов между PC1 и PC8 при помощи команды ping:

```
PC> ping –n 100 192.168.0.8
```

Параметр «–n» позволяет задать количество передаваемых эхо-запросов. Чем больше пакетов отправить, тем более точную статистику можно получить. В пределе (при $n \to \infty$) можно осуществить переход от коэффициента потерянных пакетов к вероятности потери пакета.

Отправим 100 эхо-запросов от PC1 к PC8, чтобы оценить исходное качество работы сети по числу потерянных пакетов.

Включите генератор трафика на компьютере PC3 (узел назначения – PC4, число импульсов - 350, период повторения - 0,015 с).

Оцените качество работы сети, передав контрольный поток от PC1 к PC8 (n=100). Зафиксируйте в процентах соотношение числа потерянных пакетов к числу переданных, а также среднее время прохождения пакета через сеть. Полученные результаты запишите в таблицу 1.3.

Таблица 1.3

Номер испытания	Задача испытания	Направление трафика	Параметры сигнала	Процент потерянных пакетов PC1-PC8	Средняя задержка	Джиттер[5]
1	2	3	4	5	6	7
1	Проверка исходного состояния сети	PC1-PC8	ping; n=100; N=32			
2	Передача информац. потока	PC1-PC8	ping; n=100; s=32			
		PC3-PC4	Traffic Generator s=350; T=0,15 с			

Остановите Traffic Generator на узле PC3, нажав кнопку Stop.

> В пакете Cisco Packet Tracer сетевой трафик представляет собой псевдослучайные импульсные последовательности, структура и временные соотношения между которыми устанавливаются программой эмуляции. При этом не обеспечивается независимость сигналов передаваемых с разных устройств. Тем не менее, проводимые в работе исследования позволяют оценить общие закономерности передачи сообщений в локальных вычислительных сетях.

4. Повышение пропускной способности локальной вычислительной сети путем логической структуризации

4.1. Логическая структуризация сети

Замените центральный концентратор коммутатором 2950-24 (Рис. 1.16). Для этого:

- удалите Hub1;
- поместите на освободившееся место в рабочей области Switch0 – коммутатор 2950-24;
- соедините концентраторы с коммутатором перекрестными кабелями.

[5] Джи́ттер (англ. jitter — дрожание) или фазовое дрожание цифрового сигнала данных - нежелательные фазовые и/или частотные случайные отклонения передаваемого сигнала. В данной работе разница между минимальной и максимальной задержкой.

Убедитесь, что сеть находится в рабочем состоянии. Маркеры портов коммутатора последовательно изменили красный цвет сначала на оранжевый, потом на зеленый. С компьютера PC1 доступны другие узлы сети.

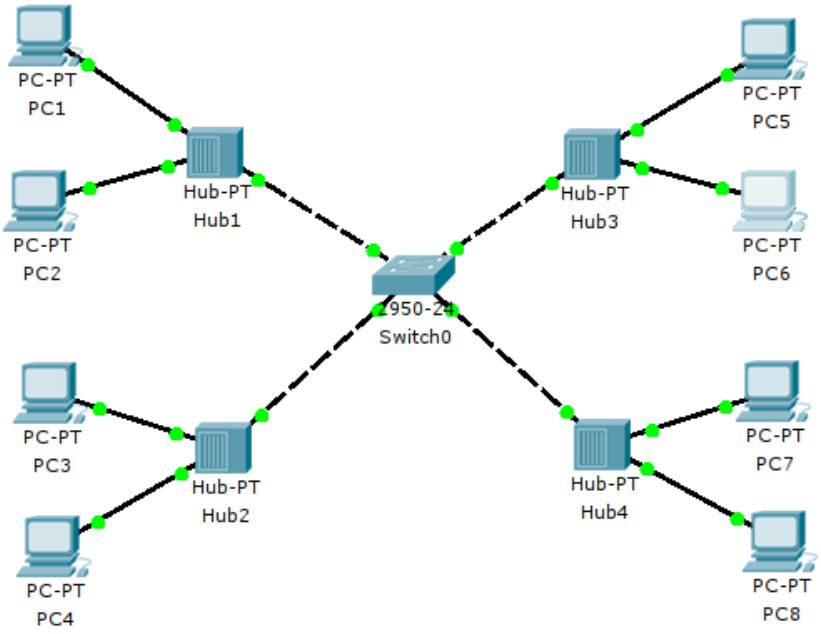


Рис. 1.17. Топология сети при замене центрального концентратора на коммутатор

При замене центрального концентратора коммутатором вся сеть разделилась на четыре логических сегмента (четыре коллизионных домена).

Включите Traffic Generator на PC3. Проследите движение пакетов в сети. Обратите внимание, что пакеты, передаваемые между PC3 и PC4, направляются только в сегменты сети, в которых находятся эти оконечные станции. Это видно по активности сетевых портов коммутатора (активно мигают зеленые индикаторы только в этих сегментах)

4.2. Визуализация передачи пакетов по структурированной сети

Перейдите в режим “Simulation”. При помощи кнопки “Capture/Forward” проследите пошаговое распространение пакетов, передаваемых между PC3 и PC4 в структурированной сети.

Проследите перемещения пакетов, используя кнопки “Capture/Forward”, “Auto Capture / Play” и записи в листе событий.

Вернитесь в режим «Realtime».

4.3. Исследование качества передачи трафика в структурированной сети

Запустите контрольный поток от PC1 на PC8 при помощи команды ping с параметром –n равным 100. Определите число потерянных пакетов.

Включите Traffic Generator на PC3 в режиме ping на PC4 (N=350, T=0,015 сек).

Включите контрольный поток от PC1 на PC8 и определите число потерянных пакетов.

Остановите Traffic Generator на узле PC3, нажав кнопку Stop.

Запишите полученный результат в таблицу 1.4.

Таблица 1.4

Номер испытания	Задача испытания	Направление трафика	Параметры сигнала	Процент потерянных пакетов PC1-PC8	Средняя задержка	Джиттер
1	Проверка исходного состояния сети	PC1-PC8	ping; n=100; N=32			
2	Передача информац. потока	PC1-PC8	ping; n=100; s=32			
		PC3-PC4	Traffic Generator s=350; T=0,15 с			

Сравните полученный результат с испытанием 3 п.3.3.

Как изменилось количество потерянных пакетов в структурированной сети по сравнению с сетью с общим доменом коллизий? Объясните полученные результаты.

5. Задание для самостоятельной работы

5.1. Исследование неструктурированной сети

Соберите сеть с одним доменом коллизий (рис. 1.7), присвойте IP-адреса рабочим станциям согласно данным из таблицы 1.2. Сгенерируйте трафик при помощи инструмента Traffic Generator в соответствии с вариантом задания, указанным в таблице 1.5.

Таблица 1.5

Вариант задания	Маршрут контрольного сигнала (ping, n=100, N=32)	Информационный трафик			
		Передатчик	Приемник	Размер пакета данных N, байт	Период повторения T, сек
1	PC1-PC4	PC7	PC8	1200	0.001
2	PC4-PC5	PC1	PC2	1000	0.002
3	PC7-PC1	PC4	PC3	950	0.001
4	PC6-PC1	PC8	PC7	1300	0.002
5	PC3-PC8	PC2	PC1	800	0.001
6	PC7-PC4	PC6	PC5	950	0.002
7	PC5-PC1	PC7	PC8	1000	0.005

8	PC2-PC6	PC3	PC4	1100	0.003
9	PC8-PC4	PC6	PC5	900	0.002
10	PC3-PC5	PC2	PC1	1300	0.004

При помощи контрольного ping-сигнала (n=100), оцените:

- исходное состояние сети;
- потери в сети при передаче информационного потока;
- время прохождения пакетов и джитпер.

Результаты запишите в таблицу 1.3.

5.2. Исследование структурированной сети с центральным коммутатором

Замените центральный концентратор коммутатором 2950-24 (Рис. 1.16). Включите Traffic Generator на оконечных станциях в соответствии с полученным вариантом задания. Проведите измерения, аналогичные измерениям по п. 5.1. Результаты запишите в таблицу 1.4.

5.3. Исследование полностью структурированной сети

Замените все концентраторы сети на коммутаторы cisco 2950-24. Включите Traffic Generator на оконечных станциях в соответствии с полученным вариантом задания. Снова проведите измерения, аналогичные измерениям по п.5.1. Результаты запишите в таблицу 1.4.

5.4. Отчет

Составьте отчет о лабораторной работе. В отчете необходимо отразить следующие вопросы:

- цели и методы логической структуризации компьютерных сетей;
- возможности программы Cisco Packet Tracer, использованные в данной работе;
- материалы по исследованию неструктурированной сети (схема сети, описание прохождения пакетов по сети, параметры передаваемого трафика, результаты пинг-контроля и оценка качества передачи);
- результаты исследования структурированной сети (схема сети, описание прохождения пакетов по сети, параметры передаваемого трафика, результаты пинг-контроля и оценка качества передачи);
- сравнение качества работы неструктурированных и структурированных сетей;
- объяснение полученных результатов и выводы

6. Рекомендуемые материалы

1. М.А.Плоткин. Лекции по курсу «Сети связи и системы коммутации». Тема 1 Компьютерные сети. Основные определения. Раздел «Коммуникационные устройства и структуризация компьютерных сетей».
2. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2010г. Глава 2 Общие принципы построения сетей.
3. http://fitos.ifmo.ru/web-downloads/packetTracer/PacketTracer533_setup.rar
4. Пакет Cisco Packet Tracer, Tutorials (Getting Started, Logical Workspace, Configuring Devices, Realtime and Simulation Modes).

Лабораторная работа №2.
Инициализация коммуникационных устройств в компьютерных сетях

1. Введение

При настройке в компьютерных сетях каждой рабочей станции и коммуникационному устройству должен быть присвоен набор исходных параметров, требующихся для работы в сетевых условиях. Операция назначения необходимых сетевых параметров называется ***инициализацией*** устройства. Обязательной частью инициализации является назначение IP-адресов (и соответствующих масок) сетевым интерфейсам компьютеров, коммутаторов и маршрутизаторов.

Присвоение сетевых адресов рабочим станциям вручную рассматривалось при выполнении лабораторной работы №1.

Ввод адресных данных непосредственно сетевым администратором требует выполнения значительного объема работ даже при не очень большом размере сети. Инициализация сетевых интерфейсов может проводиться автоматически при помощи протокола динамического конфигурирования хостов DHCP (Dynamic Host Configuration Protocol).

Протокол DHCP работает по схеме «клиент-сервер». При первом включении компьютер посылает в сеть широковещательный запрос на получение IP-адреса, а также других параметров, требующихся для работы в сетях TCP/IP. DHCP-сервер посылает в ответ сообщение, содержащее, IP-адрес и другую инициализирующую информацию.

Сервер DHCP обеспечивает различные режимы работы:

- ручное задание статических адресов, когда администратор вводит в сервер исходную информацию о соответствии IP-адресов физическим адресам или другим идентификаторам рабочих станций;
- автоматическое назначение статических адресов, когда сервер произвольным образом выбирает клиенту IP-адрес из множества наличных адресов, при этом адрес закрепляется за данным клиентом;
- динамическое распределение адресов, когда сервер выдает адрес клиенту на ограниченное время, называемое «сроком аренды»; при удалении компьютера из сети, назначенный IP-адрес автоматически освобождается. Режим динамического распределения адресов допускает построение сетей, у которых количество узлов превышает число имеющихся IP-адресов.

Инициализация коммуникационных устройств, наряду с присвоением имени узла и IP-адресов сетевым интерфейсам, включает назначение других параметров инициализации. Установка параметров инициализации производится в специальных режимах: привилегированном и режиме конфигурации. В целях безопасности доступ к таким режимам осуществляется при помощи различных паролей, выбор которых зависит от применяемой схемы инициализации.

Кроме параметров адресации, при инициализации коммуникационных устройств назначаются специализированные параметры, соответствующие особенностям конкретной компьютерной сети. Так, коммутаторам сообщаются данные либо одной общей, либо нескольких таблиц коммутации, маршрутизаторам – исходные адреса таблиц маршрутизации, IP-адрес маршрутизатора по умолчанию и др.

Включение в сеть хабов не требует какой-либо начальной установки, из-за безадресного алгоритма работы этих устройств.

После инициализации сетевые устройства обеспечивают возможность административного контроля и управления работой сети.

В лабораторной работе, в частности, проверяется работоспособность сети, оценивается состояние сетевых интерфейсов, находятся IP и MAC-адреса компьютеров и коммуникационных устройств, осуществляется управление состоянием сетевых портов, просматриваются таблицы коммутации, отключаются неиспользуемые сетевые протоколы.

2. Подключение к коммуникационному оборудованию

На рисунках 2.1 и 2.2 показаны маршрутизатор серии cisco 2811 и коммутатор серии cisco 3750 соответственно. Обратите внимание, что среди портов отсутствуют разъемы для монитора и клавиатуры. Большинство маршрутизаторов (коммутаторов) не имеют собственных мониторов и клавиатур, поэтому доступ к ним извне осуществляется через специальный консольный порт. Через этот порт производится подключение и первоначальная конфигурация устройства.

Рис. 2.1. Внешний вид маршрутизатора Cisco 2811

Рис. 2.2. Внешний вид коммутатора Cisco 3750G-24TS

Консольный порт cisco 2811 находится на лицевой панели устройства (Рис. 2.3) и представляет собой разъем RJ-45. Аналогичный порт есть и у коммутаторов, но расположен он, как правило, на задней панели. Для подключения к сетевому устройству необходим специальный консольный кабель и персональный компьютер (рис. 2.4).

Рис. 2.3. Консольный порт на маршрутизаторе Cisco 2811

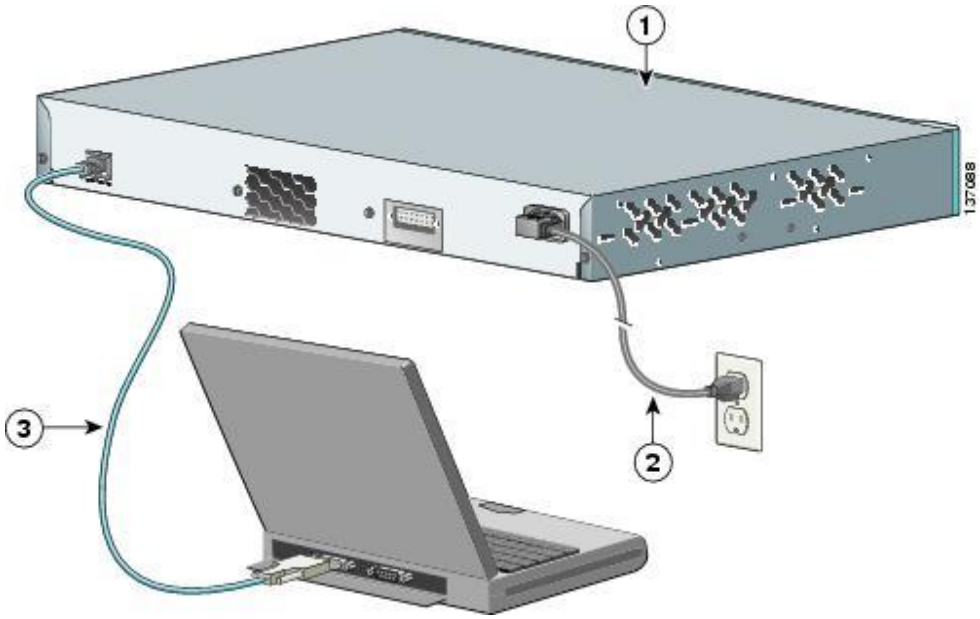


Рис. 2.4. Подключение к коммутатору при помощи консольного кабеля

Почти все современные маршрутизаторы и коммутаторы имеют свою собственную операционную систему (ОС), поэтому конфигурирование производится в режиме диалога между пользователем и ОС сетевого устройства при помощи персонального компьютера. Для организации этого диалога необходимо установить на ПК программу эмуляции терминала, которая транслирует команды пользователя в операционную систему устройства и выводит на экран компьютера результаты выполнения команд устройством.

> В маршрутизаторах и коммутаторах Cisco используется операционная система Cisco IOS (от англ. Internetwork Operating System — Межсетевая Операционная Система) Cisco IOS — многозадачная операционная система, выполняющая функции сетевой организации, маршрутизации, коммутации и передачи данных.

Чтобы максимально приблизить процесс настройки устройств к реальности, в программе Cisco Packet Tracer существует возможность подключения компьютера к консольному порту коммутатора или маршрутизатора. Для этого перенесите из панели «Выбор устройств» в рабочую область два устройства: компьютер Laptop и коммутатор 2950-24. Затем в панели «Типы подключений» выберите подключение типа «Консоль» и соедините консольным кабелем COM-порт (RS-232) компьютера Laptop с консольным портом (Console) коммутатора S1 (рис.2.5).

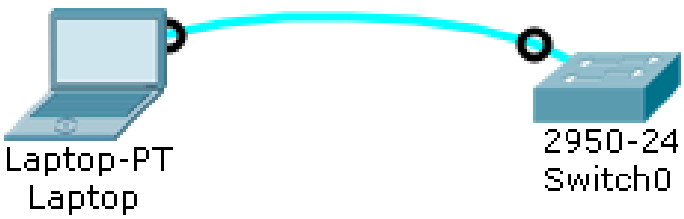


Рис. 2.5. Подключение консольного кабеля в Cisco Packet Tracer

На компьютере Laptop запустите приложение Terminal, находящееся в окне управления компьютера (рис. 2.6).

Рис. 2.6. Cisco Packet Tracer. Выбор приложения Terminal

При подключении терминала (рис. 2.7) следует указать настройки, аналогичные тем, которые используются при работе с реальным оборудованием Cisco (обычно эти настройки указываются производителем в инструкции по эксплуатации сетевого устройства).

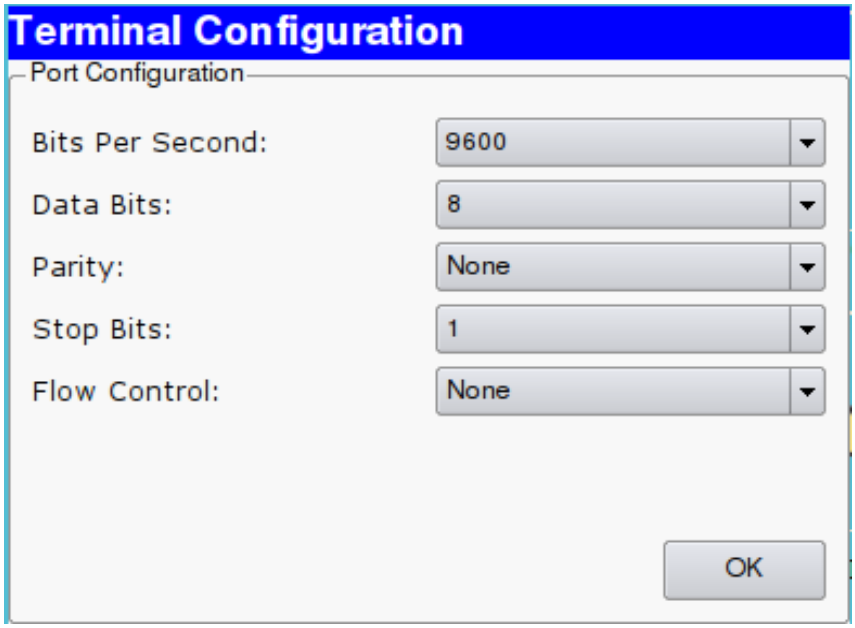


Рис. 2.7. Настройка серийного интерфейса компьютера в Cisco Packet Tracer

Если все указано правильно, то в открывшемся окне терминала вы должны увидеть текстовое сообщение, аналогичное сообщению, изображенному на рис. 2.8.

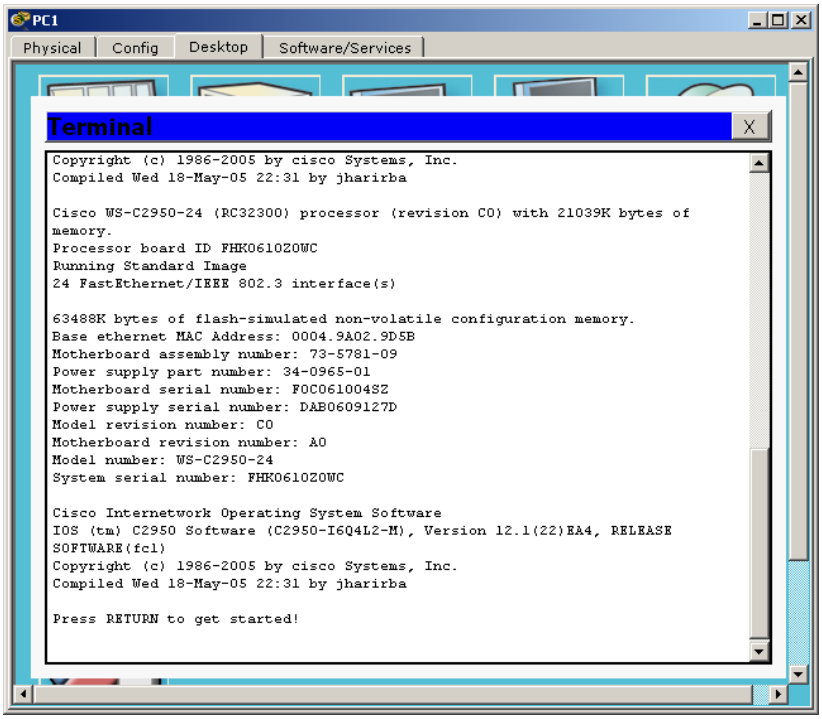


Рис. 2.8. Приглашение к диалогу конфигурации Cisco IOS

> Альтернативным способом получения доступа к консольному интерфейсу является использование вкладки CLI в окне свойств коммутатора S1. Стоит отметить, что доступ к реальному оборудованию можно получить только через терминал.

Сообщение представляет собой приглашение к диалогу по конфигурации коммутатора Switch 0 через консольный порт. Данное сообщение появляется после загрузки устройства при его непосредственной поставке с завода (устройство еще не сконфигурировано), или после удаления файла сохраненной конфигурации устройства (обсуждается ниже).

Откажитесь от использования диалога конфигурирования, нажав клавишу Enter. После этого вы увидите приглашение **`Switch>`**, говорящее о том, что вы находитесь в пользовательском режиме (рис. 2.9).

```
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of
memory.
Processor board ID FHK0610Z0WC
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0004.9A02.9D5B
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: F0C061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!


Switch>
```

Рис. 2.9. Приглашение пользовательского уровня Cisco IOS.

В операционной системе Cisco IOS существуют два уровня команд: привилегированный и непривилегированный. Отличаются эти уровни списком доступных команд. Для диагностики работоспособности сети достаточно использовать непривилегированный уровень, однако конфигурация устройства производится только в привилегированном режиме. Для перехода в привилегированный режим наберите команду **enable** и нажмите клавишу Enter. Приглашение изменится на **Switch#** (рис. 2.10). Символ # свидетельствует о том, что сейчас терминал находится в привилегированном режиме. Для выхода из привилегированного уровня используется команда **exit.**

```
memory.
Processor board ID FHK0610Z0WC
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0004.9A02.9D5B
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: F0C061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!



Switch>enable
Switch#
```

Рис. 2.10. Приглашение привилегированного уровня Cisco IOS

2.1. Система помощи

В ОС Cisco IOS встроена система помощи, обратиться к которой можно из режима исполнения команд EXEC. Система помощи является контекстной. Это означает, что выводимые подсказки зависят от того, что пользователь пытается сделать в ОС IOS на данный момент. Например, введя в командной строке знак "?", пользователь получит следующую информацию о возможных командах:

```
Switch>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
```

```
traceroute  Trace route to destination
```

Особо стоит отметить, что в операционной системе Cisco IOS не обязательно вводить всю команду — однозначно интерпретируемые команды по умолчанию будут дополнены. Это означает, что, например, ввод команд **#enable** и **#en** даст одинаковый результат.

Также очень удобным является инструмент автодополнения команд. При вводе одной или нескольких символов предполагаемой команды нажмите Tab, и IOS автоматически завершит ее, если эти символы позволяют ее однозначно интерпретировать, или предложит список команд, начинающихся с введенной последовательности символов.

Совместное использование сокращенных команд и автодополнения позволяет значительно ускорить работу и избежать ошибок, появляющихся при вводе команд вручную.

3. Базовая настройка коммутатора/маршрутизатора

Текущая конфигурация коммутатора (running-config) находится в оперативной памяти. При выполнении команд администратора в эту конфигурацию вносятся соответствующие изменения. Когда коммутатор выключается, содержимое оперативной памяти обнуляется. Поэтому для сохранения текущих настроек перед выключением устройства необходимо скопировать running-config на флеш-накопитель (в энергонезависимую память).Конфигурация, сохраненная во флеш-накопителе, называется стартовой (startup-config). При каждом включении коммутатора startup-config считывается из флеш-накопителя в оперативную память и становится текущей конфигурацией (running-config). Дальнейшие операции по настройке оборудования производятся с running-config.

3.1. Удаление старой конфигурации

Если коммутатор ранее использовался и был сконфигурирован под какие-либо задачи, то вместо приглашения к диалогу начального конфигурирования (рис. 2.10) на экран монитора будет выведено приглашение для ввода пароля или приглашение непривилегированного режима, отмеченное символом >.

Чтобы упростить настройку и избежать лишних ошибок, целесообразно удалить ранее использовавшуюся стартовую конфигурацию и восстановить исходную заводскую конфигурацию коммутатора. Для этого необходимо в привилегированном режиме удалить файл стартовой конфигурации при помощи команды **erase startup-config**.

```
Switch# erase startup-config
     Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
     [OK]
     Erase of nvram: complete
     %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Затем при помощи команды **reload** выполните перезагрузку коммутатора. Cisco IOS при загрузке не обнаружит файл стартовой конфигурации, и в running-config будет загружена минимальная заводская конфигурация. После загрузки появится приглашение, аналогичное рис. 2.9.

3.2. Вход в режим конфигурирования

Помимо уровней доступа (привилегий), в коммутаторах и маршрутизаторах Cisco существует несколько режимов и уровней конфигурирования. Так в привилегированном режиме, обозначенном приглашением **switch#**, невозможно произвести ***настройку***

оборудования. Для настройки необходимо перейти в ***режим конфигурирования***, выполнив команду **configure terminal**. Это сделано для предотвращения случайного ввода команд, способных нарушить работу устройства. При входе в режим конфигурирования приглашение изменится на Switch(config)#:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Используйте команду "?" для вывода команд, доступных в этом режиме. Обратите внимание, что список команд изменился по сравнению с ранее доступными командами.

Для выхода из режима конфигурирования используйте команду **exit** или комбинацию клавиш **Ctrl-Z**.

3.3. Настройка имени узла

Вначале зададим имя коммутатора. Это необязательная операция, но ее настоятельно рекомендуется осуществить во избежание путаницы. Если все устройства имеют одно и то же название (Switch), часто становится не очень понятно, какой из коммутаторов настраивается в данный момент.

В режиме конфигурирования (обратите внимание на приглашение **Switch(config)#**) наберите команду **hostname <имя узла>**:

```
Switch(config)#hostname S1
S1(config)#
```

Как видите, название коммутатора в приглашении изменилось на S1 **.**

3.4. Настройка баннера приветствия

Баннер – это текстовое сообщение, которое выводится при подключении к коммутатору через сеть. После ввода команды **banner motd** в режиме глобального конфигурирования напишите произвольный текст. Текст начинается и завершается вводом символа **%.**

```
S1(config)#banner motd %equipment owned by the Orbit-Networks.
Immediately leave the device!%
S1(config)#
```

В нашем случае баннер будет указывать на принадлежность маршрутизатора абстрактному оператору связи Orbit-Networks.

3.5. Настройка пароля привилегированного режима

В режиме конфигурирования для настройки пароля используйте команду **enable secret**. В качестве пароля введите class.

Внимание! При вводе паролей следует запомнить регистр, используемый при наборе буквенных символов, а также наличие (или отсутствие) пробелов между паролем и командой Enter. При последующих наборах пароля необходимо точно воспроизвести ранее введенное слово.

```
S1(config)#enable secret class
```

3.6. Настройка пароля для доступа к устройству через консоль

Команда **line console 0** предназначена для входа в режим конфигурирования консольного порта. Для настройки доступа к коммутатору через консольный порт введите команды указанные ниже.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
```

Выход из режима осуществляется вводом **exit** или комбинации клавиш **Ctrl-Z.**

3.7. Настройка пароля для доступа к устройству через сетевое подключение

Команда line vty 0 15 предназначена для входа в режим конфигурирования терминальных линий, обеспечивающих удаленный доступ в пользовательском режиме к коммутатору через telnet (протокол эмуляции терминала) или ssh (протокол удаленного управления операционной системой).

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
```

Выход из режима осуществляется вводом **exit** или комбинации клавиш **Ctrl-Z.**

3.8. Настройка сетевого интерфейса коммутатора

Одной из главных задач первоначальной настройки сетевого устройства является настройка IP-адреса на одном из сетевых интерфейсов устройства. Здесь впервые проявляется разница в настройке коммутаторов и маршрутизаторов.

У маршрутизаторов IP адрес, как правило, задается на интерфейсах, привязанных к физическим сетевым интерфейсам, а у коммутатора IP адрес задается на виртуальном интерфейсе, который по умолчанию связан со всеми физическими портами. Таким образом, коммутаторы имеют преимущество: при отключении физических интерфейсов виртуальный интерфейс остается рабочим, а IP адрес доступным.

Для настройки виртуального интерфейса на коммутаторе необходимо:

1. Из привилегированного режима перейти в режим конфигурирования при помощи команды **configure terminal**
2. Зайти в режим конфигурирования, выполнив команду **interface <Название интерфейса>**. В нашем случае для всех коммутаторов будем использовать виртуальный интерфейс по умолчанию **vlan1**. Далее в этой и последующих работах будет показано, как посмотреть список доступных интерфейсов.
3. В режиме конфигурирования интерфейса задать описание интерфейса при помощи команды **description <любой текст>** Действие не является обязательным, но делать это настоятельно рекомендуется.
4. В режиме конфигурирования задать сетевой адрес. Для задания Р адреса в IOS используется команда **ip address <IP> mask <MASK**> выполняемая в режиме конфигурирования интерфейса
5. Включить сетевой интерфейс, для этого в режиме конфигурирования интерфейса необходимо выполнить команду **no shutdown**

Ниже приведен пример конфигурирования виртуального интерфейса коммутатора S1:

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S1(config)#int vlan 1
S1(config-if)#description --< mgmt interface >--
S1(config-if)#ip address 172.17.0.1 255.255.0.0
S1(config-if)#no shutdown
```

Для возврата в привилегированный режим используйте комбинацию клавиш **Ctrl+Z** или команду exit.

4. Создание локальной сети с использованием конфигурируемого оборудования в программе Cisco Packet Tracer

4.1. Создание сети

Добавьте в рабочую область еще несколько сетевых устройств, таким образом, чтобы у вас получилась сеть с физическими подключениями как показано на рис. 2.11.

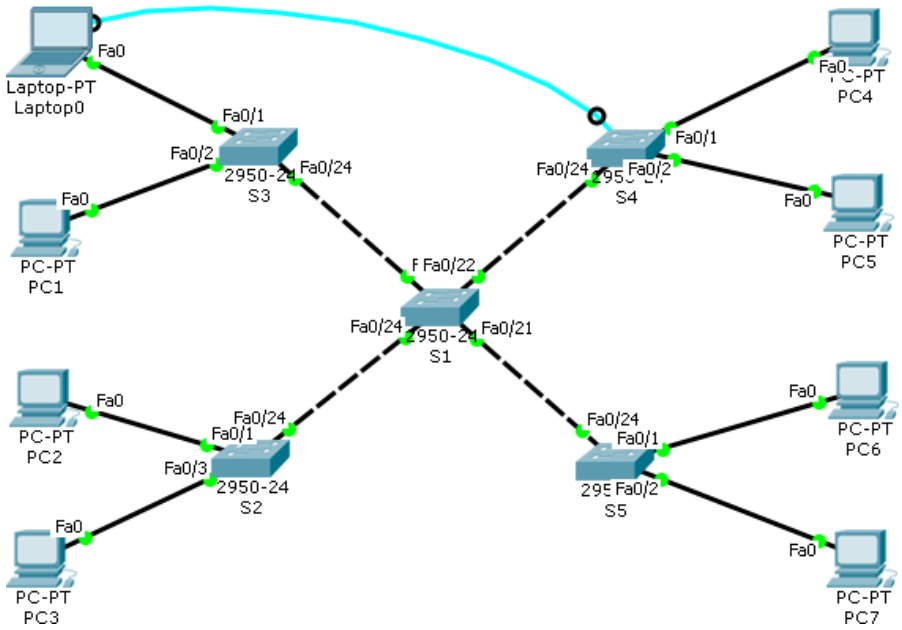


Рис. 2.4.11. Схема сети в Cisco Packet Tracer

Произведите базовую настройку коммутаторов на основе материала из главы выше, последовательно подключая Laptop консольным кабелем к каждому коммутатору.

IP-адреса коммутаторов S1-S5 взять из таблицы 2.1.

Для ускорения процесса не производите настройку паролей для доступа к оборудованию.

Таблица 2.1.

Устройство	IP-адрес	Маска
S1	172.17.0.1	255.255.0.0
S2	172.17.0.2	255.255.0.0
S3	172.17.0.3	255.255.0.0

S4	172.17.0.4	255.255.0.0
S5	172.17.0.5	255.255.0.0
Laptop	172.17.10.20	255.255.0.0
PC1	172.17.10.21	255.255.0.0
PC2	172.17.10.22	255.255.0.0
PC3	172.17.10.23	255.255.0.0
PC4	172.17.10.24	255.255.0.0
PC5	172.17.10.25	255.255.0.0
PC6	172.17.10.26	255.255.0.0
PC7	172.17.10.27	255.255.0.0

4.2. Настройка сетевых интерфейсов компьютеров

Настройте компьютеры Laptop, PC1-PC7, указав IP-адрес, маску и шлюз из таблицы 2.1. Настройка IP-адресов персональных компьютеров в Cisco Packet Tracer была описана в лабораторной работе №1.

4.3. Проверка работоспособности сети

Произведите проверку работоспособности сети, пропинговав с Laptop все остальные компьютеры сети. Проверка работоспособности сети в Cisco Packet Tracer была описана в лабораторной работе №1.

5. Возможности управляемых сетевых устройств

5.1. Проверка работоспособности сети

Использование управляемых сетевых устройств позволяет производить дополнительные действия, например, можно проверить доступность узлов сети с коммутатора. Для этого в пользовательском режиме выполните команду ping <ip_address>:

```
S1>ping 172.17.10.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.10.21, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/10 ms
```

Вывод команды аналогичен выводу команды ping, выполненной на компьютере.

> В ряде случаев (посылка первого эхо-запроса) часть пакетов может быть потеряна, что отображается в выводе команды ping в виде точек вместо восклицательных знаков.

> Данное явление является нормой и связано, как правило, с формированием динамических таблиц в сетевых устройствах. На формирование требуется время и, пока они [динамические таблицы] не будут сформированы, передача информации не может быть осуществлена.

С коммутатора S1 проверьте доступность остальных сетевых устройств (компьютеров Laptop, PC1-PC7 и коммутаторов S2-S5).

5.2. Проверка состояния сетевых интерфейсов

В привилегированном режиме выполните команду show **ip interface brief** и просмотрите вывод команды. Ниже приведен пример для коммутатора S3:

```
S3#show ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
...
FastEthernet0/21 unassigned YES manual down down
FastEthernet0/22 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual up up
Vlan1 172.17.0.3 YES manual up up
```

Из вывода команды видно, что интерфейсы коммутатора S3 FastEthernet0/3-23 находятся в состоянии **down** (не обнаружено сигнала на канальном уровне). Интерфейсы FastEthernet0/1, FastEthernet0/2, FastEthernet0/24 и Vlan1 находятся в состоянии up (включены и на канальном уровне обнаружен сигнал), что соответствует нашей схеме включения и настройки виртуального интерфейса Vlan1.

На интерфейсе Vlan1 помимо прочего задан IP адрес 172.17.0.3.

Для более подробного вывода информации по интерфейсам сетевых устройств необходимо в привилегированном режиме выполнить команду **show interfaces**:

```
S1#show interfaces
FastEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0000.0c7b.9801 (bia 0000.0c7b.9801)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
```

```
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
```

Более подробно вывод этой команды будет обсуждаться в последующих работах.

5.3. Управление состоянием физических портов

Иногда возникает необходимость административного отключения/включения сетевых интерфейсов. Для этого в режиме конфигурирования используйте команды **shutdown** (выключение) **и no shutdown** (включение).

1. Запустим команду ping на **Laptop** с ключом –t (бесконечное количество эхо-запросов).

```
PC>ping -t 172.17.10.27
```

> Замечание**.** Для остановки передачи сигнала ping используйте комбинацию клавиш **Ctrl+C**

2. Для выключения интерфейса, к которому подключен **Laptop,** на коммутаторе S3 в режиме конфигурирования интерфейса выполним команду shutdown:

```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface FastEthernet 0/1
S3(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
```

В консоли коммутатора появились диагностические сообщения об изменении статуса порта и изменении состояния порта на канальном уровне. В Cisco Packet Tracer это также отображается изменением цвета маркеров на портах с красного на зеленый.

3. Просмотрите состояние портов при помощи команды show **ip interface brief** (в привилегированном режиме) и убедитесь, что порт FastEthernet0/1 находится в состоянии **down** по причине отключения его администратором (**administratively down**):

```
S3#show ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual administratively down down
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual down down
…
```

4. Проверьте, что в этот момент команда ping, запущенная на компьютере **Laptop** стала выдавать сообщения о потере пакетов:

```
PC>ping -t 172.17.10.27
Pinging 172.17.10.27 with 32 bytes of data:

Reply from 172.17.10.27: bytes=32 time=10ms TTL=255
Reply from 172.17.10.27: bytes=32 time=0ms TTL=255
...
Request timed out.
Request timed out.
```

```
    Request timed out.
```

5. Включите обратно сетевой интерфейс:

```
S3(config)#interface fa0/1
S3(config-if)no shutdown

S3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

6. Проверьте результаты вывода команды ping на **Laptop** и убедитесь, что с **Laptop** снова доступны все устройства в сети. Остановите выполнение команды ping.

5.4. Отключение дополнительных протоколов

По умолчанию на коммутаторах включен ряд протоколов, таких как spanning-tree[6], dtp[7], cdp[8] и т.д.

При работе этих протоколов коммутатор регулярно отправляет пакеты с mac-адресами своих интерфейсов, что приводит к появлению служебных записей в таблице коммутации. Это несколько усложняет ее изучение. Рассмотрение вышеуказанных протоколов не является целью этой работы, поэтому их необходимо отключить на всех коммутаторах.

В режиме глобального конфигурирования отключите cdp и spanning-tree (пример для S1):

```
S1(config)#no cdp run
S1(config)#no spanning-tree vlan 1-4096
```

Команда **switchport nonegotiate** в режиме конфигурирования интерфейса запрещает отправку пакетов dtp через этот интерфейс (пример для S1):

```
S1(config)#interface fa0/24
S1(config-if)#switchport mode access
S1(config-if)#switchport nonegotiate
```

Выполните эту команду на всех интерфейсах, соединяющих коммутаторы.

---

[6] **STP (Spanning-Tree Protocol)** - алгоритм «покрывающего дерева», устраняет возможные сетевые петли и обеспечивает единственность маршрутов между любыми двумя узлами компьютерных сетей, построенных на коммутаторах. Включен по умолчанию.

[7] **DTP (Dynamic Trunk Protocol)** —протокол Cisco, который позволяет коммутаторам динамически распознавать настроен ли соседний коммутатор для поднятия транка и какой протокол использовать (802.1Q или ISL). Включен по умолчанию.

[8] **CDP (Cisco Discovery Protocol)** —протокол второго уровня, разработанный компанией Cisco Systems, позволяющий обнаруживать подключённое (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию IOS и IP-адреса. Включен по умолчанию.

5.5. Просмотр таблиц коммутации

Одной из важнейших возможностей управляемых коммутаторов является возможность просмотра таблицы коммутации, на основе которой коммутатор производит коммутацию пакетов только по заданному адресу (основное отличие коммутаторов от хабов).

Таблицы коммутации являются динамическими, то есть формируются большей частью автоматически на основе информации, получаемой из проходящих через коммутаторы пакетов. Поэтому данные в таблице постоянно обновляются.

При отсутствии трафика через какое-то время происходит ее очистка. На данный момент таблица должна быть уже заполнена какими-то адресами, т.к. между устройствами был обмен пакетами.

1. Просмотрите таблицу коммутации коммутатора S3.

```
S3#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c953.de18    DYNAMIC     Fa0/24
   1    000a.4109.7a18    DYNAMIC     Fa0/24
   1    0060.2f27.2417    DYNAMIC     Fa0/1
   1    00e0.b080.d1b8    DYNAMIC     Fa0/24
```

Содержание таблицы коммутации может различаться в зависимости от времени прошедшего с момента окончания обмена пакетами между устройствами.

2. Убедитесь, что выполнение команды ping остановлено. Произведите очистку таблицы коммутации при помощи команды **clear-mac-address** в привилегированном режиме:

```
S3#clear mac-address-table
```

Выполните эту команду на всех коммутаторах.

3. Просмотрите таблицу коммутации коммутатора S3, выполнив в привилегированном режиме команду **show mac-address-table**

```
S3#show mac-address-table
Mac Address Table
-------------------------------------------

Vlan Mac Address Type Ports
---- ----------- -------- -----
```

Таблица должна быть пустой, т.к. после очистки не было обмена пакетами между сетевыми устройствами.

4. Найдите mac-адреса Laptop и PC7 выполнив команду **ipconfig /all** на этих компьютерах (адреса могут отличаться от приведенных ниже):

```
PC>ipconfig /all
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.................: 0001.4393.C1E3
Link-local IPv6 Address.........: FE80::201:43FF:FE93:C1E3
IP Address......................: 172.17.10.20
```

```
     Subnet Mask.....................: 255.255.0.0
     Default Gateway.................: 0.0.0.0
     DNS Servers.....................: 0.0.0.0
     DHCP Servers....................: 0.0.0.0
     DHCPv6 Client DUID..............: 00-01-00-01-5D-92-C1-4D-00-01-43-93-
C1-E3

     PC7>ipconfig /all
     FastEthernet0 Connection:(default port)
     Connection-specific DNS Suffix..:
     Physical Address................: 0002.4A26.54AB
     Link-local IPv6 Address.........: FE80::202:4AFF:FE26:54AB
     IP Address......................: 172.17.10.27
     Subnet Mask.....................: 255.255.0.0
     Default Gateway.................: 0.0.0.0
     DNS Servers.....................: 0.0.0.0
     DHCP Servers....................: 0.0.0.0
     DHCPv6 Client DUID..............: 00-01-00-01-28-BD-C1-12-00-02-4A-26-
54-AB
```

5. Сгенерируйте обмен пакетами между Laptop и PC7, выполните команду ping:

```
PC>ping 172.17.10.27
```

6. Снова проверьте таблицу коммутации на S3:

```
S3#show mac-address-table
Mac Address Table
-------------------------------------------

Vlan Mac Address Type Ports
---- ----------- -------- -----

1 0001.4393.c1e3 DYNAMIC Fa0/1
1 0002.4a26.54ab DYNAMIC Fa0/24
```

Обратите внимание, что

- адрес 0001.4393.c1e3 соответствует Laptop, который подключен на нашей схеме к порту Fa0/1 коммутатора S1
- адрес 0002.4a26.54ab соответствует PC7, который подключен напрямую к коммутатору S5, но на схеме S1 подключен к S5 через порт Fa0/24.

7. Просмотрите таблицы коммутации на коммутаторах S1 и S5. Убедитесь в том, что адреса устройств в таблицах коммутации связаны с интерфейсами, на которые нужно отправить пакет, чтобы он достиг устройства с этим адресом.

Затем проанализируйте таблицу коммутации на коммутаторах S2 и S4.

8. Поочередно с Laptop “пропингуйте” остальные компьютеры в сети, параллельно просматривая изменение в таблице коммутации на S3. Убедитесь что новые mac-адреса появляются на нужных портах коммутатора.

Просмотрите и дайте пояснения по таблицам коммутации на коммутаторах S1, S2, S4, S5.

6. Контрольные вопросы

1. Какие преимущества дает использование управляемого сетевого оборудования?
2. Зачем в коммутаторах используется таблица коммутации?

3. Для чего каждая запись в таблице коммутации имеет ограниченное время жизни и удаляется, если устройство с данным mac-адресом перестает отправлять пакеты?
4. В классическом варианте технологии Ethernet (с общей разделяемой средой передачи) основным фактором, ограничивающим максимальное количество устройств в сети, было возрастание вероятности возникновения коллизии. При использовании коммутаторов коллизии отсутствуют. Чем тогда, на ваш взгляд ограничивается максимальное количество устройств в такой сети?

7. Задание для самостоятельной работы

1. Получите у преподавателя pka-файл с персональным заданием. Откройте этот файл в программе Cisco Packet Tracer и следуйте инструкциям, которые появятся после открытия файла.
2. Ознакомьтесь с исходными данными и выполните задание.
3. Сохраните конфигурацию всех сетевых устройств.
4. Сохраните изменения в pka-файле и отправьте его преподавателю в качестве отчета о выполнении самостоятельной работы.

8. Рекомендуемые материалы

1. М.А.Плоткин. Лекции по курсу «Сети связи и системы коммутации». Тема 4 Технологии локальных вычислительных сетей. Раздел «Технология виртуальных локальных сетей (VLAN)».
2. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г. Глава 14 Интеллектуальные функции коммутаторов. Раздел «Виртуальные локальные сети», стр.467-474.
3. Леммл Т., Хейз К. Настройка коммутаторов Cisco. Учебное руководство, Лори, 2002, С. 464.
4. Шин Одом, Хенсон Ноттингем Коммутаторы CISCO, Кудиц Образ, 2003, С. 522, ISBN: 5-93378-051-0
5. Интернет ресурс http://www.cisco.com
6. Интернет ресурс http://xug.ru

Лабораторная работа №3.
Конфигурирование и мониторинг виртуальных компьютерных сетей

1. Введение

Построение крупных локальных сетей на основе технологии Ethernet связано с определенными трудностями.

Структуризация сети Ethernet путем формирования логических сегментов позволяет сократить нагрузку на каждый сегмент и повысить производительность, безопасность и управляемость всей сети. Тем не менее, в структурированных локальных сетях, использующих в качестве коммуникационных устройств коммутаторы, в которых обрабатываются передаваемые кадры с плоскими MAC-адресами, существует ряд проблем:

- возможность возникновения широковещательных штормов (Broadcast Storm);
- трудности объединения в одном логическом сегменте удаленных пользователей.

Напомним, что коммутатор обеспечивает три основных алгоритма обработки передаваемых кадров:

- продвижение (Forwarding) кадра, принятого через данный порт, к другому порту в соответствии с записью в таблице коммутации;
- фильтрация (Filtering) кадра, принятого через данный порт, если MAC-адрес получателя доступен через этот же порт; в этом случае кадр отбрасывается, т.к. пользователь уже должен был получить этот кадр;
- передача кадра, принятого через данный порт, ко всем портам коммутатора – затопление сети (Flooding); в таком режиме передаются кадры с широковещательными MAC-адресами, а также кадры с неизвестными групповыми или индивидуальными адресами назначения.

При создании локальных сетей на основе коммутаторов все узлы сети представляют собой единый широковещательный домен, т.е. широковещательный трафик передается всем узлам сети.

При программных или аппаратных сбоях протокола верхнего уровня или сетевого адаптера возможна генерация с высокой интенсивностью ошибочных кадров с широковещательным или неизвестным адресами. При этом коммутатор передает ошибочный трафик во все сетевые сегменты. Такая ситуация называется ***широковещательным штормом***. Мосты и коммутаторы не защищают сети от широковещательных штормов.

Затопление сети широковещательными штормами может также вызываться широковещательными запросами или оповещениями, часто применяемыми современными сетевыми протоколами.

Например, ARP (Address Resolution Protocol) – протокол определения локального адреса по IP-адресу, предполагает рассылку по сети широковещательных запросов. Протокол ARP передает широковещательный запрос на канальном уровне, если требуемый локальный адрес отсутствует в имеющейся ARP-таблице сетевого устройства, или формирует широкополосное сообщение об адресации для вновь установленного или замененного сетевого оборудования.

При структуризации сети с помощью коммутаторов логические сегменты, как правило, формируются из компьютеров, расположенных на небольшом расстоянии от концентратора или коммутатора, объединяющего пользователей данного сегмента. При построении больших сетей более рационально было бы объединять рабочие станции и сервера по организационным или функциональным требованиям.

Технология виртуальных локальных сетей успешно решает указанные проблемы. Виртуальной локальной сетью VLAN (англ. Virtual Local Area Network) называется ***группа узлов*** сети, для которых любой трафик, включая широковещательный, ***полностью*** изолирован на ***канальном*** уровне от других узлов сети. Узлы объединяются в локальную сеть программными средствами, независимо от пространственного размещения этих узлов. Изменение состава виртуальной сети осуществляется без трудоемких физических переключений.

Изоляция трафика, в том числе широковещательного, осуществляется на ***канальном*** уровне при помощи коммутаторов с поддержкой технологии VLAN (стандарт 802.1q).

Устройства разных виртуальных сетей «не видят» друг друга на канальном уровне. Для связи между отдельными виртуальными сетями необходим выход на сетевой уровень и применение маршрутизаторов.

Технология виртуальных сетей обеспечивает:

- создание специализированных, функционально разделенных сетей, независимо от пространственного размещения входящих в нее рабочих станций или серверов;
- повышение производительности сети;
- препятствие для возникновения широковещательных штормов;

– локализацию широковещательного трафика, а также трафика с неизвестными групповыми или индивидуальными адресами в пределах данной виртуальной сети;
– повышение безопасности работы сетей и упрощение проведения сетевой политики по отношению к группам пользователей.

2. Технология виртуальных сетей (VLAN)

Организация виртуальных сетей требует специальной настройки портов коммутаторов.

В зависимости от структуры исходной сети в технологии VLAN применяются различные способы настройки коммутаторов

2.1. Организация VLAN в компьютерных сетях с простой топологией

При организации VLAN на ***одном*** коммутаторе порты этого коммутатора распределяются между создаваемыми виртуальными сетями, а в таблицу коммутации вводится дополнительный столбец для индексов VLAN_ID, определяющих принадлежность порта к определенной VLAN. Коммутируемые кадры могут передаваться только между портами, относящимися к одной виртуальной сети.

Порты и подключенные к ним сетевые узлы, входящие в одну виртуальную локальную сеть, используют отдельную часть таблицы коммутации.

Такой метод организации виртуальных сетей называется методом ***группирования портов.*** Группирование портов, как правило, осуществляется вручную сетевым администратором.

Организация VLAN методом группирования портов на одном коммутаторе показана на рис. 3.1.

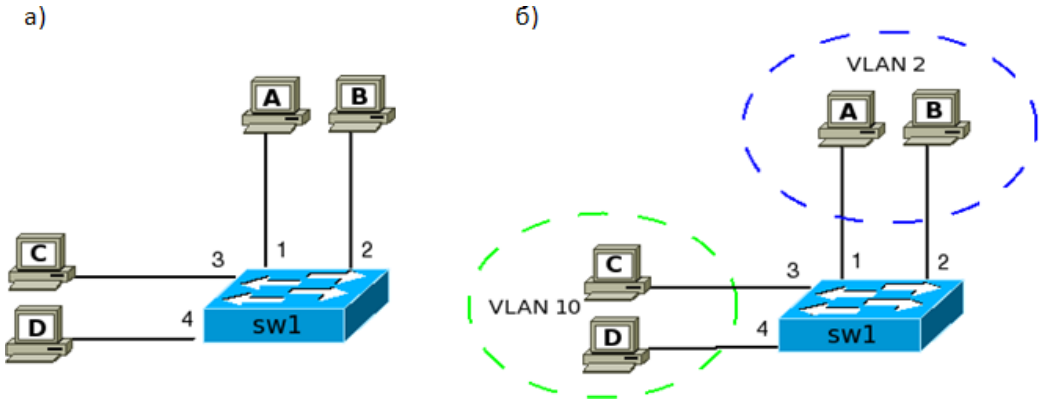


Рис. 3.1. Организация VLAN на одном коммутаторе: а – схема исходной сети (таблица коммутации коммутатора представлена в табл. 3.1); б – сеть, разделенная на две VLAN (таблица коммутации коммутатора представлена в табл. 3.2))

Таблица 3.1. Таблица коммутации до формирования VLAN

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	1	A

Таблица 3.2. Таблица коммутации с VLAN

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	2	A

2	1	B
3	1	C
4	1	D

2	2	B
3	10	C
4	10	D

Для организации VLAN методом группирования портов в компьютерных сетях с ***несколькими*** коммутаторами необходимо связать коммутаторы, содержащие порты одной VLAN, соединительными линиями. При этом чтобы устранить переходы трафика между виртуальными сетями, ***каждая*** виртуальная сеть должна иметь ***собственные*** соединительные линии.

Организация VLAN методом группирования портов на двух коммутаторах показана на рис. 3.2.

Коммутаторы S1 и S2 соединены линиями «10 – 9» для VLAN 2 и «11 – 12» для VLAN 10.

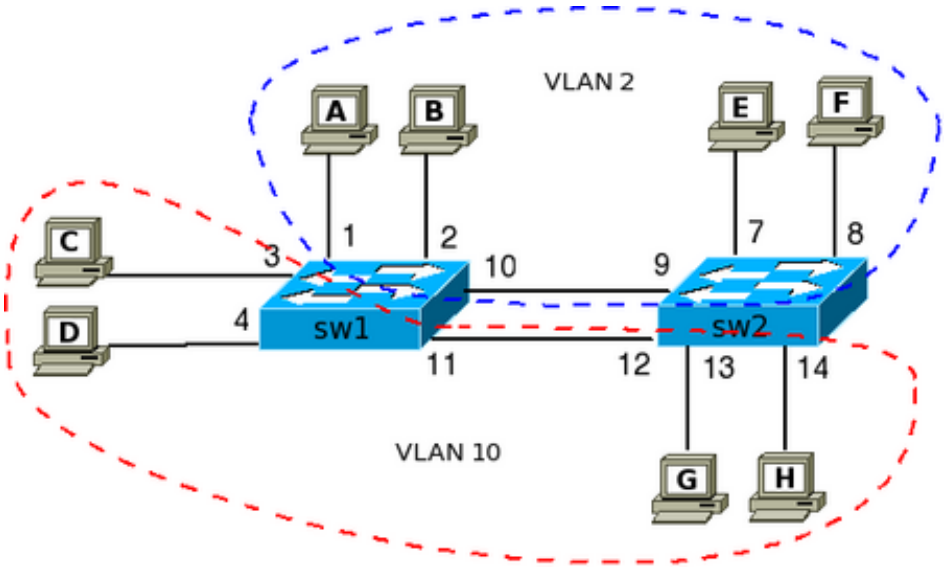


Рис.3.2. Организация VLAN на двух коммутаторах методом группирования портов

Таблица 3.3 - Таблица коммутации SW1

Порт коммутатора	VLAN ID	MAC-адрес компьютера
1	2	A
2	2	B
10	2	E
10	2	F
3	10	C
4	10	D

Таблица 3.4 - Таблица коммутации SW2

Порт коммутатора	VLAN ID	MAC-адрес компьютера
7	2	E
8	2	F
9	2	A
9	2	B
13	10	G
14	10	H

11	10	G
11	10	H

12	10	C
12	10	D

Применение данного метода требует избыточных связей между коммутаторами. При увеличении количества коммутаторов в исходной сети быстро возрастает число соединительных линий и существенно увеличивается объем работ сетевого администратора по организации и изменению состава виртуальных сетей.

Поэтому группирование портов применяется для организации VLAN лишь в простых компьютерных сетях, использующих один-два коммутатора.

2.2. Организация VLAN в сложных компьютерных сетях

Компьютеры и другие оконечные устройства, подключенные к ***различным коммутаторам***, могут объединяться в виртуальные сети при помощи специальных меток, вводимых в передаваемые кадры (стандарт IEEE 802.1Q).

Все порты коммутаторов разделяются на две группы:

- порты ***доступа*** ***(***англ. ***access)***, подключающие оконечные устройства (компьютеры, серверы, принтеры и пр.) к коммутатору;
- порты ***линий связи (***англ. ***trunk)***, соединяющие коммутаторы между собой.

Порты ***доступа*** коммутаторов, как и ранее, распределяются по создаваемым виртуальным сетям.

Получив от оконечного устройства кадр для передачи по сети Ethernet, оборудование портов доступа вводит в кадр ***специальные метки,*** свидетельствующие о принадлежности данного кадра к ***определенной*** виртуальной сети. Кадр с такой меткой называется «тегированным» - помеченным (англ. Tag – ярлык, метка). Внутри коммутатора передаются только тегированные кадры.

Коммутатор продвигает кадр только между портами, имеющими ***общий*** тег, т.е. входящими в одну виртуальную сеть.

При передаче коммутированного кадра получателю информации на конечный сетевой узел, порт доступа изымает из кадра ранее введенный тег, и сетевые пользователи получают исходные информационные кадры без каких-либо следов тегирования.

Порты доступа работают в режиме ***access.***

В отличие от портов доступа, порты, подключенные к линиям связи между коммутаторами, могут принимать и передавать кадры ***различных*** виртуальных сетей.

Наличие меток в передаваемых кадрах позволяет использовать ***общие*** соединительные линии между коммутаторами для передачи кадров нескольких виртуальных сетей при обеспечении изоляции трафика каждой сети.

Порты линий связи между коммутаторами работают в режиме ***trunk.***

По умолчанию все конечные пользователи и порты коммутаторов относятся к исходной сети VLAN1.

При формировании виртуальных сетей на коммутаторах порты ***доступа*** вводятся в режим работы access и распределяются между различными виртуальными сетями, получая соответствующее значение идентификатора для каждого порта.

Порты линий связи между коммутаторами вводятся в режим работы trunk. Такие порты получают ***несколько*** значений идентификаторов, соответствующих виртуальным сетям, трафик которых должен передаваться по данной линии связи.

Организация VLAN на основе тегирования портов и использования общей линией связи между коммутаторами показана на рис.3.3. Порты 21 и 22 – транкинговые порты, имеющие идентификаторы VLAN_2 и VLAN_10.

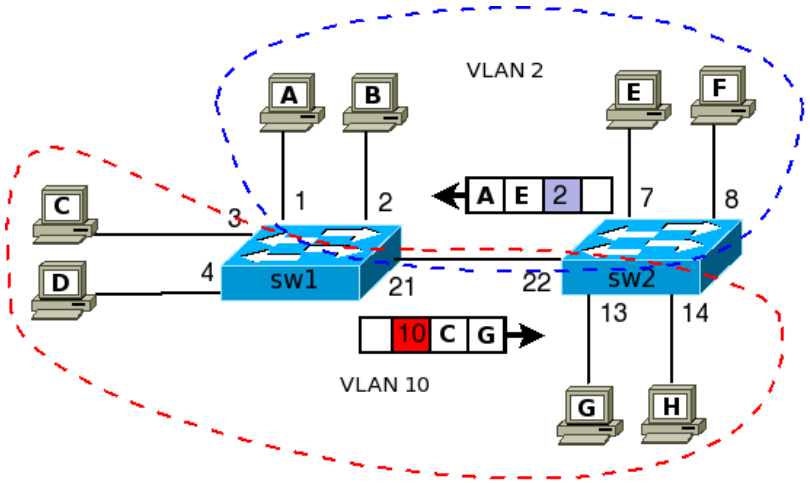


Рис. 3.3. Организация VLAN путем тегирования передаваемых кадров по стандарту IEEE 802.1Q.

В лабораторной работе предлагается создать VLAN-ы на сети, состоящей из трех коммутаторов, порты которых работают в режимах access и trunk.

При выполнении работы необходимо:

- построить исходную компьютерную сеть;
- провести конфигурацию коммутаторов;
- создать виртуальные сети;
- установить режимы access и trunk для портов коммутаторов;
- проанализировать адресные таблицы коммутаторов;
- проверить прохождение информационных пакетов в преобразованной сети.

3. Построение сети на основе виртуальных локальных сетей в пакете Cisco Packet Tracer

3.1. Создание модели сети

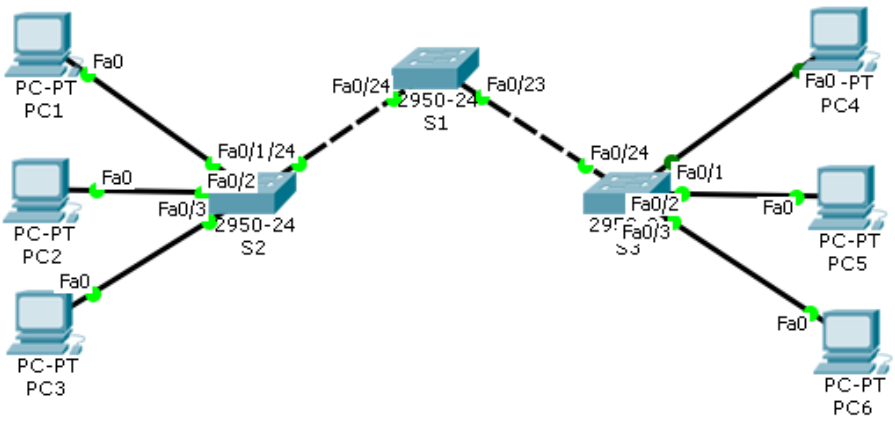


Рис. 3.4. Схема исходной компьютерной сети

В исходной сети, показанной на рис. 3.4., необходимо организовать три виртуальные локальные сети:

- VLAN_10, в которую входят PC1 и PC4;
- VLAN_20, в которую входят PC2 и PC5;
- VLAN_30, в которую входят PC3 и PC6.

Откройте Cisco Packet Tracer и создайте сеть, показанную на рис. 3.4. При соединении устройств используйте типы кабелей, соответствующие схеме. Напоминаем, что компьютеры принято подключать к коммутаторам через порты с малыми номерами (fa0/1, fa0/2 и fa0/3), а для связей между коммутаторами обычно используются порты с большими номерами (fa0/24 и fa0/23).

3.2. Настройка компьютеров

Используя окно IP Configuration в окне Desktop компьютера, задайте компьютерам ip-адреса, указанные в таблице 1.

Таблица 3.5.

Устройство	VLAN	IP-адрес	Маска
PC1	10	172.17.10.21	255.255.0.0
PC2	20	172.17.20.22	255.255.0.0
PC3	30	172.17.30.23	255.255.0.0
PC4	10	172.17.10.24	255.255.0.0
PC5	20	172.17.20.25	255.255.0.0
PC6	30	172.17.30.26	255.255.0.0

С помощью команды **ping** в режиме командной строки (Command Prompt) для одного из компьютеров, например PC1, проверьте доступность всех компьютеров сети.

3.3. Начальная конфигурация коммутаторов

Начальная конфигурация коммутаторов в данной работе не отличается от конфигурации, рассмотренной в лабораторной работе 2. Используя вкладку командной строки (CLI) в окне каждого коммутатора, выполните следующие команды на коммутаторах S1, S2 и S3:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
```

```
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]? [OK]
Building configuration...
[OK]
```

Не забудьте дать коммутаторам разные имена.

3.4. Проверка состояния сетевых интерфейсов

Проверьте правильность подключения портов коммутатора, выполнив на S2 в привилегированном режиме команду show **ip interface brief**.

```
S2#show ip interface brief
Interface              IP-Address    OK? Method Status                Proto
FastEthernet0/1        unassigned    YES manual up                    up
FastEthernet0/2        unassigned    YES manual up                    up
FastEthernet0/3        unassigned    YES manual up                    up
FastEthernet0/23       unassigned    YES manual down                  down
 …
FastEthernet0/24       unassigned    YES manual up                    up
Vlan1                  unassigned    YES manual administratively down down
```

Убедитесь, что порты, к которым подключены компьютеры и другие коммутаторы находятся в состоянии up.

Проделайте аналогичные действия на коммутаторах S1 и S3.

3.5. Отключение дополнительных протоколов

Для упрощения таблиц коммутации следует отключить ряд протоколов, работающих на коммутаторах.

В режиме глобального конфигурирования отключите cdp и spanning-tree (пример для S1):

```
S1(config)#no cdp run
S1(config)#no spanning-tree vlan 1-4096
```

Установите запрет на отправку пакетов dtp через этот интерфейс (пример для S1):

```
S1(config)#interface fa0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
```

Выполните эту команду на всех интерфейсах, соединяющих коммутаторы (для S1 это fa0/24 и fa0/23) .

В режиме привилегированного пользователя произведите очистку таблиц коммутации на всех коммутаторах:

```
S1#clear mac-address-table
```

3.6. Проверка таблиц коммутации

Сгенерируйте трафик при помощи команды ping, проверив доступность всех компьютеров с PC1.

Изначально все компьютеры входят в одну локальную сеть (по умолчанию на коммутаторах cisco это VLAN 1). Убедитесь в этом, выполнив команду #show mac-address table в привилегированном режиме.

```
S1#show mac-address-table
      Vlan    Mac Address       Type        Ports
      ----    -----------       --------    -----

         1    0004.9a19.1418    DYNAMIC     Fa0/23
         1    00d0.bc4b.b818    DYNAMIC     Fa0/24
         1    0001.c98d.9d66    DYNAMIC     Fa0/23
         1    0002.1656.528a    DYNAMIC     Fa0/24
         1    0001.9614.d392    DYNAMIC     Fa0/23
         1    00d0.bce5.234a    DYNAMIC     Fa0/24
         1    0001.97e1.8486    DYNAMIC     Fa0/24
         1    0001.c958.a094    DYNAMIC     Fa0/23
```

Важно! Если долго (более 10 мин) не было обмена пакетами между устройствами (компьютерами), таблицы коммутации могут очиститься. Для их восстановления необходимо снова “пропинговать” все компьютеры в сети.

3.7. Создание виртуальных сетей на коммутаторах

Создайте новые виртуальные сети vlan_10, vlan_20 и vlan_30 на каждом коммутаторе (S1, S2 и S3), введя команды во вкладке CLI в привилегированном режиме.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name vlan_10
S1(config-vlan)exit
S1(config)#vlan 20
S1(config-vlan)#name vlan_20
S1(config-vlan)exit
S1(config)#vlan 30
S1(config-vlan)#name vlan_30
S1(config-vlan)#exit
```

Проверьте состояние vlan-ов, выполнив в привилегированном режиме команду **show vlan brief**:

```
S1#show vlan brief
VLAN Name                         Status    Ports
---- ---------------------------- --------- ---------------------------
1    default                      active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                            Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                            Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                            Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   vlan_10                      active
```

```
20   vlan_20                  active
30   vlan_30                  active
1002 fddi-default             active
1003 token-ring-default       active
1004 fddinet-default          active
1005 trnet-default            active
```

Изучите вывод команды. Убедитесь, что на коммутаторе организованы 10, 20, 30 vlan.

Обратите внимание, что все порты коммутатора находятся на данный момент в vlan с номером 1. Виртуальные сети с номерами 1, 1002, 1003, 1004, 1005 были автоматически созданы коммутатором и используются для служебных задач.

3.8. Настройка виртуальных сетей на портах коммутаторов

В режиме конфигурации интерфейсов сконфигурируйте порты коммутаторов, подключенные к компьютерам, с учетом номеров портов и vlan-ов.

На коммутаторе S2 переведите порты, соединяющие S2 с коммутатором S1, в режим транка при помощи команды **switchport mode trunk**, а затем добавьте в транк необходимые VLANы при помощи команды **switchport trunk allowed vlan add <vlan_id>**:

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int fa0/1
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#int fa0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#int fa0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#int fa0/24
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan add 10
S2(config-if)#switchport trunk allowed vlan add 20
S2(config-if)#switchport trunk allowed vlan add 30
S2(config-if)#no shutdown
S2(config-if)#exit
```

В привилегированном режиме снова выполните команду **show vlan brief**:

```
S2#show vlan brief

VLAN Name                         Status    Ports
---- ---------------------------- --------- -------------------------------
1    default                      active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                            Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                            Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                            Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                            Fa0/20, Fa0/21, Fa0/22,Fa0/23
10   vlan_10                      active    Fa0/1
20   vlan_20                      active    Fa0/2
30   vlan_30                      active    Fa0/3
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Обратите внимание на изменения в выделенных строчках.

Для вывода состояния транков используйте команду **show interfaces trunk** в привилегированном режиме:

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/24      10,20,30

Port        Vlans allowed and active in management domain
Fa0/24      10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      10,20,30
```

Из вывода команды видно, что виртуальные сети 10,20,30 включены в режиме транка на интерфейсе Fa0/24

Конфигурация для S1 будет выглядеть следующим образом:

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

S1(config)#interface fa0/24
S1(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/24,
changed state to down
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/24,
changed state to up
S1(config-if)#switchport trunk allowed vlan add 10
S1(config-if)#switchport trunk allowed vlan add 20
S1(config-if)#switchport trunk allowed vlan add 30
S1(config-if)#exit
S1(config)#interface fa0/23
S1(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/23,
changed state to down
%LINEPROTO-5-UPDOWN:  Line  protocol  on  Interface  FastEthernet0/23,
changed state to up
S1(config-if)#switchport trunk allowed vlan add 10
S1(config-if)#switchport trunk allowed vlan add 20
S1(config-if)#switchport trunk allowed vlan add 30
S1(config-if)#no shutdown
S1(config-if)#exit
```

Аналогичным образом сконфигурируйте порты коммутатора S3.При помощи команд #**show running config**, #**show vlan brief** и #**show interfaces trunk** проверьте конфигурацию виртуальных сетей на коммутаторах S1 и S3.

3.9. Проверка работы виртуальных сетей

При помощи команды ping снова проверьте с компьютера PC1 доступность всех компьютеров сети. Как изменилась доступность конечных узлов по сравнению с результатами, полученными в п. 3.4? Проверьте доступность узлов сети с PC2, PC3.

Просмотрите таблицу mac-адресов на каждом коммутаторе, для этого в привилегированном режиме выполните команду **show mac-address-table:**

```
S1#show mac-address-table
```

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.c98d.9d66    DYNAMIC     Fa0/23
  10    0002.1656.528a    DYNAMIC     Fa0/24
  20    0001.9614.d392    DYNAMIC     Fa0/23
  20    00d0.bce5.234a    DYNAMIC     Fa0/24
  30    0001.97e1.8486    DYNAMIC     Fa0/24
  30    0001.c958.a094    DYNAMIC     Fa0/23
```

Определите физические устройства, соответствующие mac-адресам, указанным в таблице в окне CLI.

3.10. Создание виртуальных интерфейсов и назначение IP-адресов

Основным отличием коммутаторов от маршрутизаторов является том, что, как правило, на маршрутизаторах IP-адреса назначаются на физических интерфейсах, а у коммутаторов – на виртуальных интерфейсах, привязанных к существующим в коммутаторе виртуальным сетям. Так, например, для виртуальной сети **10** можно создать виртуальный интерфейс **vlan10**.

Создайте и сконфигурируйте на коммутаторах в виртуальной сети 10 интерфейсы для сети управления (используйте данные из таблицы 3.6):

Таблица 3.6 – IP адреса коммутаторов

Название устройства	Interface	IP	Mask
S1	Vlan10	172.17.10.11	255.255.0.0
S2	Vlan10	172.17.10.12	255.255.0.0
S3	Vlan10	172.17.10.13	255.255.0.0

```
S2(config)#interface vlan 10
S2(config-if)#ip address 172.17.10.12 255.255.0.0
S2(config-if)#no shutdown
```

Сконфигурируйте основной шлюз коммутаторов командой **ip default-gateway 172.17.10.1** (необходимо для доступа к коммутатору из другой сети)

```
S2(config)ip default-gateway 172.17.10.1
```

Выполните в привилегированном режиме команду **show ip interface brief:**

```
S2#show ip interface brief
Interface          IP-Address      OK? Method Status            Protocol
FastEthernet0/1    unassigned      YES manual up                  up
FastEthernet0/2    unassigned      YES manual up                  up
FastEthernet0/3    unassigned      YES manual up                  up
…
FastEthernet0/23   unassigned      YES manual down                down
```

```
FastEthernet0/24   unassigned      YES manual up                    up
Vlan1              unassigned      YES manual administratively down down
Vlan10             172.17.10.11    YES manual up                    up
```

Обратите внимание на наличие виртуальных интерфейсов VLan1 и Vlan10.

Аналогичным образом создайте и настройте виртуальные интерфейсы на коммутаторах S1 и S3, используя следующие адреса.

Проверьте с PC1, PC2 и PC3 доступность виртуальных интерфейсов коммутаторов. Почему с одних ПК виртуальные интерфейсы доступны, а с других недоступны, и как это можно использовать в сети?

3.11. Проверка и сохранение конфигурации

Проверьте конфигурацию коммутатора, выполнив команду **show running-config**.

Сохраните конфигурация коммутатора, выполнив в привилегированном режиме команду **copy running-config startup-config**.

4. Контрольные вопросы

1. Как изменилась доступность узлов сети после добавления виртуальных сетей?
2. Как изменилась таблица коммутации?
3. Чем отличается вывод команд show vlan, show vlan brief, show interface trunk?
4. Какие преимущества дает использование виртуальных сетей (VLAN)?
5. Почему VLAN 10 в работе можно назвать служебным?

5. Задание для самостоятельной работы

1. Получите у преподавателя pka-файл с персональным заданием. Откройте этот файл в программе Cisco Packet Tracer и следуйте инструкциям, которые появятся после открытия файла.
2. Ознакомьтесь с исходными данными и выполните задание.
3. Сохраните конфигурацию всех сетевых устройств.
4. Сохраните изменения в pka-файле и отправьте его преподавателю в качестве отчета о выполнении самостоятельной работы.

Важные замечания по выполнению домашнего задания:

- Обратите внимание на то, что пользователи различных виртуальных сетей могут иметь одинаковые внутренние IP-адреса. Проведите базовые настройки коммутаторов.
- Записи адресов в таблицах коммутации имеют динамический характер и *удаляются* программой CPT, если трафик в данной виртуальной сети отсутствует более 10 минут. Поэтому просматривать таблицы mac-адресов следует *непосредственно* после генерации трафика в сети (например, проверки доступности узлов при помощи команды ping).

6. Рекомендуемые материалы

1. М.А.Плоткин. Лекции по курсу «Сети связи и системы коммутации». Тема 4 Технологии локальных вычислительных сетей. Раздел «Технология виртуальных локальных сетей (VLAN)».

2. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г. Глава 14 Интеллектуальные функции коммутаторов. Раздел «Виртуальные локальные сети», стр.467-474.
3. С. Пахомов. Возможности современных коммутаторов по организации виртуальных сетей. КомпьютерПресс 4, 2005 (http://www.cpress.ru/).
4. Интернет ресурс http://xgu.ru

Лабораторная работа №4.
Построение составной сети с бесклассовой адресацией

1. Введение

Для организации локальной компьютерной сети Интернет-провайдер предоставляет в распоряжение пользователя некоторую, как правило, непрерывную область адресов.

Область выделенных адресов либо соответствует одному из стандартных классов IP-адресов, либо задается определенной адресной маской. В любом случае все адреса выделенной области имеют одинаковый ***префикс***, т.е. одинаковую цифровую последовательность в старших разрядах.

Сетевой администратор может управлять предоставленным ему адресным пространством, обеспечивая гибкую логическую структуризацию вновь создаваемой сети.

Гибкая структуризация сети использует бесклассовую адресацию, основанную на переменной длине ***маски подсети*** (англ. VLSM - Variable Length Subnet Mask). Маска указывается в настройках каждого сетевого устройства совместно с IP-адресом и определяет границу между номером сети и номером узла. Двоичная запись маски имеет единицы в разрядах, определяющих номер сети, и нули в разрядах, соответствующих номеру узла.

Структуризация позволяет формировать пользовательские сегменты (подсети) в целях:

- ***разбиения*** собственной сети на несколько подсетей (subnetting) для локализации трафика и повышения надежности без получения от поставщика услуг дополнительных номеров сетей;
- ***объединения*** адресных пространств имеющихся у него нескольких сетей (supernetting) с целью упрощения внутрисетевого обмена, уменьшения объема таблиц маршрутизации и повышения производительности сетей.

Количество адресов в подсети не равно количеству возможных узлов. Нулевой IP адрес резервируется для идентификации ***подсети***, последний — в качестве ***широковещательного*** адреса. Поэтому в сетях максимальное количество адресов узлов в сети на два меньше, чем общее количество адресов.

Рассмотрим некоторые случаи разделения адресного пространства на отдельные подсети.

Пример 1

Сетевому пользователю выделено адресное пространство 226.205.50.0/24. Требуется организовать 4 подсети, наибольшая из которых насчитывает 40 узлов. Следует учесть возможный рост числа узлов на 20%.

Для организации 4 подсетей увеличим длину префикса на два разряда. При этом расширенный сетевой префикс (постоянная часть адреса) будет содержать 24+2 = 26 разрядов. Переменная часть адресов в каждой подсети обеспечивается 6 оставшимися битами, что с учетом адреса сети и широковещательного адреса позволяет создать подсеть с 26 - 2 = 62 узлами; такое адресное пространство достаточно для работы самой большой подсети.

Для каждой подсети нижняя граница адресного пространства смещается на сумму численных значений кодовых символов, входящих в префикс этой подсети. При заданном адресном пространстве префиксы подсетей размещаются в двух старших разрядах 4-го байта.

Установим для подсети «0» префикс 00, для подсети «1» – префикс 01, для подсети «2» - префикс 10 и для подсети «3» - префикс 11. Тогда адресное пространство для узлов подсети «0» начнется со значения 226.205.50.1, адресное пространство для узлов подсети «1» - со значения 226.205.50.65, для подсети «2» - со значения 226.205.50.129 и для подсети «3» - со значения 226.205.50.193

Результаты расчета адресов подсетей сведены в таблицу 4.1.

Таблица 4.1.

Название сети	IP-адрес сети	Сетевой префикс	Префикс	Диапазон адресов узлов подсети	Широковещательны адрес
Основная сеть	226.205.50.0/24	11100010.11001101.00110010	-	–	–
Подсеть 0	226.205.50.0/26	11100010.11001101.00110010.00	00	226.205.50.1 - 226.205.50.62	226.205.50.63
Подсеть 1	226.205.50.64/26	11100010.11001101.00110010.01	01	226.205.50.65 - 226.205.50.126	226.205.50.127
Подсеть 2	226.205.50.128/26	11100010.11001101.00110010.10	10	226.205.50.129 - 226.205.50.190	226.205.50.191
Подсеть 3	226.205.50.192/26	11100010.11001101.00110010.11	11	226.205.50.193 - 226.205.50.254	226.205.50.255

В данном примере было рассмотрено формирование подсетей равного размера.

На практике часто требуется организовать подсети неравного размера. Например, кроме основных подсетей, для связи маршрутизаторов необходимы соединительные подсети из небольшого числа адресов.

Пример 2

Пользователю выделен блок адресов 192.144.128.0/22. Требуется организовать три подсети по 50 узлов, выделить адреса для двух пар маршрутизаторов и оставить некоторый резерв.

Разделим адресное пространство на 4 одинаковые подсети, выделив 2 бита для нумерации этих подсетей: подсеть S0(00), подсеть S1(01), подсеть S2(10) и подсеть S3(11). Каждой подсети соответствует 256 адресов.

В пространстве подсети S3 дополнительно организуем две подсети S3-1 и S3-2, каждая на 4 адреса для подключения маршрутизаторов.

Результаты формирования адресного пространства приведены в таблице 4.1.

Таблица 4.2.

Адресный пул поставщика	Префикс поставщика (22 разряда)	Наименование подсети	Основной префикс пользователя (2 разряда)	Дополнительный. префикс пользователя (6 разрядов)	Количество адресов подсети
210= 1024 адреса	11000000.10010000.100000	S0	00	-	256
	11000000.10010000.100000	S1	01	-	256
	11000000.10010000.100000	S2	10	-	256
	11000000.10010000.100000	S3, включая S3-1 S3-2	11 11 11	- 000000 000001	256, в том числе S3-1 – 4 адреса; S3-2 – 4 адреса; резерв – 248 адресов

Использование масок переменной длины позволило сформировать подсети с ***перекрывающимися*** адресными пространствами. Так, адресные пространства подсетей S3-1 и S3-2 разместились внутри адресного пространства подсети S3.

Подключение сети пользователя к глобальной сети осуществляется сетевым провайдером (Internet Service Provider), как правило, через отдельный маршрутизатор (роутер), обозначаемый как $\mathbf{R_{ISP}}$.

Возможная структура сети пользователя, соответствующая условиям данного примера и проведенному разделению адресного пространства, показана на рис.4.1.

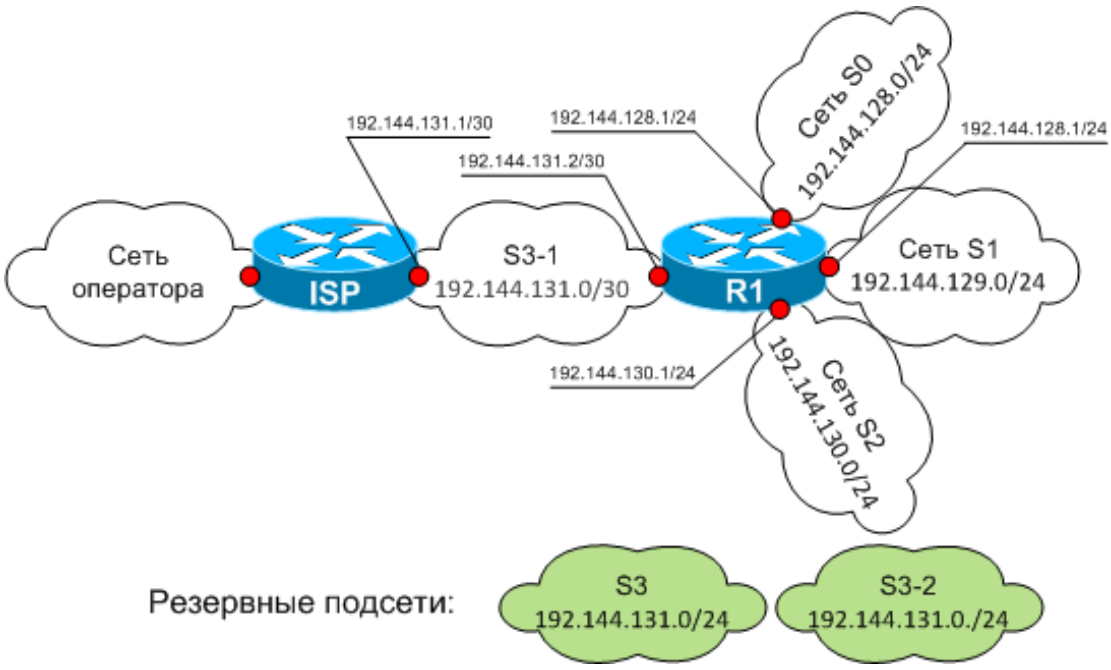


Рис. 4.1 - Сконфигурированная сеть пользователя

Использование бесклассовой технологии позволяет гибко формировать в сети Интернет отдельные адресные пространства (домены); при этом информация о внутренних подсетях используется только в пределах этого адресного пространства. Вне такого пространства всем внутренним подсетям, имеющим общий префикс, соответствует одна запись адреса назначения в таблицах маршрутизации.

При передаче информации от внешнего источника к данному домену все подсети этого адресного пространства фактически объединяются (агрегатируются) в одну общую сеть, что существенно сокращает время обработки передаваемых сообщений, особенно в магистральных маршрутизаторах.

Агрегатирование подсетей может применяться и при передаче информации внутри домена. Используя одинаковые символы в старших разрядах префикса, можно производить объединение нескольких подсетей для повышения производительности маршрутизаторов внутри домена.

При проведении лабораторной работы необходимо:

- разделить адресное пространство исходной сети между несколькими подсетями;
- присвоить адреса сетевым интерфейсам компьютеров и маршрутизаторов;
- собрать сеть с заданной топологией;
- провести настройку используемых сетевых устройств;
- проверить работу составной сети;
- выполнить индивидуальное задание.

2. Расчет подсетей

Разделите исходную сеть класса С **198.133.219.0/24** на 16 подсетей, используя 4 старших бита последнего байта заданного адреса. Определите маску для новых подсетей. В первых двух подсетях LAN_1 и LAN_2 (Рис. 4.2) определите диапазон адресов, доступных для использования, адрес сети и широковещательный адрес.

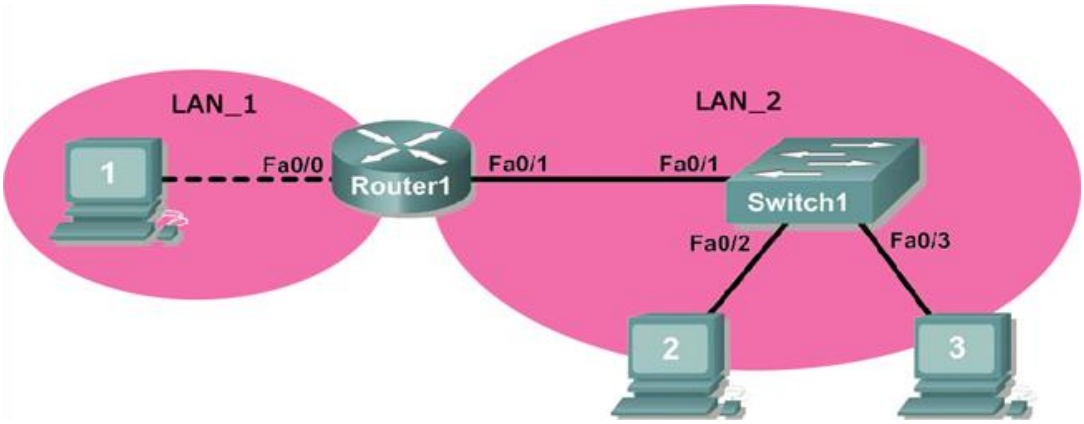


Рис. 4.2- Схема сети с указанием двух подсетей

Портам маршрутизатора присвойте первые адреса, а портам сетевых карт компьютеров – последние адреса в подсетях.

Результаты расчетов занесите в таблицу 4.3.

Таблица 4.3.

Название устройства	Интерфейс	Подсеть	IP-адрес	Маска	Шлюз
R	Fa0/0	LAN_1			-
PC1	Eth0	LAN_1			
R	Fa0/1	LAN_2			-

PC2	Eth0	LAN_2			
PC3	Eth0	LAN_2			

3. Создание модели сети в программе Cisco Packet Tracer

Откройте Cisco Packet Tracer и создайте сеть со структурой, приведенной на рис. 4.3. Для этого используйте устройства, указанные в таблице 4.4.

Таблица 4.4.

Группа устройств	Название устройства	Кол-во
Маршрутизаторы	1841	1
Коммутаторы	2950-24	1
Конечные устройства	PC-PT (компьютер)	3

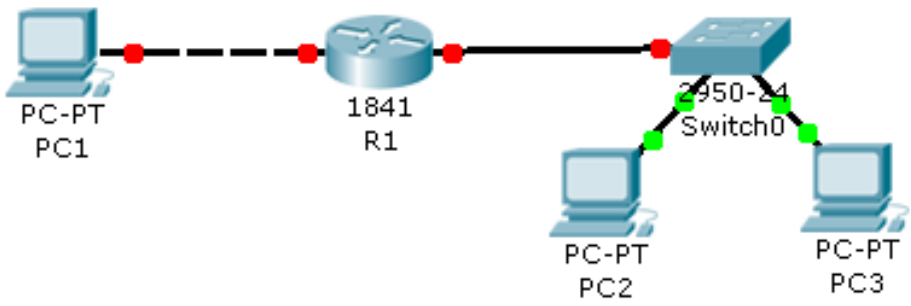


Рис. 4.3 - Модель сети в Cisco Packet Tracer

3.1. Настройка сетевых интерфейсов компьютеров

Настройте компьютеры PC1, PC2, PC3, указав IP-адрес, маску и шлюз из таблицы 4.3. Настройка IP-адресов персональных компьютеров в Cisco Packet Tracer была описана в методических указаниях к лабораторной работе №1.

3.2. Проверка настроек компьютеров

Проверьте правильность настроек сетевого интерфейса компьютера PC1, PC2, PC3, выполнив команду **ipconfig /all**. В выводе команды на экран найдите установленные ранее значения IP-адреса, маски и шлюза.

3.3. Проверка доступности узлов сети

Проверьте доступность сетевых узлов при помощи команды ping. При тестировании сети сначала необходимо проверить доступность наиболее близких узлов. Так, для PC1 необходимо сначала проверить доступность шлюза:

```
PC>ping 198.133.219.1
```

```
Pinging 198.133.219.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.133.219.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Сетевое оборудование еще не настроено, поэтому часть сетевых устройств не доступна. Последовательно выполните следующие действия:

- проверьте доступность интерфейса маршрутизатора Fa0/1 с компьютеров PC2 и PC3.
- исследуйте доступность дальних интерфейсов маршрутизатора (Fa0/0 с PC2,PC3; Fa0/1 с PC1)
- проверьте взаимную доступность PC2 , PC3 и PC1.

Объясните полученные результаты.

3.4. Начальная настройка маршрутизатора

Начальная настройка маршрутизаторов практически не отличается от настройки коммутаторов, рассмотренной в работе 2. Используя вкладку командной строки (CLI), выполните следующие команды на маршрутизаторе R1:

```
Router>enable
Router #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
SR1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]? [OK]
Building configuration...
[OK]
```

3.5. Настройка сетевых интерфейсов маршрутизатора

Настройка сетевых интерфейсов маршрутизаторов также не отличается от настройки интерфейсов коммутаторов, однако на маршрутизаторах IP адрес задается на интерфейсах, соответствующих физическим сетевым портам устройства, а не на виртуальных интерфейсах (interface VLAN), как это принято в коммутаторах. Для настройки сетевого интерфейса на маршрутизаторе необходимо:

1. Из привилегированного режима перейти в режим конфигурирования при помощи команды **configure terminal.**
2. Выбрать физический интерфейс, который вы планируете настраивать. Зайти в режим конфигурирования этого интерфейса, выполнив команду **interface <Название интерфейса>**. В нашем случае это интерфейсы **FastEthernet0/0** и **FastEthernet0/1** (список доступных интерфейсов можно получить в привелигированном режиме при помощи команды #show ip interface brief).
3. В режиме конфигурирования интерфейса задать описание интерфейса при помощи команды **description <любой текст>**. Действие не является обязательным, но делать это настоятельно рекомендуется.
4. В режиме конфигурирования задать сетевой адрес. Для задания IP адреса в IOS используется команда **ip address <IP> mask <MASK**>, выполняемая в режиме конфигурирования интерфейса.
5. Включить сетевой интерфейс, для этого в режиме конфигурирования интерфейса необходимо выполнить команду **no shutdown.**

Ниже приведен пример конфигурирования интерфейса FastEthernet 0/0. При включении интерфейса выводится диагностическое сообщение о “поднятии” интерфейса FastEthernet0/0 (выделено серым):

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#description --< link to LAN_1> --
R1(config-if)#ip address 198.133.219.1 255.255.255.240
R1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

R1(config-if)#
```

Аналогичным образом сконфигурируйте интерфейс fastEthernet 0/1:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/1
R1(config-if)#description --< link to LAN_2> --
R1(config-if)#ip address 198.133.219.17 255.255.255.240
R1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

R1(config-if)#
```

1.6 Проверка настройки маршрутизатора

Проверьте правильность конфигурации маршрутизатора, выполнив в привилегированном режиме команду #**show run**:

```
R1#show running-config
Building configuration...
…
!
interface FastEthernet0/0
description --< link to LAN_1> --
ip address 198.133.219.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet0/1
description --< link to LAN_2 >--
ip address 198.133.219.17 255.255.255.240
duplex auto
speed auto
!
…
```

Серым выделены изменения, которые должны появиться в настройках.

Затем выполните в привилегированном режиме команду просмотра состояния интерфейсов **show ip interface brief**:

```
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0    198.133.219.1    YES manual up up
FastEthernet0/1    198.133.219.17   YES manual up up
Vlan1                unassigned        YES unset administratively down
down
```

Убедитесь, что интерфейсы FastEthernet0/0 и FastEthernet0/1 находятся в состоянии “up”.

1.7 Проверка работы сети

Проверьте доступность компьютеров в сети, выполнив на маршрутизаторе команду #ping:

```
R1#ping 198.133.219.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.14, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1
```

Снова проверьте доступность узлов сети с компьютера PC1. Напоминаем, что при тестировании необходимо сначала проверить доступность наиболее близких узлов и адресов, затем более дальних, постепенно приближаясь к конечному узлу. Так, для PC1 необходимо сначала проверить доступность шлюза (адрес интерфейса FastEthernet0/0):

```
PC>ping 198.133.219.1
```

```
Pinging 198.133.219.1 with 32 bytes of data:
Reply from 198.133.219.1: bytes=32 time=0ms TTL=255
Reply from 198.133.219.1: bytes=32 time=0ms TTL=255
Reply from 198.133.219.1: bytes=32 time=10ms TTL=255
Reply from 198.133.219.1: bytes=32 time=10ms TTL=255

Ping statistics for 198.133.219.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 5ms
```

Затем проверьте доступность дальнего интерфейса маршрутизатора fastEthernet0/1. После этого можно проверить доступность компьютеров PC2 и PC3.

1.8Просмотр arp-таблиц

Просмотрите arp-таблицу маршрутизатора, выполнив в привилегированном режиме команду **show arp**:

```
    R1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
    Internet    198.133.219.1                       -      0005.5ED4.7201    ARPA
FastEthernet0/0
Internet  198.133.219.14          8   00E0.8F2B.D86D  ARPA   FastEthernet0/0
Internet  198.133.219.17          -   0005.5ED4.7202  ARPA   FastEthernet0/1
Internet  198.133.219.29          6   00E0.8FA5.290C  ARPA   FastEthernet0/1
Internet  198.133.219.30          7   0030.F232.A79B  ARPA   FastEthernet0/1
```

Затем просмотрите arp-таблицу на компьютерах PC1, выполнив команду **arp –a** (рис. 4. 4).

```
PC>arp -a
  Internet Address      Physical Address      Type
  198.133.219.1         0005.5ed4.7201        dynamic

PC>
```

Рис. 4.4. Вывод arp-таблицы с помощью команды arp –a

Объясните, почему в таблице содержатся только адреса устройств, находящихся в одной подсети с компьютером, на котором выполнялась команда, а у маршрутизаторав таблице присутствуют все адреса.

Аналогичным образом выполните следующие действия:

- Проверьте доступность шлюза с компьютеров PC2 и PC3.
- Проверьте доступность “дальнего интерфейса” маршрутизатора с компьютеров PC2 и PC3.
- Убедитесь при помощи команды ping, что компьютеров PC2, и PC3 доступен PC1.
- Проверьте доступность компьютеров с маршрутизатора.
- Изучите arp-таблицы на компьютерах и маршрутизаторе.

2. Контрольные вопросы

1. В чем заключается основное отличие между коммутатором и маршрутизатором?
2. Перечислите преимущества технологии VLSM перед классовой адресацией?
3. Что хранится в arp-таблице?
4. Для чего используются arp-таблицы?

5. Задание для самостоятельной работы

1. Получите у преподавателя pka-файл с персональным заданием. Откройте этот файл в программе Cisco Packet Tracer и следуйте инструкциям, которые появятся после открытия файла.
2. Ознакомьтесь с исходными данными и выполните задание.
3. Сохраните конфигурацию всех сетевых устройств.
4. Сохраните изменения в pka-файле и отправьте его преподавателю в качестве отчета о выполнении самостоятельной работы.

6. Рекомендуемые материалы

1. М.А. Плоткин. Лекции по курсу «Сети связи и системы коммутации» Тема 5. Технология Интернет. Раздел «Способы адресации в Интернет-сетях».
2. В.Г. Олифер и др. Компьютерные сети. 4-е издание. ПИТЕР, 2012г. Глава 15 «Адресация в стеке протоколов TCP/IP».
3. Джо Хабракен. Как работать с маршрутизаторами Cisco. Пер. с англ. – М.: ДМК Пресс. 2005.
4. Джером Ф. Димарцио. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. Символ, 2003
5. Интернет ресурс http://www.cisco.com
6. Интернет ресурс http://xug.ru

Лабораторная работа №5.
Статическая маршрутизация в компьютерных сетях

1. Введение

Транспортировка пакетов в IP-сетях осуществляется на основе информации о текущей конфигурации сети, имеющейся у маршрутизаторов и оконечных станций.

Рациональный маршрут следования пакета выбирается путем анализа данных, содержащихся в ***таблицах маршрутизации***. По результатам анализа IP-пакет, принятый маршрутизатором или сформированный в компьютере пользователя, продвигается в направлении узла-получателя сообщения.

Таблицы маршрутизации могут различаться в зависимости от фирмы-производителя и принятой операционной системы, однако, в любом случае должны содержать следующую информацию:

- адрес сети назначения с указанием маски;
- сетевой адрес следующего маршрутизатора;
- выходной порт маршрутизатора, на который должен быть направлен пакет:

– метрика маршрута, характеризующая меру предпочтения данного маршрута в соответствии с заданным критерием[9].

В зависимости от способа ввода информации в таблицу маршрутизации различают статическую и динамическую (адаптивную) маршрутизации.

При ***статической*** маршрутизации все записи в таблице имеют неизменный, статический характер и вносятся вручную администратором сети. При изменении состояния сети администратор должен внести изменения в таблицы соответствующих маршрутизаторов, чтобы обеспечить корректную работу сети.

При ***динамической*** маршрутизации все данные вносятся в таблицы маршрутизации с помощью специальных сетевых протоколов. Протоколы маршрутизации позволяют непрерывно собирать информацию о топологии межсетевых соединений и оперативно вносить в таблицы маршрутизаторов данные об изменениях связей, возникающих в сети.

В таблицах при динамической маршрутизации обычно содержится информация об интервале времени, в течение которого данный маршрут считается действительным. Это время называют временем жизни TTL (Time To Live) маршрута. Если по истечении времени жизни существование маршрута не подтверждается данными протокола маршрутизации, то маршрут считается нерабочим.

Результатом работы протоколов является согласование содержания таблиц маршрутизации у взаимодействующих маршрутизаторов.

На практике возможно совместное применение методов статической и динамической маршрутизации.

1. Статическая маршрутизация

Статическая маршрутизация – вид маршрутизации, при котором записи в таблице маршрутизации создаются и удаляются вручную сетевым администратором.

Содержание записей таблиц маршрутизации различается в зависимости от размещения сети назначения и требований конкретных пользователей.

В маршрутах к сетям, непосредственно подключенным к портам данного маршрутизатора, сетевой администратор указывает адрес выходного порта без ссылки на какой-либо другой маршрутизатор.

Известные маршруты к конкретным удаленным сетям получают номер соответствующего выходного порта и адрес следующего маршрутизатора.

Для отдельного пользователя возможно назначение специфического маршрута, отличающегося от типового маршрута данной сети; при этом в таблицу заносится полный IP-адрес узла назначения.

Пакеты, адресованные пользователям сетей, данные о которых отсутствуют в графе «сеть назначения», направляются к одному из соседних маршрутизаторов, через который обеспечивается доступ к этим сетям. Такой маршрутизатор называется ***маршрутизатором по умолчанию.***

При статической маршрутизации каждый маршрутизатор принимает решение “самостоятельно”, без какого-либо анализа таблиц соседних маршрутизаторов.

Все записи в таблице имеют статус «статических» с условно бесконечным сроком действия. При возникновении изменений в сети администратор должен оперативно

[9] Наиболее часто применяется критерий, учитывающий количество промежуточных маршрутизаторов (хопов) в данном маршруте. Кроме того, используются метрики, соответствующие признакам D, T и R в поле сервиса IP-пакета (D – пропускная способность, T – вносимая задержка, R – надежность маршрута).

скорректировать таблицы маршрутизации для тех маршрутизаторов, у которых произошедшие изменения требуют смены маршрутов следования пакетов.

Статическая маршрутизация осуществляется администратором сети без участия каких-либо протоколов маршрутизации и обычно применяется в сетях с простой топологией, объединяющих небольшое (1-3) число подсетей и имеющих доступ к сети Интернет через шлюз, являющийся шлюзом по умолчанию.

Достоинства статической маршрутизации:

- простота отладки и конфигурирования в малых компьютерных сетях;
- экономия аппаратных ресурсов маршрутизатора;
- отсутствие динамической нагрузки на сеть.

Основным ***недостатком*** статической маршрутизации является чувствительность к повреждениям линий связи. Если маршрутизатор выходит из строя или канал связи становится недоступным, маршрутизатор не реагирует на неисправность, статический маршрут остается активным, при этом другие маршрутизаторы в сети будут продолжать передавать данные по недоступному маршруту.

В малых сетях (например, с тремя локальными сетями, соединенными между собой маршрутизаторами) подобные ситуации могут оперативно решаться администратором. Однако, при масштабировании сети существенно возрастает трудоемкость коррекции таблиц маршрутизации. Поэтому в крупных сетях более предпочтительным оказывается использование специальных протоколов маршрутизации, обеспечивающих автоматический ввод и коррекцию данных в таблицы маршрутизаторов.

Маршруты статической маршрутизации вводятся командой ***ip route***.

Задание порта по умолчанию производится командой ***ip route 0.0.0.0 0.0.0.0 interface/next hop ip address***.

Просмотр текущего состояния таблицы маршрутизации осуществляется при помощи команды ***show ip route***.

Данные таблиц статической и динамической маршрутизации объединяются в общей таблице, в которую вводятся лучшие из сформированных маршрутов.

В данной лабораторной работе изучаются методы организации составной сети на основе статической маршрутизации. Выполнение работы позволяет студентам детально ознакомиться с общими процедурами маршрутизации пакетов в IP-сетях.

2. Построение сети со статической маршрутизацией в пакете Cisco Packet Tracer

2.1. Создание модели сети в программе Cisco Packet Tracer

Откройте программу Cisco Packet Tracer и создайте сеть, аналогичную показанной на рис. 5.1.

Используйте типы и названия устройств, указанные в таблице 5.1.

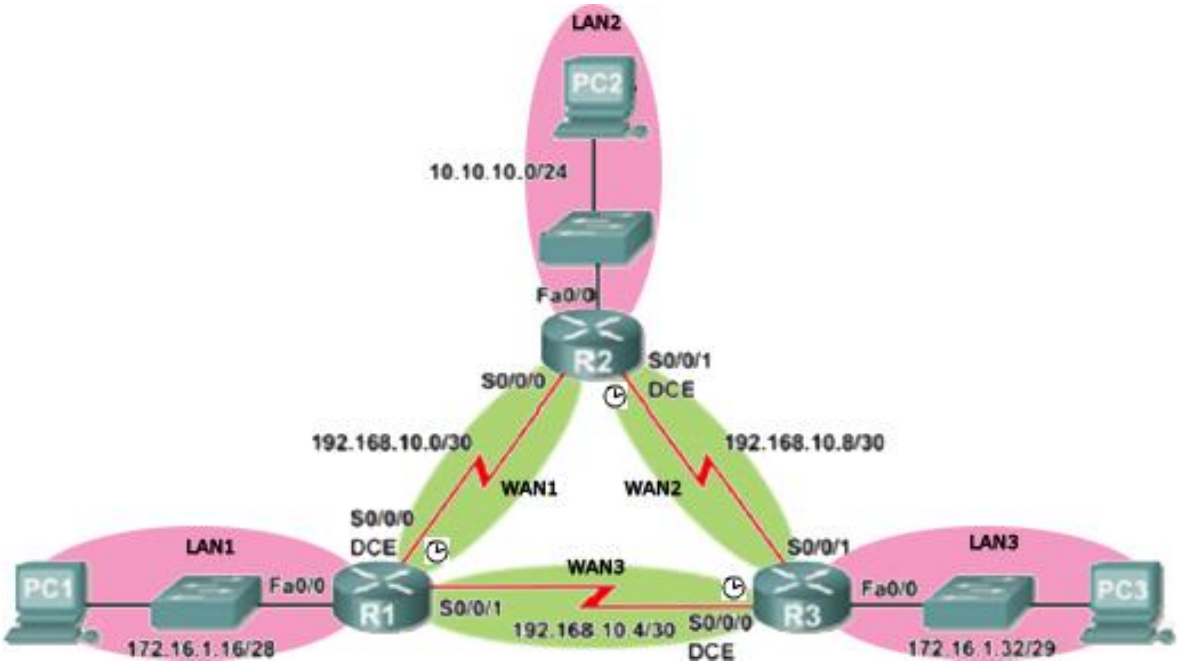


Рис. 5.1. Сетевая структура с тремя локальными сетями, объединенными маршрутизаторами

Таблица 6.

Группа устройств	Название устройства	Кол-во	Дополнительные модули
Маршрутизатор	1841	3	WIC-2T
Коммутаторы	2950-24	3	-
Конечные устройства	PC-PT (компьютер)	3	-

Важное замечание. Чтобы номера интерфейсов совпадали с номерами, указанными в данном руководстве, модуль WIC-2T необходимо вставить в свободный (правый) слот расширения slot0 маршрутизатора. Номера слотов расширения видны на изображении маршрутизатора на вкладке “Physical” при увеличении (воспользуйтесь кнопкой “Zoom In”).

Если линии связи между маршрутизаторами организуются по каналам цифровых глобальных сетей (SDH, телефонные сети и т.д.), то для согласования источника передачи дискретной информации со стандартными цифровыми каналами в аппаратуре cisco применяются специальные модули, например WIC-2T. Модуль WIC-2T предназначен для передачи изохронных цифровых потоков по трактам СЦИ (синхронной цифровой иерархии) глобальных цифровых сетей, используя выделенные стандартные цифровые каналы, например, E1 (2048 кбит/с).

Модуль используется, в основном, для подключения к WAN. В сети на рис. 5.1 локальные сети LAN_1, LAN_2 и LAN_3 соединяются между собой через глобальные сети WAN-1, WAN-2 и WAN-3.

Максимальная скорость в синхронном режиме работы составляет 8 Мбит/с. Модуль Cisco WIC-2T может работать в режимах «ведущий/ведомый». В режиме «ведущий»

устройство задает тактовую частоту работы другим «ведомым» устройствам. В пакете CPT ведущее устройство обозначено значком «часы»

2.2. Расчет подсетей

На основе рис. 5.1 определите ip-адреса и маски для всех устройств. Для всех подсетей определите диапазон адресов, доступных для использования и широковещательный адрес. Портам маршрутизатора присвойте первые адреса, а портам сетевых карт компьютеров – последние адреса подсетей. Также для однозначности в сетях, соединяющих маршрутизаторы, назначайте меньшие IP адреса маршрутизаторам с меньшим номером (например: 192.168.10.1 – R1, 192.168.10.2 – R2). Результаты расчетов занесите в таблицу 5.2.

Таблица 5.2

Название устройства	Интерфейс	Подсеть	IP
R1	Fa0/0	LAN_1	
R1	S0/0/0	WAN_1	
R1	S0/0/1	WAN_3	
R2	Fa0/0	LAN_2	
R2	S0/0/0	WAN_1	
R3	Fa0/0	LAN_3	
R3	S0/0/0	WAN_3	
R3	S0/0/1	WAN_2	
PC1	Eth0	LAN_1	
PC2	Eth0	LAN_2	
PC3	Eth0	LAN_3	

2.3. Начальная настройка маршрутизаторов

Удалите старую конфигурацию и произведите базовую настройку маршрутизаторов (подробно базовая настройка маршрутизатора рассматривалась в лабораторной работе №2).

```
Router > enable
Router #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
```

```
R1(config-line)#login
R1(config-line)#exit
```

Полезное замечание! Не забудьте задать маршрутизаторам разные имена.

2.4. Настройка интерфейсов Fast Ethernet

При настройке интерфейсов (FastEthernet) используйте рассчитанные ранее адреса и маски (таблица 5.2). Ниже приведен пример настройки для интерфейса FastEthernet 0/0 на маршрутизаторе R1:

```
R1(config)# interface fa0/0
R1(config-if)# description --< connection to PC1 >--
R1(config-if)# ip address 172.16.1.17 255.255.255.240
R1(config-if)# no shutdown
```

2.5. Настройка интерфейсов Serial

Для соединения маршрутизаторов между собой используются серийные порты (см. рис. 5.1), в настройке которых имеются отличия от FastEthernet: на интерфейсе необходимо задать скорость канала в битах в секунду. Скорость задается на интерфейсе только с одной стороны канала связи, на DCE устройстве (Data Circuit-terminating Equipment – Аппаратура Передачи Данных). DCE устройство конвертирует сигналы от DTE (Data Terminal Equipment – Оконечное Оборудование Данных) и преобразует их в форму, приемлемую для передачи по линии WAN-служб. Поэтому, чтобы произвести настройку серийного интерфейса, необходимо узнать тип устройства на каждой стороне. Эту информацию можно получить при помощи команды show controllers serial. В примере ниже вывод команды сильно сокращен. Интересующая нас информация находится в начале и выделена красным:

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
------< вывод команды сокращен  >-----
```

Следующим шагом является настройка интерфейса на маршрутизаторах.

При передаче информации от маршрутизатора R1 к маршрутизатору R2 аппаратура DCE на R1 работает в ведущем режиме, а аппаратура DCE на R2 – в ведомом режиме.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.252
R1(config-if)#clock rate 2000000
R1(config-if)#no shutdown

R2(config)#interface serial 0/0/0
R2 (config-if)#ip address 192.168.10.2 255.255.255.252
R2 (config-if)#no shutdown
```

Аналогичным образом настройте другие интерфейсы Serial на всех маршрутизаторах в соответствии с обозначениями рис. 5.1.

Важно! clock rate устанавливается только со стороны DCE устройства, задающего тактовую частоту работы приемопередатчиков на линии связи между маршрутизаторами.

После этого проверьте доступность соседних маршрутизаторов (имеющих непосредственное подключение друг к другу) при помощи команды ping:

```
R2 #ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/21/22
ms
```

2.6. Настройка компьютеров

Настройте компьютеры PC1, PC2, PC3, указав IP-адрес, маску и шлюз из таблицы 5.2 (настройка IP-адресов в Cisco Packet Tracer была описана в методических указаниях к лабораторной работе №1).

При помощи команды **ping** проверьте доступность узлов сети: внутренние и внешние интерфейсы ближайших маршрутизаторов, дальних маршрутизаторов и компьютеров. Объясните полученные результаты.

2.7. Настройка статической маршрутизации

Для продвижения пакетов из одной сети в другую маршрутизаторам необходимо знать, куда направлять входящие пакеты. По умолчанию после первоначальной настройки в таблице маршрутизации имеются записи только о непосредственно подключенных сетях. Эти записи формируются на основе настроек сетевых интерфейсов. Просмотреть таблицу маршрутизации можно в привилегированном режиме при помощи команды show ip route. Ниже приведен результат работы команды для маршрутизатора R1:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/28 is subnetted, 1 subnets
     C 172.16.1.16 is directly connected, FastEthernet0/0
192.168.10.0/30 is subnetted, 2 subnets
     C 192.168.10.0 is directly connected, Serial0/0/0
     C 192.168.10.4 is directly connected, Serial0/0/1
```

В выводе команды символом C отмечены сети, непосредственно подключенные к маршрутизатору. Расшифровка символов приводится в самом начале вывода команды.

Обратите внимание, что интерфейс fa 0/0 маршрутизатора R1 имеет адрес, принадлежащий сети LAN1, интерфейс Se 0/0/0 относится к сети WAN1, а Se 0/0/1 – к сети

WAN3. Поэтому маршрутизатор изначально знает о существовании этих сетей, что в таблице маршрутизации отмечено символом C.

Таким образом, после первоначальной настройки (задания IP-адресов на сетевых интерфейсах), маршрутизатор может перенаправлять пакеты только между непосредственно подключенными к нему сетями. Для обеспечения связности между всеми узлами сети необходимо добавить в таблицу маршрутизации информацию о других сетях. Один из способов сделать это – статическая маршрутизация. В оборудовании компании Cisco добавление статических маршрутов осуществляется в режиме глобальной конфигурации при помощи команды **ip route**. Команда имеет следующий синтаксис:

ip route (destination ip network address) (mask) (interface/next hop ip address)(metric),

где

destination ip network address - ip-адрес сети назначения;

mask - маска сети назначения;

interface/next hop ip address – выходной интерфейс текущего маршрутизатора или ip-адрес следующего маршрутизатора, соответственно;

metric – метрика или приоритет маршрута (при существовании одинаковых маршрутов до одной и той же сети выбирается маршрут с меньшей метрикой). По умолчанию используется значение метрики, равное 1.

Так, чтобы на маршрутизаторе R1 добавить маршрут до локальной сети LAN_2, в режиме глобальной конфигурации выполните команду:

```
R1(config)#ip route 10.10.10.0 255.255.255.0 192.168.10.2
```

Чтобы просмотреть текущую таблицу маршрутизации, выполните в привилегированном режиме команду **show ip route**:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 [1/0] via 192.168.10.2
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.1.16 is directly connected, FastEthernet0/0
     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
```

В выводе команды появилась строчка, отмеченная символом S - статический маршрут, т.е. маршрут, добавленный администратором вручную.

На маршрутизаторе R1 добавьте статические маршруты до остальных сетей, к которым маршрутизатор R1 непосредственно не подключен (LAN3, WAN2):

```
R1(config)#ip route 172.16.1.32 255.255.255.248 192.168.10.6
R1(config)#ip route 192.168.10.8 255.255.255.252 192.168.10.2
```

Затем проверьте правильность указания статических маршрутов, изучив вывод команды show ip route:

```
R1#show ip route
-----< вывод команды сокращен >-----
     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 [1/0] via 192.168.10.2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
S       172.16.1.32/29 [1/0] via 192.168.10.6
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
S       192.168.10.8 [1/0] via 192.168.10.2
```

Проверьте с компьютера PC1 доступность интерфейсов маршрутизатора R2, R3 и компьютера PC2, PC3. Как изменилась доступность узлов по сравнению с проверкой, выполнявшейся в п.3.3 настоящей работы?

> **Важно!** Маршруты должны быть прописаны, как для направления передачи, так и для направления приема. Это необходимо для того, чтобы передаваемые пакеты не только могли достичь узла назначения, но и ответ от узла назначения мог вернуться к узлу-источнику.

Изучите таблицу маршрутизации на остальных маршрутизаторах (R2, R3). Добавьте необходимые статические маршруты, чтобы обеспечить полносвязность сети. Для проверки изучите таблицы маршрутизации на маршрутизаторах R2 и R3.

С компьютера PC1 проверьте доступность интерфейсов маршрутизаторов и компьютеров в других локальных сетях. Как изменилась доступность узлов по сравнению с предыдущей проверкой?

2.8. Исследование отказоустойчивости сети со статической маршрутизацией

Статическая маршрутизация помимо преимуществ – простоты настройки и отсутствия вычислительной нагрузки на ЦП, имеет важный недостаток – неспособность автоматически реагировать на изменения топологии, происходящие в результате сбоев или модернизации сети.

В Cisco Packet Tracer удалите линию связи между маршрутизаторами R1 и R3. Затем с компьютера PC1 проверьте доступность интерфейсов маршрутизаторов и компьютеров в других локальных сетях. Объясните недоступность части узлов в сети.

2.9. Создание альтернативных маршрутов

Одним из способов повышения отказоустойчивости сети является задание альтернативных маршрутов.

Восстановите все линии связи между маршрутизаторами. Просмотрите текущую настройку статической маршрутизации на R1 при помощи команды #**show running-config**:

```
R1#show running-config
Building configuration...

------< вывод команды сокращен  >-----

!

ip classless
ip route 10.10.10.0 255.255.255.0 192.168.10.2
ip route 172.16.1.32 255.255.255.248 192.168.10.6
ip route 192.168.10.8 255.255.255.252 192.168.10.2
!
------< вывод команды сокращен  >-----
```

Продублируйте все существующие маршруты, заменив на них next hop ip-адресом интерфейса другого маршрутизатора. Ниже приведен пример добавления альтернативных маршрутов для сетей LAN_2, LAN_3, WAN2 для R1:

```
R1(config)#ip route 10.10.10.0 255.255.255.0 192.168.10.6 2
R1(config)#ip route 172.16.1.32 255.255.255.248 192.168.10.2 2
R1(config)#ip route 192.168.10.8 255.255.255.252 192.168.10.6 2
```

При добавлении альтернативных маршрутов в примере дополнительно используется параметр “Метрика”, идущий после next-hop. Метрика показывает вес маршрута. Чем больше вес (метрика), тем хуже маршрут. По умолчанию статическим маршрутам присваивается метрика, равная 1. В итоговую таблицу маршрутизации попадают только маршруты с лучшей метрикой, поэтому добавление статических маршрутов с метрикой 2 никак не повлияет на текущую таблицу маршрутизации. Убедиться в этом можно, выполнив команду **#show ip route**.

```
R1#show ip route
-----< вывод команды сокращен >-----
     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 [1/0] via 192.168.10.2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
S       172.16.1.32/29 [1/0] via 192.168.10.6
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
S       192.168.10.8 [1/0] via 192.168.10.2
```

Аналогичным образом пропишите альтернативные прямые и обратные маршруты на маршрутизаторах R2 и R3.

2.9.1. Проверка отказоустойчивости сети с альтернативными маршрутами

При помощи команды **show ip route** просмотрите таблицу маршрутизации на R1 и R2. Убедитесь, что сеть LAN_2 на R1 доступна через интерфейс R2 se0/0/0 (192.168.10.2), а на R2 LAN_1 доступен через интерфейс R1 se0/0/0 (192.168.10.1) (кратчайшие пути):

```
R1#show ip route
-----< вывод команды сокращен >-----
     10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 [1/0] via 192.168.10.2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
S       172.16.1.32/29 [1/0] via 192.168.10.6
```

```
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
S       192.168.10.8 [1/0] via 192.168.10.2

R2#show ip route
-----< вывод команды сокращен >-----
10.0.0.0/24 is subnetted, 1 subnets
     C       10.10.10.0 is directly connected, FastEthernet0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     S       172.16.1.16/28 [1/0] via 192.168.10.1
     S       172.16.1.32/29 [1/0] via 192.168.10.10
192.168.10.0/30 is subnetted, 3 subnets
     C       192.168.10.0 is directly connected, Serial0/0/0
     S       192.168.10.4 [1/0] via 192.168.10.1
     C       192.168.10.8 is directly connected, Serial0/0/1
```

На PC1 выполните команду tracert до PC2. Команда tracert показывает IP адреса устройств до пункта назначения (маршрутизаторы), через которые проходит пакет, прежде чем попасть к получателю:

```
PC1> tracert 10.10.10.254

Tracing route to 10.10.10.254 over a maximum of 30 hops:

  1   54 ms     44 ms     53 ms     172.16.1.17
  2   65 ms     65 ms     65 ms     192.168.10.2
  3   108 ms    108 ms    108 ms    10.10.10.254

Trace complete.
```

Изучите вывод команды. По IP-адресам определите, через какие маршрутизаторы проходит пакет.

На PC1 при помощи команды ping с параметром –t запустите проверку доступности PC2:

```
PC1> ping –t 10.10.10.254
```

Перейдите в режим симуляции и, нажимая на кнопку “Capture/Forward”, наблюдайте продвижение ping-пакетов через сеть. Убедитесь, что наблюдаемый маршрут совпадает с маршрутом, зафиксированным при помощи команды tracert.

Вернитесь в режим Real-time; ping на PC1 оставьте включенным.

> **Полезное замечание!** В реальной жизни режима симуляции не существует, поэтому на практике, сетевым администраторам для определения маршрута прохождения пакета доступна только утилита tracert.

Оборвите линию связи между R1 и R2. Наблюдайте за выводом команды ping на PC1. Отключение линии связи практически никак не сказалось на обмене сообщениями между PC1 и PC2.

Изучите вывод команды show ip route на маршрутизаторе R1 и R2:

```
R1#sh ip route

------< вывод команды сокращен >-----
     10.0.0.0/24 is subnetted, 1 subnets
     S       10.10.10.0 [2/0] via 192.168.10.6
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     C       172.16.1.16/28 is directly connected, FastEthernet0/0
     S       172.16.1.32/29 [1/0] via 192.168.10.6
```

```
     192.168.10.0/30 is subnetted, 2 subnets
          C       192.168.10.4 is directly connected, Serial0/0/1
          S       192.168.10.8 [2/0] via 192.168.10.6
```

Обратите внимание на то, что в таблице маршрут до сети LAN_2 изменился на альтернативный.

Затем проследите маршрут прохождения пакетов в режиме симуляции. Пакеты продвигаются более длинным маршрутом. Вернитесь в Real-time режим, остановите ping на PC1 и выполните команду tracert до PC2:

```
PC>tracert 10.10.10.254

Tracing route to 10.10.10.254 over a maximum of 30 hops:
  1   70 ms     40 ms     40 ms     172.16.1.17
  2   60 ms     50 ms     50 ms     192.168.10.6
  3   80 ms     80 ms     78 ms     192.168.10.9
  4   120 ms    121 ms    120 ms    10.10.10.254
Trace complete.
```

Как согласуются результаты команды tracert с визуализацией движения пакетов в режиме симуляции?

Восстановите связь между маршрутизаторами R1 и R2. При помощи команды tracert убедитесь, что пакеты снова стали перемещаться по старому маршруту.

> **Важное замечание!** В сети, показанной на рис. 5.1, альтернативные маршруты очевидны. В сетях с более сложной топологией при создании альтернативных маршрутов могут возникать маршрутные «петли», по которым пакеты данных будут циркулировать до тех пор, пока не истечет время жизни пакета. При проектировании сложных сетей следует проверить возможность возникновения «петель» при изменениях топологии сети.

2.10. Формирование маршрута «по умолчанию»

В сети часто возникают ситуации, когда требуется отправить пакет к сети назначения, отсутствующей в таблице маршрутизации. В этом случае пакеты направляются на интерфейс (интерфейсы) маршрутизатора, подключенные к сетям, через которые можно достичь сеть назначения. Для этого формируется, так называемый, маршрут «по умолчанию». Синтаксис команды следующий:

```
ip route 0.0.0.0 0.0.0.0 (interface/ next hop ip address)
```

В маршруте «по умолчанию» ip-адрес сети назначения указан как 0.0.0.0 и маска сети назначения как 0.0.0.0.

Пример команды: `ip route 0.0.0.0 0.0.0.0.0 192.168.10.1`

Команда означает, что все пакеты, имеющие неизвестные адреса назначения, следует отправлять на адрес 192.168.10.1.

> **Важно!** В случае наличия нескольких альтернативных маршрутов со статической маршрутизацией выбирается более специфичный, т.е. тот, в котором более точно указана сеть назначения. Таким образом, получается, что маршрут по умолчанию имеет самый низкий приоритет. Это удобно, т.к. позволяет значительно сократить количество статических записей в таблице маршрутизации: можно создавать только те маршруты, у которых next-hop отличается от маршрута «по умолчанию».

Для изучения работы “маршрута по умолчанию” в Cisco Packet Tracer создайте устройство Generic Server-PT и подключите его к порту FastEthernet 0/1 маршрутизатора R2, как показано на рис. 5.2. При этом получается, что сервер и маршрутизатор образовали

новую локальную сеть LAN_4, отсутствующую в таблицах маршрутизации роутеров R1 и R3.

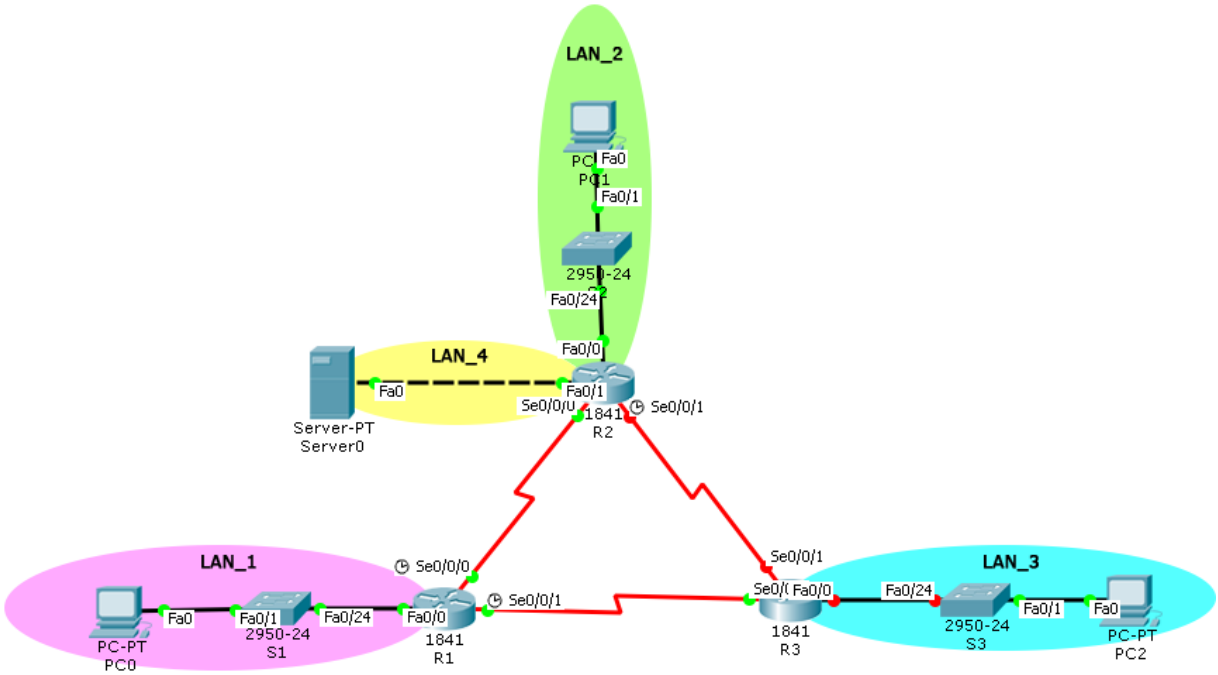


Рис. 5.2. Добавление сервера к исходной сети

Настройте интерфейсы сервера и маршрутизатора, используя данные из таблицы 5.3. Настройка IP-адреса, маски и шлюза сервера производится при помощи вкладки IP Configuration, аналогично настройке компьютера.

Таблица 5.3.

Название устройства	Интерфейс	Подсеть	IP	Маска	Шлюз
R2	Fa0/1	10.10.11.0/30	10.10.11.1	255.255.255.252	-
Server1	Fa	10.10.11.0/30	10.10.11.2	255.255.255.252	10.10.11.1

На маршрутизаторах R1 и R3 пропишите маршрут «по умолчанию» на маршрутизатор R2:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.9
```

Просмотрите таблицу маршрутизации на R1, R3:

```
R1#sh ip route

------< вывод команды сокращен  >-----
10.0.0.0/24 is subnetted, 1 subnets
      S      10.10.10.0 [1/0] via 192.168.10.2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
      C      172.16.1.16/28 is directly connected, FastEthernet0/0
      S      172.16.1.32/29 [1/0] via 192.168.10.6
192.168.10.0/30 is subnetted, 3 subnets
```

```
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
S       192.168.10.8 [1/0] via 192.168.10.2
S*   0.0.0.0/0 [1/0] via 192.168.10.2
```

Проверьте доступность интерфейса Fa0/1 маршрутизатора R2 и сервера Server1 с компьютеров локальных сетей (PC1, PC2, PC3) при помощи команды ping.

3. Контрольные вопросы

1. Какой, на ваш взгляд, главный недостаток статической маршрутизации?
2. Предложите несколько ситуаций, в которых удобно использовать маршрут «по умолчанию».
3. В каких случаях использовать маршрут «по умолчанию» нежелательно?

4. Задание для самостоятельной работы

1. Получите у преподавателя pka-файл с персональным заданием. Откройте этот файл в программе Cisco Packet Tracer и следуйте инструкциям, которые появятся после открытия файла.
2. Ознакомьтесь с исходными данными и выполните задание.
3. Сохраните конфигурацию всех сетевых устройств.
4. Сохраните изменения в pka-файле и отправьте его преподавателю в качестве отчета о выполнении самостоятельной работы.

5. Рекомендуемые материалы

1. М.А.Плоткин. Лекции по курсу «Сети связи и системы коммутации». Тема 6 Технология Интернет. Раздел «Маршрутизация в IP-сетях».
2. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г.
3. Глава 16 Протокол межсетевого взаимодействия. Раздел «Схема IP-маршрутизации», стр.517-533;
4. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г.
5. Глава 17 Базовые протоколы TCP/IP. Раздел «Общие свойства и классификация протоколов
6. маршрутизации», стр. 572-574.
7. Димарцио Д.Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. Перевод с англ. - СПб: Символ Плюс, 2003г.
8. Хаброкен Д. Как работать с маршрутизаторами Cisco. Перевод с англ. – М: ДМК Пресс. 2005г.
9. Интернет ресурс linkmeup. Сети для самых маленьких. Часть третья. Статическая маршрутизация - http://linkmeup.ru/blog/14.html, 2013 г.

Лабораторная работа №6.
Динамическая маршрутизация в компьютерных сетях на основе протокола RIP

1. Введение

Динамическая маршрутизация – вид маршрутизации, при котором сведения о сетевых маршрутах вносятся программно в таблицы маршрутизации специальными служебными протоколами. В отличие от мостов и коммутаторов, которые строят адресные таблицы, анализируя информационные кадры, передаваемые конечными узлами сети, маршрутизаторы самостоятельно обмениваются специальными служебными пакетами, сообщая об известных им сетях и других маршрутизаторах.

Протоколы динамической маршрутизации должны обеспечивать:

- рациональность выбранного маршрута;
- экономичное использование ресурсов, т.е. не требовать большого служебного трафика;
- оперативное отслеживание изменений в структуре сетей.

Динамическая маршрутизация использует два основных алгоритма:

- дистанционно-векторные алгоритмы;
- алгоритмы состояния связей.

При ***дистанционно-векторном алгоритме*** каждый маршрутизатор рассылает по сети сообщение-вектор, содержащее расстояния от данного маршрутизатора до всех известных ему сетей. При получении вектора от соседа, маршрутизатор наращивает указанные в сообщении расстояния на величину расстояния до данного соседа, добавляет информацию об известных ему других сетях, и рассылает по сети новое значение вектора. В конечном итоге каждый маршрутизатор получает информацию обо всех подсетях.

Дистанционно-векторные алгоритмы хорошо работают в сетях с простой структурой и относительно редкими изменениями топологии связей. При увеличении числа сетей существенно возрастает объем служебного трафика. Маршрутизаторы располагают лишь косвенной информацией о топологии сети – вектором расстояний. При возникновении изменений в сети маршрутизаторы в течение некоторого переходного периода используют устаревшую информацию об уже несуществующих маршрутах.

Алгоритмы состояния связей позволяют построить ***точный*** граф связей сети. Для получения информации о состоянии линий связи, подключенных к его портам, маршрутизатор периодически обменивается короткими пакетами HELLO со своими ближайшими соседями. Передача более объемных сообщений происходит только при изменении состояния какой-либо связи, поэтому служебный трафик, создаваемый протоколами алгоритмов состояния связей, имеет меньший объем, чем при дистанционно-векторных алгоритмах.

2. Протокол RIP

Наиболее распространенным протоколом, использующим дистанционно-векторный алгоритм, является протокол маршрутной информации RIP (англ. Routing Information Protocol).

Основной характеристикой маршрута является условное расстояние до сети назначения. Стандарты протокола RIP допускают различные виды метрик расстояния: число промежуточных маршрутизаторов (хопов), параметры пропускной способности, вносимые задержки, надежность сетей. В большинстве реализаций протокола RIP используется

простейшая метрика – число хопов, которые нужно преодолеть пакету на пути к сети назначения.

В соответствии с протоколом RIP каждый маршрутизатор периодически и широковещательно рассылает по сети сообщения о расстояниях до известных ему сетей.

В результате обмена сообщениями маршрутизаторы после нескольких итераций получают информацию обо всех имеющихся сетях и о расстояниях до этих сетей.

Последовательно анализируя содержание принимаемых служебных пакетов, маршрутизатор формирует таблицу маршрутов, оптимизированных по выбранному критерию. Маршрутизатор, передавший информацию о маршруте с наименьшим значением метрики, вносится в таблицу маршрутизации как следующий (next hop).

Рассмотрим формирование таблицы маршрутизации для маршрутизатора R1 в составной сети, показанной на рис. 6.1.

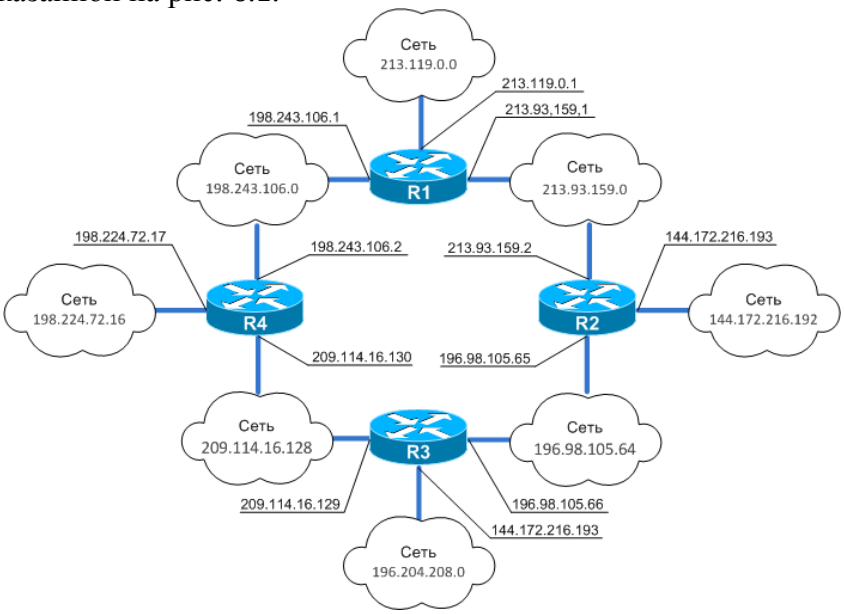


Рис. 6.1. Сеть с маршрутизаторами, объединяющая восемь подсетей

В исходном состоянии каждый маршрутизатор формирует минимальную таблицу маршрутизации, содержащую только непосредственно подсоединенные сети. Данные для такой таблицы собираются автоматически программным обеспечением стека TCP/IP. Все подсоединенные сети имеют метрику 1.

Минимальная таблица маршрутизатора R1 показана в таблице 6.1.

Таблица 6.1.

Номер сети	Адрес следующего маршрутизатора	Номер порта	Расстояние
198.243.106.0	198.243.106.1	1	1
213.119.0.0	213.129.0.1	2	1
213.93.159.0	213.93.159.1	3	1

На первом шаге каждый маршрутизатор посылает соседям сообщения, содержащие информацию о своей минимальной таблице. Соседями маршрутизатора являются маршрутизаторы, которым IP-пакет может передаваться по одной из непосредственно

подсоединенных сетей. На схеме рис. 6.1 соседями маршрутизатора R1 являются маршрутизаторы R2 и R4.

Сообщения протокола RIP передаются в форме дейтаграмм протокола UDP; для каждой сети указывается IP-адрес сети и расстояние до нее от маршрутизатора, передавшего это сообщение.

На первом шаге маршрутизатор R1 передает маршрутизаторам R2 и R4 следующие сообщения:

- сеть 198.243.106.0, расстояние 1;
- сеть 213.129.0.0, расстояние 1;
- сеть 213.93.159.0, расстояние 1.

На следующем, втором шагепроисходит получение RIP-сообщений от соседей и обработка принятой информации. Получив сообщения от маршрутизаторов R2 и R4, маршрутизатор R1 может внести новую запись в таблицу; при этом полученное значение метрики маршрута увеличивается на единицу, а также фиксируются порт и адрес маршрутизатора, от которого получена эта информация.

Протокол RIP изменяет запись о какой-либо сети, если новая информация позволяет получить маршрут с лучшей метрикой, чем указано в существующей записи. После сравнения, в таблице маршрутизации остается только одна запись о каждой сети. Если поступает несколько записей с равнозначными маршрутами, то сохраняется запись, которая поступила первой по времени.

После 2-го шага маршрутизатор R1 оставляет в таблице семь записей (см. табл. 6.2) с максимальной метрикой 2.

Таблица 6.2.

Номер сети	Адрес следующего маршрутизатора	Номер порта	Расстояние
198.243.106.0	198.243.106.1	1	1
213.129.0.0	213.129.0.1	2	1
213.93.159.0	213.93.159.1	3	1
144.172.216.192	213.93.159.2	3	2
196.98.105.64	213.93.159.2	3	2
198.224.72.16	198.243.106.2	1	2
209.114.16.128	198.243.106.2	1	2

Аналогичные операции производятся на остальных маршрутизаторах сети.

На 3-м шаге соседям рассылаются новые RIP-сообщения, содержащие сведения обо всех известных сетях - как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из полученных на предыдущем шаге RIP-сообщений.

На следующем (4-м) шаге повторяются операции 2-го шага – маршрутизаторы принимают RIP-сообщения от соседей, обрабатывают содержащуюся в них информацию и соответствующим образом корректируют свои таблицы маршрутизации.

После 4-го шага в таблице маршрутизатора R1 содержится восемь строк с максимальной метрикой 3 (см. табл. 6.3), описывающих маршруты ко всем восьми сетям, показанным на рис. 6.1.

Таблица 6.3.

Номер сети	Адрес следующего маршрутизатора	Номер порта	Расстояние
198.243.106.0	198.243.106.1	1	1
213.119.0.0	213.129.0.1	2	1
213.93.159.0	213.93.159.1	3	1
144.172.216.192	213.93.159.2	3	2
196.98.105.64	213.93.159.2	3	2
198.224.72.16	198.243.106.2	1	2
209.114.16.128	198.243.106.2	1	2
196.204.208.0	213.93.159.2	3	3

Если структура сети остается постоянной, то дальнейшие шаги рассылки и обработки RIP-сообщений не будут изменять записи в таблицах маршрутизации.

В реальных сетях в процессе эксплуатации постоянно происходят различные изменения, например, нарушается работоспособность маршрутизаторов или линий связи, подключаются новые сети и пр.

Время адаптации сети к возникающим изменениям зависит от частоты посылки RIP-сообщений.

В протоколе RIP период рассылки равен 30 секундам. Величина тайм-аута выбрана равной шестикратному значению периода рассылки. Соответственно, если маршрутизатор перестает передавать своим соседям сообщения о доступных ему сетях, то по истечении 180 секунд, записи, занесенные в таблицы ближайших соседей на основании сообщений от этого маршрутизатора, становятся недействительными. Через 360 секунд аналогичный процесс повторится на более удаленных маршрутизаторах и т.д.

Для коррекции записей в таблицы маршрутизации, отражающих нарушения ранее зафиксированного маршрута, используются два способа:

- ограничение времени жизни записи о маршруте;
- указание условно бесконечного расстояния до сети, ставшей недоступной.

Каждая запись таблицы маршрутизации, полученная по протоколу RIP, имеет определенное время жизни, TTL (англ. Time To Live). Получение сообщения, подтверждающего содержание конкретной записи, устанавливает таймер времени жизни в исходное состояние. Если за время тайм-аута не поступят новые сообщения о данном маршруте, то он отмечается как недействительный. Метод тайм-аута применяется, когда маршрутизатор не может передать сообщение об отказавшем маршруте своим соседям.

Если маршрутизатор ***может*** передать сообщение, то протокол RIP предусматривает регистрацию условно бесконечного расстояния (16 хопов) до сети, ставшей недоступной.

Протокол RIP является наиболее простым протоколом динамической маршрутизации и применяется в небольших сетях (с количеством промежуточных маршрутизаторов до 15).

3. Построение сети на основе протокола RIP в пакете CPT

3.1. Создание модели сети в программе Cisco Packet Tracer

В пакете Cisco Packet Tracer создайте сеть, аналогичную показанной на рис. 6.2. Используйте типы и названия устройств, указанные в таблице 4.

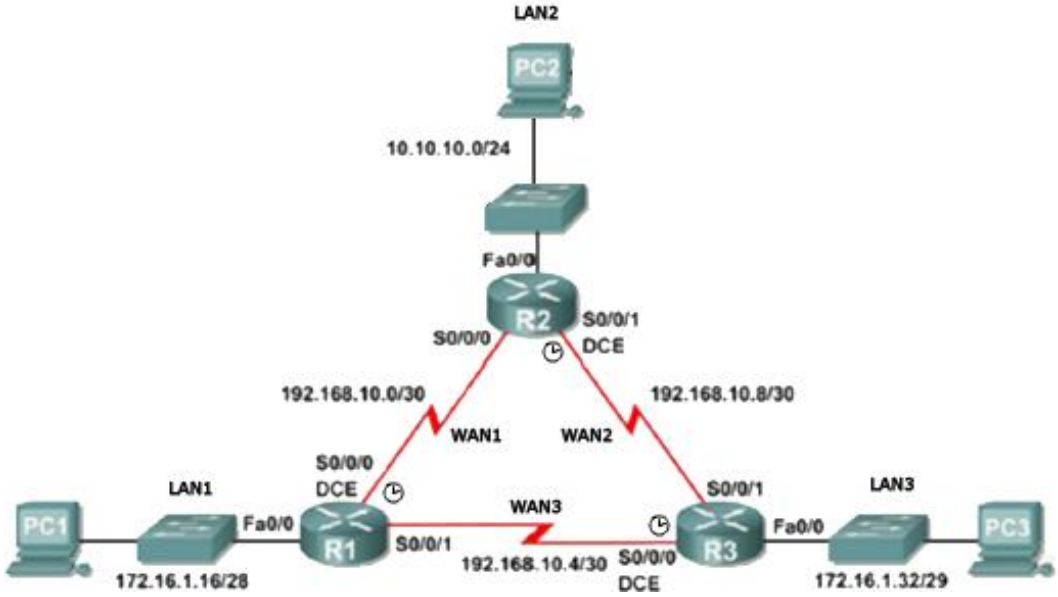


Рис. 6.2. - Сетевая структура с тремя подсетями, объединенными маршрутизаторами

Таблица 6.4.

Группа устройств	Название устройства	Кол-во	Дополнительные модули
Маршрутизатор	1841	3	WIC-2T
Коммутаторы	2950-24	3	-
Конечные устройства	PC-PT (компьютер)	3	-

3.2. Расчет подсетей

На основе схемы рис.6.2 определите ip-адреса и маски для всех устройств. Для всех подсетей определите диапазон адресов, доступных для использования, и широковещательный адрес. Портам маршрутизаторов присвойте первые адреса, а портам сетевых карт компьютеров – последние адреса подсетей. Результаты расчетов занесите в таблицу 6.5.

Таблица 6.5.

Название устройства	Интерфейс	Подсеть	IP	Маска	Шлюз
R1	Fa0/0	LAN_1			-

R1	S0/0/0	WAN_1			-
R1	S0/0/1	WAN_3			-
R2	Fa0/0	LAN_2			-
R2	S0/0/0	WAN_1			-
R2	S0/0/1	WAN_2			-
R3	Fa0/0	LAN_3			-
R3	S0/0/0	WAN_3			-
R3	S0/0/1	WAN_2			-
PC1	Eth0	LAN_1			
PC2	Eth0	LAN_2			
PC3	Eth0	LAN_3			

3.3. Начальная настройка маршрутизаторов

Удалите старую конфигурацию и произведите базовую настройку маршрутизаторов (подробно базовая настройка маршрутизатора рассматривалась в лабораторной работе №2).

```
Router > enable
Router # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 15
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
```

Важное замечание. Не забудьте задать маршрутизаторам разные имена.

3.4. Настройка интерфейсов Fast Ethernet

При настройке интерфейсов используйте рассчитанные ранее адреса и маски (таблица 6.2). Ниже приведен пример настройки для интерфейса FastEthernet 0/0 на маршрутизаторе R1:

```
R1(config)# interface fa0/0
R1(config-if)# description connection to PC1
R1(config-if)# ip address 172.16.1.17 255.255.255.240
R1(config-if)# no shutdown
```

3.5. Настройка интерфейсов Serial

При настройке интерфейсов используйте рассчитанные ранее адреса и маски (таблица 6.2). Ниже приведен пример настройки для интерфейса Serial0/0/0

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.252
R1(config-if)# clock rate 2000000
R1(config-if)# no shutdown
```

Важное замечание. Подробнее настройка серийного порта описана в работа №5.

После этого проверьте доступность соседних маршрутизаторов (имеющих непосредственное подключение друг к другу) при помощи команды ping.

3.6. Настройка компьютеров

Настройте компьютеры PC1, PC2, PC3, указав IP-адрес, маску и шлюз из таблицы 6.2 (настройка IP-адресов в Cisco Packet Tracer была описана в методических указаниях к лабораторной работе №1).

При помощи команды ping проверьте доступность узлов сети: внутренние и внешние интерфейсы ближайших маршрутизаторов.

3.7. Настройка динамической маршрутизации

Для продвижения пакетов из одной сети в другую маршрутизаторам необходимо знать, куда направлять входящие пакеты. Один из вариантов сделать это – статическая маршрутизация. Второй способ – использование протоколов маршрутизации. Протокол RIP (англ. Routing Internet Protocol) является наиболее простым и распространенным протоколом, использующим дистанционно-векторный алгоритм.

В оборудовании компании cisco настройка протоколов маршрутизации осуществляется в режиме конфигурации соответствующего протокола. Для перехода в режим конфигурирования протокола RIP выполните в режиме глобального конфигурирования команду *router rip:*

```
R1(config )# router rip
```

В режиме конфигурирования протокола RIP укажите версию протокола RIP (в работе используется 2-я версия):

```
R1(config-router)# version 2
```

В режиме конфигурирования протокола RIP отключите автосуммирование (по умолчанию включен режим автосуммирования, при котором роутер формирует сетевые классовые адреса вместо используемых в нашей сети адресов подсетей на основе масок).

```
R1(config-router)# no auto-summary
```

Затем в режиме конфигурирования протокола RIP укажите сети, информацию о которых необходимо сообщать другим маршрутизаторам, например:

```
R1(config-router)#network 172.16.1.16
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.10.4
```

Аналогично выполните конфигурирование RIP на маршрутизаторах R2, R3.

Используя режим симуляции в Cisco Packet Tracer, убедитесь, что маршрутизаторы обмениваются информацией, т.е. пересылают друг другу пакеты RIPv2. Отключите визуализацию служебных протоколов (STP, CDP, DTP) при помощи фильтра (Edit Filters):

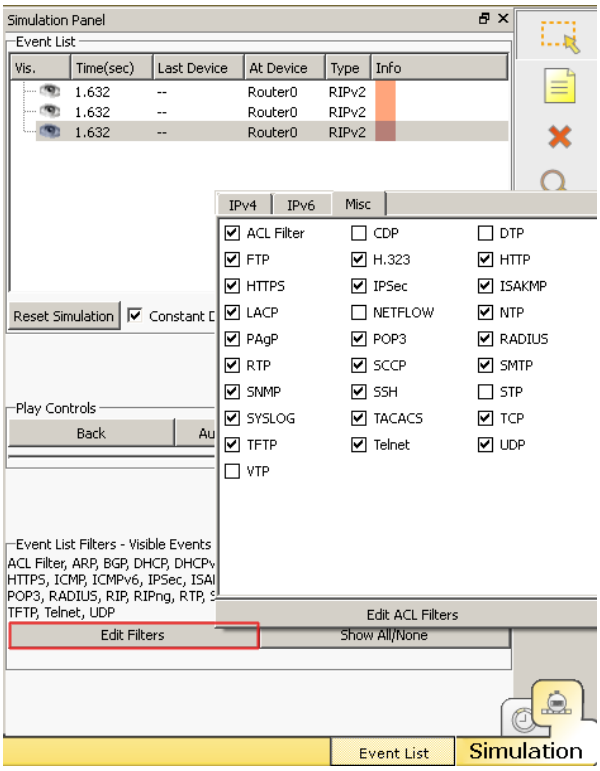


Рисунок 6.3. Cisco Packet Tracer - настройка фильтра пакетов в режиме симуляции

Вернитесь в режим Real-time и просмотрите таблицы маршрутизации на каждом маршрутизаторе. Например, таблица маршрутизации для R1 будет выглядеть следующим образом:

```
R1 #show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
     R 10.10.10.0 [120/1] via 192.168.10.2, 00:00:13, Serial0/0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     C 172.16.1.16/28 is directly connected, FastEthernet0/0
     R 172.16.1.32/29 [120/1] via 192.168.10.6, 00:00:04, Serial0/0/1
192.168.10.0/30 is subnetted, 3 subnets
     C 192.168.10.0 is directly connected, Serial0/0/0
     C 192.168.10.4 is directly connected, Serial0/0/1
     R 192.168.10.8 [120/1] via 192.168.10.6, 00:00:04, Serial0/0/1
                    [120/1]     via     192.168.10.2,     00:00:13,
               Serial0/0/0
```

Маршруты в таблице делятся на два типа - первого уровня (Parent) и второго уровня (Child). Маршруты первого уровня - маршруты с маской меньшей или равной классовой маске сетевого адреса. Примеры маршрутов первого уровня: маршрут по умолчанию (default), маршрут сетевой суммированный (supernet), маршрут сетевой (network). Маршруты второго уровня - маршруты с маской равной или большей, чем классовая.

Если в таблице указан один маршрут первого уровня и у него несколько маршрутов второго уровня без указания маски, значит, маршрут поделён на сети с одинаковой маской, равной маске маршрута первого уровня. В случае использования VLSM, маски маршрутов второго уровня будут указаны.

При получении пакета, маршрутизатор ищет подходящую сеть по совпадению битов ip адреса назначения и битов ip адреса маршрутов первого уровня. Выбирается маршрут с максимальным числом совпадающих битов. Если совпадение есть - отправляет, если нет - возвращается на первый уровень и ищет другой маршрут. Если ни один из маршрутов не подходит, отсылает пакет на маршрут по умолчанию (default route).

Так, запись первого уровня "**192.168.10.0/30 is subnetted, 3 subnets**" говорит о том, что в сети класса C 192.168.10.0 присутствует три подсети /30, которые представлены ниже тремя записями второго уровня. При этом сеть 192.168.10.8 имеет два альтернативных маршрута. Они оба попали в таблицу маршрутизации, т.к. с точки зрения протокола маршрутизации (RIP) являются равнозначными.

Маршрутизаторы cisco допускают использование нескольких альтернативных маршрутов, имеющих равные административные дистанции и метрики, что позволяет, при необходимости, повысить производительность сети.

Как уже отмечалось, символы, стоящие перед маршрутами, указывают, каким образом информация попала в таблицу маршрутизации. Так сети, непосредственно подключенные к маршрутизатору, обозначены символом "C"; сети, информация, о которых получена из протокола RIP, обозначены символом "R" и т.д. (полный список протоколов и их обозначений отображается в начале вывода команды #**show ip route**).

Каждый источник имеет свою административную дистанцию (коэффициент доверия), которая указывается первым числом в квадратных скобках после сети назначения. Сети, непосредственно присоединенные к маршрутизатору, имеют наименьшую административную дистанцию и не отображаются в таблице. Второе число в скобках указывает метрику, т.е. цену маршрута в рамках данного протокола. Административная дистанция и метрика позволяют определить приоритет одного маршрута перед другим, если он получен из разных источников (протоколов маршрутизации), или один протокол маршрутизации предлагает несколько альтернативных маршрутов.

При помощи команды ping с компьютера PC1 проверьте работоспособность сети.

Исследование отказоустойчивости сети с динамической маршрутизацией

При помощи команды **show ip route** просмотрите таблицу маршрутизации на R1. Убедитесь, что сеть LAN_2 (10.10.10.0/24) доступна через интерфейс R1 se0/0/0 по маршруту через R2 (192.168.10.2) :

```
R1# sh ip route
------< вывод команды сокращен  >-----

10.0.0.0/24 is subnetted, 1 subnets
     R 10.10.10.0 [120/1] via 192.168.10.2, 00:00:13, Serial0/0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     C 172.16.1.16/28 is directly connected, FastEthernet0/0
     R 172.16.1.32/29 [120/1] via 192.168.10.6, 00:00:04, Serial0/0/1
192.168.10.0/30 is subnetted, 3 subnets
     C 192.168.10.0 is directly connected, Serial0/0/0
     C 192.168.10.4 is directly connected, Serial0/0/1
     R 192.168.10.8 [120/1] via 192.168.10.6, 00:00:04, Serial0/0/1
```

```
                    [120/1]     via     192.168.10.2,     00:00:13,
                Serial0/0/0
```

В обратном направлении сеть LAN_1 (172.16.1.16/28) доступна на R2 через интерфейс se0/0/0:

```
R2# sh ip route
------< вывод команды сокращен  >-----

10.0.0.0/24 is subnetted, 1 subnets
     C 10.10.10.0 is directly connected, FastEthernet0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     R 172.16.1.16/28 [120/1] via 192.168.10.1, 00:00:04, Serial0/0/0
     R   172.16.1.32/29   [120/1]   via   192.168.10.10,   00:00:07,
 Serial0/0/1
192.168.10.0/30 is subnetted, 3 subnets
     C 192.168.10.0 is directly connected, Serial0/0/0
     R 192.168.10.4 [120/1] via 192.168.10.10, 00:00:07, Serial0/0/1
                    [120/1] via 192.168.10.1, 00:00:04, Serial0/0/0
C 192.168.10.8 is directly connected, Serial0/0/1
```

На PC1 выполните команду **tracert** до PC2. Команда **tracert** показывает промежуточные маршрутизаторы, через которые проходит пакет, прежде чем попасть к получателю:

```
PC1> tracert 10.10.10.254

Tracing route to 10.10.10.254 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 172.16.1.17
2 20 ms 10 ms 10 ms 192.168.10.2
3 10 ms 10 ms 10 ms 10.10.10.254
Trace complete.
```

Изучите вывод команды. По IP-адресам определите, через какие маршрутизаторы проходит пакет.

На PC1 при помощи команды ping с параметром –t запустите проверку доступности PC2:

```
PC1> ping –t 10.10.10.254
```

Перейдите в режим симуляции и, нажимая на кнопку “Capture/Forward”, наблюдайте продвижение icmp-пакетов через сеть (ping). Убедитесь, что их маршрут совпадает с результатами, полученными при помощи команды tracert. Вернитесь в режим Real-time, ping на PC1 оставьте запущенным.

Оборвите линию связи между R1 и R2. Наблюдайте за выводом команды ping на PC1. Сначала должны появиться сообщения о недоступности узла, через некоторое время доступность PC2 должна восстановиться.

Вновь получите вывод команды show ip route на маршрутизаторе R1:

```
R1#sh ip route

------< вывод команды сокращен  >-----
10.0.0.0/24 is subnetted, 1 subnets
     R 10.10.10.0 [120/2] via 192.168.10.6, 00:00:11, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     C 172.16.1.16/28 is directly connected, FastEthernet0/0
     R 172.16.1.32/29 [120/1] via 192.168.10.6, 00:00:11, Serial0/0/1
192.168.10.0/30 is subnetted, 2 subnets
     C 192.168.10.4 is directly connected, Serial0/0/1
```

```
     R   192.168.10.8   [120/1]   via   192.168.10.6,   00:00:11,
Serial0/0/1
```

Обратите внимание, что сеть LAN_2 стала доступной через маршрутизатор R3, но с увеличенной метрикой 2. Аналогичным образом с маршрутизатора R2 сеть LAN_1 стала доступной через R3:

```
R2#sh ip route

------< вывод команды сокращен  >-----
10.0.0.0/24 is subnetted, 1 subnets
     C 10.10.10.0 is directly connected, FastEthernet0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
     R   172.16.1.16/28   [120/2]   via   192.168.10.10,   00:00:15,
Serial0/0/1
     R   172.16.1.32/29   [120/1]   via   192.168.10.10,   00:00:15,
Serial0/0/1
192.168.10.0/30 is subnetted, 2 subnets
     R 192.168.10.4 [120/1] via 192.168.10.10, 00:00:15, Serial0/0/1
     C 192.168.10.8 is directly connected, Serial0/0/1
```

В режиме симуляции проследите изменения маршрута прохождения пакетов.

Вернитесь в Real-time режим, остановите ping на PC1 и выполните команду tracert до PC3:

```
PC1>tracert 10.10.10.254
Tracing route to 10.10.10.254 over a maximum of 30 hops:
1 0 ms 10 ms 0 ms 172.16.1.17
2 10 ms 21 ms 10 ms 192.168.10.6
3 20 ms 30 ms 10 ms 192.168.10.9
4 10 ms 20 ms 40 ms 10.10.10.254
Trace complete.
```

Как согласуются результаты команды tracert с визуализацией движения пакетов в режиме симуляции?

Восстановите связь между маршрутизаторами R1 и R3. При помощи команды tracert убедитесь, что пакеты снова стали передаваться по старому маршруту. Просмотрите таблицу маршрутизации на R1, R2; убедитесь, что сеть LAN_2 вновь доступна через R2, а маршрут с метрикой 2 отсутствует.

4. Контрольные вопросы

1. Объясните, почему удаление одной любой линии связи в схеме на рис. 6.2 не приводит к потере полносвязности сети?
2. Укажите, какие недостатки имеет динамическая маршрутизация по сравнению со статической.

5. Задание для самостоятельной работы

1. Получите у преподавателя pka-файл с персональным заданием. Откройте этот файл в программе Cisco Packet Tracer и следуйте инструкциям, которые появятся после открытия файла.
2. Ознакомьтесь с исходными данными и выполните задание.
3. Сохраните конфигурацию всех сетевых устройств.
4. Сохраните изменения в pka-файле и отправьте его преподавателю в качестве отчета о выполнении самостоятельной работы.

6. Рекомендуемые материалы

1. М.А.Плоткин. Лекции по курсу «Сети связи и системы коммутации». Тема 6 Технология Интернет. Раздел «Маршрутизация в IP-сетях».
2. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г.
3. Глава 16 Протокол межсетевого взаимодействия. Раздел «Схема IP-маршрутизации», стр.517-533.
4. В.Г.Олифер и др. Компьютерные сети. 4-е издание, ПИТЕР, 2012г.
5. Глава 17 Базовые протоколы TCP/IP. Раздел «Общие свойства и классификация протоколов
6. маршрутизации», стр. 572-574.
7. Димарцио Д.Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. Перевод с англ. - СПб: Символ Плюс, 2003г.
8. Хаброкен Д. Как работать с маршрутизаторами Cisco. Перевод с англ. – М: ДМК Пресс. 2005г.

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА СВЕТОВОДНОЙ ФОТОНИКИ

Кафедра химии, на базе которой была создана кафедра Физики И Техники Оптической Связи (позднее кафедра Световодной Фотоники), входила в состав первых 14 кафедр ЛИТМО, сформированных в 1930 году. В 30-60 годах кафедра работала в составе факультета точной механики, возглавлял кафедру известный русский ученый-химик профессор С.А. Щукарев.

В 1976 кафедра вошла в состав инженерно-физического факультета. Были приглашены И.К. Мешковский, В.И. Земский и позднее В.Ф. Пашин из ФТИ им. Иоффе, а затем О.С. Попков и Ю.П. Тарлаков из ЛТИ им. Ленсовета и А.Ф. Новиков из ГОИ им. Вавилова. Заведующим кафедрой был избран И.К. Мешковский, который руководит кафедрой и по сей день. В эти годы в рамках кафедры была предложена и реализована новая учебная программа по курсу "Общая и физическая химия", которая базировалась на новейших достижениях науки и методики преподавания. В то время на кафедре развивались два научно-технических направления:

- технология оптического волокна;
- создание новых композиционных оптических материалов.

По инициативе И.К. Мешковского в 1982 году впервые в СССР кафедра стала осуществлять подготовку инженеров по специализации «Волоконная и интегральная оптика» и была переименована в кафедру Физической химии, волоконной и интегральной оптики. На кафедру были приглашены С.А. Миронов из ГП "Дальняя связь" и С.В. Данилов из ГОИ им. Вавилова. На базе кафедры были проведены первые в России разработки по технологии производства оптического волокна, оптических жгутов, различных волоконно-оптических приборов и систем.

Благодаря работам заведующего кафедрой, академика Российской Академии инженерных наук профессора И.К. Мешковского, профессоров В.И.Земского и А.Ф. Новикова в 1986 г. возникла научная школа в области фотоники дисперсных и нелинейных сред. Созданы новые композиционные оптические материалы на основе пористого силикатного стекла с внедренными в поры молекулами органических и неорганических веществ, на основе которых впервые были созданы активные элементы твердотельных перестраиваемых лазеров на красителях, а также разработано множество волоконно-оптических и фотонных сенсоров и микрооптических элементов. Доцентом Г.Б. Дейнека развиты работы по компьютерному моделированию физических и химических процессов.

В 1998 г. в связи с развитием систем телекоммуникации и высокими потребностями в специалистах по волоконно-оптической связи кафедра первой в Санкт-Петербурге стала осуществлять подготовку инженеров по специальности "Физика и техника оптической связи", а с 2003 г. — выпуск инженеров по этой специальности. На кафедру были

приглашены И.А. Соколов из ООО "Оптен", Ю.А. Зингеренко из ЗАО "Новел Ил", А.В. Борисенко из ГУТ им. Бонч-Бруевича, С.В. Кухтин из ООО "Метроком".

С начала 2000-х годов на кафедре ведутся разработки в области волоконно-оптических датчиков. Особенно успешным оказалось сотрудничество с ОАО «Концерн «ЦНИИ «Электроприбор», начатое в 2005г., в области создания прецизионных волоконно-оптических гироскопов, а также навигационных приборов на их основе. Эта работа оказала значительное влияние на дальнейшее направление научной деятельности кафедры.

В 2013 году на базе университета и кафедры Световодной фотоники был создан Научно-исследовательский центр Световодной фотоники. Деятельность данного центра плотно связана с разработками кафедры.

Для более эффективной реализации научного потенциала, развития творческой мысли и успешной реализации технических решений при кафедре созданы научные лаборатории, оснащенные современным оборудованием:

- сборки и юстировки устройств световодной фотоники;
- Лаборатория программируемой электроники;
- Лаборатория световодной фотоники;
- Лаборатория моделирования и программирования.

Для успешной реализации технического потенциала и научных решений кафедра световодной фотоники ведет сотрудничество с ведущими международными институтами и научными техническими центрами:

- Берлинский технический институт (Technical University Berlin подразделение нелинейной оптики (Nonlinear Optics) лаборатория лазерной физики и волоконной оптики (Laserphysik und Faseroptik)
- Фраунгоферовский институт исследования надежности и микроинтеграции (Fraunhofer Institute for Reliability and Microintegration) подразделение системной интеграции и технологий соединений (System Integration and Interconnection Technologies) лаборатория технологий оптических соединений (Optical Interconnection Technology)
- Йенский технический университет имени Фридриха Шиллера (Friedrich-Schiller-Universität Jena)
- Чешская Академия наук (Институт физики, Прага)

Совместные лабораторные эксперименты, разработка современных проектов производится и с крупнейшими научными центрами России:

- АО "Концерн "ЦНИИ "Электроприбор
- ФГУП "НИТИОМ ВНЦ "ГОИ им. С.И. Вавилова"
- Физико-технический институт имени А.Ф.Иоффе Российской академии наук

В рамках программы обучения и во время прохождения практики учащиеся кафедры имеют возможность поработать в лабораториях наших партнеров (университетов и предприятий). Сама кафедра также располагает своими лабораториями с уникальным оборудованием. Так в лаборатории световодной фотоники присутствуют: спектроанализатор, эксимерный лазер и С02 лазеры, комплекс записи волоконных решеток Брэгга, несколько стендов для прецизионной юстировки и исследования поляризационных свойств оптических волокон с двулучепреломлением, аппаратура для сварки оптических волокон с сохранением поляризации.

Не стоит забывать, что специалисты, работающие в области разработок, проектирования, строительства и эксплуатации оптических линий связи, в настоящее время востребованы на российском и мировом рынке труда. Многие бакалавры и магистранты кафедры световодной фотоники еще до завершения обучения успешно устраиваются на работу в известные технологические компании. Наших выпускников можно встретить на технических и руководящих должностях в следующих организациях: Ростелеком, Мегафон,

МТС, TELE2, Yota, АО "Концерн "ЦНИИ "Электроприбор, ФГУП "НИТИОМ ВНЦ "ГОИ им. С.И. Вавилова", Волоконно-оптический кабельный завод ООО «ОПТЕН», ОАО «НПП Дальняя Связь», ООО «Новел – ИЛ», ООО “Optimum Networks”, ЗАО «Петерлинк», ЗАО «Политэк» ООО «Севкабель» и др.

Плоткин Михаил Абрамович
Шарков Илья Александрович
Дейнека Иван Генадьевич

Методическое руководство для проведения цикла лабораторных работ по курсу «Сети связи и системы коммутации»

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО

Зав. РИО	Н.Ф. Гусарова
Подписано к печати	13.05.2016
Заказ №	3696
Тираж	90 экз.

Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49