В. Г. Кулаков, Ю. Л. Леохин

МОДЕЛИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ В СИМУЛЯТОРЕ CISCO PACKET TRACER 6

Учебное пособие

Москва, 2016

УДК 004.7
ББК 73
К 90

Рецензенты:
Е. В. Никульчев, д.т.н., профессор
(Московский технологический институт);
А. В. Вишнеков, д.т.н., профессор
(Национальный исследовательский университет «Высшая школа экономики»)

Кулаков В. Г., Леохин Ю. Л.
Моделирование компьютерных сетей в симуляторе Cisco Packet Tracer 6 : учеб. пособие — М. : Изд-во МТИ, 2016. — 175 с.; ил.

ISBN 978-5-9906422-4-9

Учебное пособие предназначено для студентов, изучающих дисциплину «Вычислительные системы, сети и телекоммуникации». В пособии рассматриваются основные принципы моделирования компьютерных сетей в симуляторе Cisco Packet Tracer, а также приведены краткие справочные сведения по командам операционной системы Cisco IOS. С целью закрепления изученного материала студентам предлагается выполнить набор упражнений и заданий для самостоятельной работы.

Оглавление

ВВЕДЕНИЕ ... 6
1. ОСНОВЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ... 7
1.1. Некоторые особенности натурных экспериментов в компьютерной сети ... 7
1.2. Понятие модели ... 8
1.3. Имитационное моделирование ... 9
2. ЗНАКОМСТВО С ПРОГРАММОЙ CISCO PACKET TRACER ... 11
2.1. Интерфейс программы Cisco Packet Tracer ... 11
2.1.1. Ознакомление с основными элементами интерфейса симулятора ... 15
2.2. Термины и условные обозначения ... 15
2.2.1. Ознакомление с пиктограммами сетевого оборудования ... 19
2.3. Справочные и учебные материалы ... 19
2.4. Задание для самостоятельной работы ... 19
3. ЛОКАЛЬНЫЕ СЕТИ НА БАЗЕ КОММУТАТОРОВ ВТОРОГО УРОВНЯ ... 20
3.1. Простейшая сеть из двух компьютеров ... 20
3.1.1. Прямое соединение компьютеров ... 20
3.2. Сеть на базе концентратора ... 24
3.2.1. Модель сети с концентратором ... 25
3.3. Сеть на базе коммутатора второго уровня ... 28
3.3.1. Модель сети с коммутатором ... 29
3.4. Древовидная топология связей ... 32
3.5. Создание резервных линия связи между коммутаторами ... 33
3.5.1. Сеть с резервной линией связи ... 34
3.6. Динамическое распределение IP-адресов ... 35
3.6.1. Настройка сервиса DHCP на сервере ... 36
3.7. Задание для самостоятельной работы ... 40
4. УПРОЩЕННЫЙ РЕЖИМ НАСТРОЙКИ МОДЕЛЕЙ МАРШРУТИЗАТОРОВ ... 41
4.1. Настройка параметров в окне модели маршрутизатора ... 41
4.1.1. Модель сети с маршрутизатором ... 41
4.1.2. Модель сети с маршрутизатором и двумя коммутаторами ... 44
4.2. Протокол маршрутизации RIP ... 47
4.2.1. Модель сети с двумя маршрутизаторами ... 47
4.3. Петлевидные соединения между маршрутизаторами ... 50
4.3.1. Модель сети с петлевидным соединением маршрутизаторов ... 50
4.4. Настройка параметров последовательных портов ... 52
4.4.1. Настройка последовательного канала связи ... 52
4.5. Задание для самостоятельной работы ... 54
5. ЗНАКОМСТВО С CISCO IOS ... 56
5.1. Командный интерпретатор Exec ... 56
5.2. Справочная система IOS ... 57
5.2.1. Использование справочной системы ... 58
5.3. Команды IOS для базовой настройки оборудования ... 58
5.3.1. Ограничение доступа к маршрутизатору ... 61
5.4. Команды IOS для настройки интерфейсов ... 63
5.5. Команды IOS для настройки параметров протокола RIP ... 65
5.6. Особенности реализации утилит ping и traceroute ... 66
5.7. Настройка сетевого оборудования с внешнего терминала ... 67
5.7.1. Настройка маршрутизатора с вкладки CLI и с консоли ... 67
5.8. Настройка статических маршрутов ... 73

5.9. Команды IOS для настройки сервиса DHCP ... 74
5.9.1. Настройка статических маршрутов и сервиса DHCP ... 75
5.10. Сброс настроек оборудования в исходное состояние ... 78
5.11. Задание для самостоятельной работы ... 79
6. БЕСКЛАССОВАЯ АДРЕСАЦИЯ ... 81
6.1. Маска подсети ... 81
6.2. Использование масок ... 81
6.2.1. Разделение локальной сети на подсети ... 82
6.2.2. Моделирование взаимодействия подсетей ... 83
6.3. Задание для самостоятельной работы ... 84
7. КОНФИГУРИРОВАНИЕ ВИРТУАЛЬНОЙ СЕТИ ... 85
7.1. Виртуальные локальные сети ... 85
7.2. Конфигурирование статических сетей ... 86
7.2.1. Сеть на базе управляемых коммутаторов ... 87
7.2.2. Первый способ объединения виртуальных сетей ... 89
7.2.3. Второй способ объединения виртуальных сетей ... 91
7.3. Задание для самостоятельной работы ... 93
8. ПРОТОКОЛ EIGRP ... 94
8.1. Команды Cisco IOS для настройки EIGRP ... 94
8.1.1. Настройка маршрутизаторов для работы по протоколу EIGRP ... 95
8.2. Распределение нагрузки ... 99
8.2.1. Моделирование распределения нагрузки ... 99
8.3. Задание для самостоятельной работы ... 102
9. ПРОТОКОЛ OSPF ... 104
9.1. Команды Cisco IOS для настройки OSPF ... 105
9.1.1. Сеть с одной зоной ... 106
9.1.2. Сеть с двумя зонами ... 109
9.2. Задание для самостоятельной работы ... 111
10. БЕСПРОВОДНЫЕ СЕТИ WI-FI ... 113
10.1. Создание сети Wi-Fi с точкой доступа ... 113
10.1.1. Беспроводная сеть с одной точкой доступа ... 114
10.2. Настройка точки доступа, встроенной в маршрутизатор ... 117
10.2.1. Беспроводная сеть с маршрутизатором и точкой доступа ... 118
10.2.2. Настройка маршрутизатора по беспроводному соединению ... 122
10.3. Задание для самостоятельной работы ... 125
11. ТЕХНОЛОГИЯ FRAME RELAY ... 126
11.1. Протокол Frame Relay ... 126
11.2. Настройки интерфейса на работу с каналом Frame Relay ... 127
11.3. Облако Cloud-PT ... 127
11.3.1. Соединение двух сетей каналом Frame Relay ... 128
11.4. Особенности использования общего IP-интерфейса ... 132
11.4.2. Моделирование сети, использующей звездообразную топологию ... 136
11.5. Использование подинтерфейсов ... 141
11.5.1. Создание подинтерфейсов на интерфейсах, подключенных к каналам Frame Relay ... 142
11.6. Задание для самостоятельной работы ... 146
12. СПИСОК УПРАВЛЕНИЯ ДОСТУПОМ ACL ... 147
12.1. Стандартный ACL ... 147
12.1.1. Настройка стандартного списка ACL ... 149
12.2. Расширенный список ACL ... 153

12.2.1. Настройка расширенного списка ACL 154
12.3. Задание для самостоятельной работы 156
13. ТЕХНОЛОГИИ NAT И PAT 157
13.1. Технология преобразования сетевых адресов 157
13.2. Настройка режима преобразования адресов в маршрутизаторе 157
13.2.1. Моделирование перегруженной трансляции адресов 159
13.3. Задание для самостоятельной работы 161
14. ПРОТОКОЛ IPv6 163
14.1. Адресация по протоколу IPv6 163
14.1.1. Настройка адресации в случае прямого соединения компьютеров 165
14.2. Команды для настройки интерфейсов 166
14.3. Команды для настройки маршрутизации 168
14.4. Команды для проверки правильности настройки 169
14.5.1. Настройка сети с двумя маршрутизаторами 169
14.6. Задание для самостоятельной работы 172
ЗАКЛЮЧЕНИЕ 173
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 174

ВВЕДЕНИЕ

Симулятор Cisco Packet Tracer является специализированным учебным программным обеспечением, предназначенным для изучения технологий сетей передачи данных. Cisco Packet Tracer позволяет имитировать и визуализировать процессы работы технологий и протоколов, использующихся в компьютерных сетях, а также служит инструментом для выполнения лабораторных работ, в том числе работ с автоматической проверкой результата. Cisco Packet Tracer может применяться для совместной работы нескольких пользователей по сети, а также может использоваться для игр и соревнований в рамках учебного процесса.

Используя Cisco Packet Tracer, инструкторы могут разрабатывать особые индивидуальные и групповые занятия. Студенты могут создавать, настраивать, изучать сети и устранять неисправности, используя виртуальное оборудование и модели соединений. Учебная среда на основе имитационных моделей помогает студентам развивать критическое мышление и творческий подход к решению задач.

Задания с использованием Cisco Packet Tracer входят в учебные программы IT Essentials, CCNA и CCNA Security.

Студенты многих российских вузов, специализирующиеся в области информационных технологий, параллельно с основным образовательным процессом могут посещать курсы Сетевой Академии Cisco. В учебных программах все большее количество времени выделяется на самостоятельную работу, однако студенты часто пренебрегают возможностью самоподготовки, которую предоставляет симулятор Cisco Packet Tracer.

С симулятором Cisco Packet Tracer студенты обычно знакомятся в процессе изучения курса IT Essentials, но активно использовать его начинают только при изучении курсов CCNA. Данное учебное пособие предназначено для самостоятельной тренировки студентов в процессе прохождения курса CCNA Routing and Switching.

Сетевое оборудование, выпускаемое компанией Cisco Systems, работает под управлением фирменной операционной системы Cisco IOS. Полное описание набора команд Cisco IOS (Cisco IOS Configuration Command Reference) состоит из нескольких десятков книг и занимает тысячи страниц, и даже краткий справочник по командам имеет объем более семисот страниц [1], поэтому в дальнейшем мы будем рассматривать только те команды Cisco IOS, которые необходимы для выполнения упражнений.

1. ОСНОВЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Программа Cisco Packet Tracer предназначена для моделирования компьютерных сетей, и прежде, чем вы начнете работу с этой программой, вам будет полезно ознакомиться с основами имитационного моделирования, например, по первой главе из книги Роберта Шеннона «Имитационное моделирование систем: искусство и наука» [18].

1.1. Некоторые особенности натурных экспериментов в компьютерной сети

Прежде чем перейти к рассмотрению принципов имитационного моделирования, необходимо объяснить, зачем оно нужно.

Любые действия всегда связаны с риском, полное бездействие также связано с риском, а эксперименты связаны с повышенным риском — если бы до проведения эксперимента точно были известны его результаты, то не нужно было бы его проводить.

В процессе проведения натурного эксперимента объект, над которым он проводится, может быть поврежден или разрушен, поэтому натурные эксперименты желательно проводить в специально созданных лабораториях, где с помощью всевозможных мер предосторожности обычно стараются свести к минимуму возможный ущерб от ошибок экспериментаторов.

Проведение экспериментов непосредственно на рабочем сетевом оборудовании собственной фирмы или организации — это весьма рискованный трюк. Вспомните шуточную поговорку: «Квалификация инженера прямо пропорциональна количеству сожженной им аппаратуры». Смысл поговорки заключается в том, что тренировки на реальном оборудовании часто заканчиваются поломкой этого самого оборудования и последующим его ремонтом.

Все изменения в работе компьютерной сети специалисты обычно производят после завершения рабочего дня, чтобы не мешать нормальному функционированию других сотрудников организации. В случае проведения эксперимента это, скорее всего, означает, что он будет проводиться не только вечером, но и ночью, так как эксперименты имеют свойство затягиваться намного дольше предполагаемого времени. Экспериментатор, соответственно, будет проводить опыты в усталом и полусонном состоянии, что повышает вероятность ошибок. Последствия этих ошибок могут проявиться только утром, когда сотрудники организации приступят к работе и, следовательно, резко возрастет нагрузка на компьютерную сеть. Экспериментатор, скорее всего, в это время уже уедет домой отсыпаться и, естественно, отключит свой телефон.

Вывести оборудование из строя можно не только в результате неправильного подключения. Даже такая «безобидная» операция, как обновление программного обеспечения в энергонезависимой памяти устройства (так называемое «обновление прошивки»), может закончиться поломкой устройства, если по ошибке будет загружен файл, предназначенный для другой модели оборудования. Иногда совершенно несовместимыми друг другом оказываются файлы прошивок для оборудования одной и той же модели, но разных лет выпуска. Исправить ошибку прошивки обычно можно только в сервисном центре, так как после подобной ошибки устройство перестает запускаться. Кроме того, самостоятельная прошивка программной памяти устройства может аннулировать гарантийные обязательства фирмы-изготовителя, так как в инструкции по эксплуатации может быть указано, что прошивка должна производиться в сервисном центре.

Корпорация Cisco Systems выпускает высокопроизводительное оборудование. Следовательно, повреждение этого оборудования в результате ошибки экспериментатора может оставить без связи сразу большое количество сотрудников той организации, в которой эксперимент проводится.

Прежде, чем ставить какой-либо опыт на рабочем оборудовании, постарайтесь найти ответы на следующие вопросы:

- Где хранится инструкция по эксплуатации оборудования? Хорошо ли вы ее запомнили?
- Были ли сохранены текущие настройки оборудования? Где и как они хранятся? Сколько времени потребуется на их восстановление?
- Что произойдет, если устройство, на котором проводится опыт, полностью выйдет из строя? Предусмотрено ли резервирование оборудования и каналов связи на том участке компьютерной сети, где будет проводиться эксперимент? Имеется ли в запасе резервное оборудование, чтобы временно заменить неисправное? Какое количество сотрудников и на какой период времени может быть лишено связи, если никакого запасного оборудования нет? Какой экономический и моральный ущерб понесет за это время организация?
- Где находится ближайший сервисный центр, в какое время он работает и есть ли у вас его телефон? Сколько времени обычно занимает ремонт оборудования? Сколько времени нужно на то, чтобы довезти его до сервисного центра, а потом привезти обратно?
- Не будут ли в процессе эксперимента производиться действия, которые могут привести к утрате гарантии на обслуживание оборудования, которую дает фирма-изготовитель? Сколько стоит платный ремонт оборудования?
- Сколько стоит оборудование и где его можно купить? Сколько времени потребуется на оформление заказа и поставку нового оборудования, если старое окажется невозможным отремонтировать?
- Где находится ближайший огнетушитель? Пригодна ли эта модель для тушения электронной аппаратуры?

1.2. Понятие модели

Рассмотрим кратко основные понятия и принципы моделирования.

Под моделью обычно понимается некоторый образ реального объекта, отражающий существенные свойства этого объекта и заменяющий его в процессе решения какой-либо задачи.

Модель представляет собой используемый для предсказания и сравнения инструмент, позволяющий спрогнозировать последствия альтернативных действий и указать, какому из этих действий нужно отдать предпочтение.

Применение моделей позволяет проводить эксперименты в таких ситуациях, в которых экспериментирование на реальных объектах было бы практически невозможным, экономически нецелесообразным или слишком опасным.

Благодаря тому, что поведение модели можно полностью контролировать, при экспериментировании с моделью сложной системы часто можно больше узнать о ее внутренних взаимодействующих факторах, чем путем манипулирования параметрами реальной системы.

Различают модели материальные (натурные) и идеальные (абстрактные). Материальные модели, в свою очередь, делят на физические, представляющие собой

уменьшенную или увеличенную физическую копию объекта, и аналоговые, основанные на процессах, аналогичных в каком-то отношении изучаемому.

Модель может применяться в качестве:

- средства осмысления действительности;
- средства общения;
- средства обучения и тренировки;
- инструмента прогнозирования;
- средства постановки экспериментов.

Например, программу Cisco Packet Tracer мы будем в дальнейшем использовать как средство для тренировки.

Создавая модель, помните о том, что любую задачу можно решать различными способами и любую задачу можно разделить на части. Деление сложной модели на части называется декомпозицией и производится до тех пор, пока не будет достигнута возможность реализовать каждую из частей.

1.3. Имитационное моделирование

После того, как были изобретены электронные вычислительные машины, одним из наиболее важных и полезных орудий анализа структуры сложных систем стало имитационное моделирование.

Имитационное моделирование есть процесс конструирования модели реальной системы и постановки экспериментов на этой модели с целью понять поведение системы или оценить различные стратегии, обеспечивающие ее функционирование.

Имитационное моделирование является экспериментальной и прикладной методологией. Процесс моделирования включает и конструирование модели, и ее аналитическое применение для изучения некоторой проблемы.

Для того чтобы смоделировать работу некоторой системы, необходимо поставить эксперимент, отражающий основные условия моделируемой ситуации, и придумать способ имитации последовательности происходящих в системе событий.

Имитационная модель — это модель типа «Черный ящик». Имитационные модели не способны формировать свое решение в том виде, в каком это имеет место в аналитических моделях: для получения результатов необходимо выполнять прогон модели, а не решать ее, как систему уравнений.

Имитационное моделирование — это циклический процесс. Вначале создается упрощенная модель системы. После того, как эта модель будет налажена и будут получены первые результаты, модель усложняют, добавляя новые параметры, элементы и связи между элементами, и проводят на ней новую серию экспериментов. Модель, таким образом, совершенствуется до тех пор, пока не начнет давать полезные для практического применения результаты.

Одной из самых серьезных проблем, с которыми сталкиваются разработчики моделей, является тенденция имитировать излишнее число деталей и особенностей реальной системы. Никогда не следует забывать о том, что модель должна отражать только такие свойства объекта, которые можно считать существенными для решаемой задачи, так как у любого реального объекта имеются тысячи самых разнообразных свойств и промоделировать все эти свойства не сможет даже суперкомпьютер.

Сила мелочей — в их многочисленности. Например, если в модели простой компьютерной сети имеется десять устройств, для каждого из которых нужно задать значения десяти различных параметров, то в процессе настройки модели потребуется выполнить сотню операций.

В моделях, используемых в программе Cisco Packet Tracer, настройка такого элемента, как сервер или маршрутизатор, может потребовать выполнения нескольких десятков операций. Поэтому не следует без необходимости включать в модель сети дополнительные элементы «просто на всякий случай».

Процесс обучения моделированию обычно включает три основных этапа:

- копирование чужих моделей;
- внесение изменений в чужие модели;
- создание собственных моделей.

Тренировка — это обязательная часть процесса обучения. Освоение любого мастерства начинается с простого подражания. Копировать чужое нужно точно и очень аккуратно. Примеры, которые приводятся в учебниках, нужно проделывать полностью, создавая модели и вводя исходные данные вручную, а не копируя с диска или из Интернет в виде готового файла.

Второй этап обучения — внесение изменений в модель для того, чтобы определить, что произойдет, если изменить значение какого-либо параметра, добавить или убрать какие-либо элементы модели. Вносить изменения нужно последовательно, друг за другом, а не все сразу, чтобы можно было проконтролировать последствия каждого изменения.

Последний этап — это разработка своих собственных моделей. Работу с моделью компьютерной сети в программе Cisco Packet Tracer можно разделить на три этапа:

- создание модели сети;
- проведение экспериментов на модели;
- анализ полученных результатов.

Для создания модели компьютерной сети нужно выполнить следующие действия:

- разработать схему сети;
- разделить сеть на подсети, присвоить номера и маски подсетям;
- разместить в рабочем пространстве Cisco Packet Tracer пиктограммы сетевых устройств и компьютеров;
- соединить все устройства между собой в соответствии со схемой сети;
- настроить параметры оборудования;
- проверить правильность настройки.

После того, как модель сети будет создана и налажена, можно приступать к проведению экспериментов.

2. ЗНАКОМСТВО С ПРОГРАММОЙ CISCO PACKET TRACER

Запустить программу Cisco Packet Tracer на выполнение можно из меню «Пуск» или с помощью ярлыка, размещенного на рабочем столе.

2.1. Интерфейс программы Cisco Packet Tracer

После запуска программы Cisco Packet Tracer открывается окно, изображенное на рис. 2.1.

Вдоль верхнего края окна расположен **заголовок**, содержащий имя запущенной в окне программы (Cisco Packet Tracer), имя файла, в котором хранится модель компьютерной сети, и стандартные кнопки управления, с помощью которых можно изменить размер окна, свернуть его или закрыть.

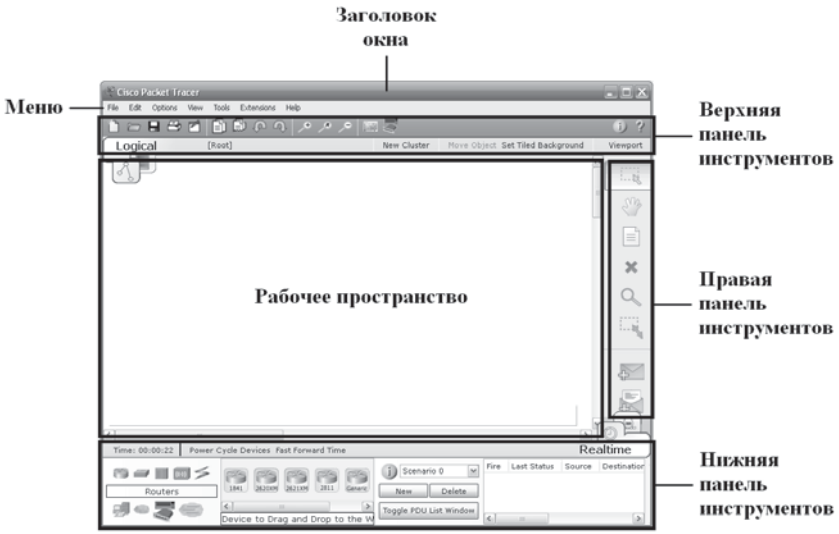

Рис. 2.1. Интерфейс программы Packet Tracer

Под заголовком окна расположена **строка главного меню**, которая включает следующие пункты-подменю:

- подменю **File** содержит команды, которые позволяют сохранять и открывать файлы, описывающие топологию сетей;
- подменю **Edit** включает команды, которые позволяют редактировать изображение в рабочем пространстве;
- подменю **Options** служит для настройки рабочего окружения;
- подменю **View** содержит команды настройки параметров пользовательского интерфейса;

- подменю **Tools** содержит команды, которые позволяют создавать дополнительные модели устройств;
- подменю **Extensions** обеспечивает доступ к вспомогательным программам;
- подменю **Help** включает команды, которые позволяют обратиться к справочнику, просмотреть учебные материалы или получить сведения о текущей версии программы Cisco Packet Tracer.

Под строкой меню находится **верхняя панель инструментов**.

Первый ряд кнопок, размещенных на верхней панели инструментов, содержит **ярлыки** для наиболее часто используемых команд из главного меню Cisco Packet Tracer:

- **New** — создать новую модель;
- **Open** — загрузить модель из файла;
- **Save** — сохранить модель в файле;
- **Print** — вывести модель на печатающее устройство;
- **Activity Wizard** — создать инструкции по упражнениям, которые должны быть выполнены с помощью данной модели;
- **Copy** — скопировать выделенный фрагмент модели в буфер;
- **Paste** — вставить данные из буфера в окно модели;
- **Undo** — отменить последние изменения, внесенные в модель;
- **Redo** — восстановить изменения, отмененные командой Undo;
- **Zoom In** — увеличить изображение;
- **Zoom Reset** — восстановить исходный размер изображения;
- **Zoom Out** — уменьшить изображение;
- **Drawing Palette** — задать цвета для рисования элементов модели;
- **Custom Devices Dialog** — вызвать программу для создания пользовательских (модифицированных) моделей устройств.

Во втором ряду верхней панели инструментов располагаются следующие кнопки:

- **Logical/Physical** — переключатель режима отображения рабочего пространства;
- **Root / Back** — кнопка для развертывания и свертывания кластера;
- **New Cluster** — кнопка для объединения устройств в одну группу (кластер);
- **Move Object** — кнопка для перемещения (включения) объектов в кластер;
- **Set Tiled Background** — кнопка для выбора фонового изображения;
- **Viewport** — кнопка для просмотра рабочего пространства в уменьшенном масштабе.

Переключатель режима отображения рабочего пространства имеет два состояния:

- **Logical Workspace** — в рабочем пространстве отображается топология компьютерной сети;
- **Physical Workspace** — в рабочем пространстве отображается модель размещения сетевого оборудования в физическом пространстве.

Под панелью инструментов располагается рабочее пространство и правая панель инструментов.

Рабочее пространство служит для построения модели компьютерной сети и визуального наблюдения за процессом моделирования. Снизу и справа от рабочего пространства располагаются полосы прокрутки.

Правая панель содержит инструменты, которые позволяет перемещать, дублировать и стирать объекты в рабочем пространстве. На правой панели расположены следующие кнопки:

- **Select** — выбрать объект;
- **Place Note** — вставить примечание;
- **Delete** — удалить объект;
- **Inspect** — просмотреть параметры объекта;
- **Draw a Polygon** — нарисовать фигуру;
- **Resize Shape** — изменить размер области;
- **Add Simple PDU** — передать простой пакет (пакет протокола icmp);
- **Add Complex PDU** — передать сложный пакет.

Под рабочим пространством размещается **нижняя панель инструментов**, которая состоит из горизонтального ряда кнопок и расположенного под ним ряда специальных областей.

Нижняя панель инструментов содержит следующие кнопки:

- **Power Cycle Devices** — кнопка для имитации одновременного перезапуска всего сетевого оборудования в результате сброса по питанию;
- **Fast Forward Time** — кнопка для кратковременного ускорения процесса моделирования;
- **Realtime/Simulation** — переключатель режима моделирования.

Переключатель режима моделирования имеет два состояния:

- **Realtime** — работа в режиме реального времени;
- **Simulation** — работа в пошаговом режиме.

Слева от ряда кнопок на нижней панели инструментов располагаются **часы**, которые отображают модельное время (время, прошедшее с момента создания или открытия файла модели).

Под кнопками на нижней панели инструментов располагаются следующие **специальные области**:

- область для выбора типа сетевого оборудования;
- область для выбора конкретной модели оборудования;
- область для создания сценария моделирования;
- область для отображения результатов моделирования.

Область для выбора типа оборудования позволяет выбрать один из следующих классов сетевых устройств:

- **Routers** — маршрутизаторы;
- **Switches** — коммутаторы;
- **Hubs** — концентраторы;
- **Wireless Devices** — беспроводные устройства;
- **Connections** — сетевые кабели;
- **End Devices** — оконечные устройства;
- **Security** — защитные устройства (межсетевые экраны);
- **WAN Emulation** — эмуляторы оборудования глобальных сетей;
- **Custom Made Devices** — модифицированные пользователем модели сетевых устройств;
- **Multiuser Connection** — многопользовательское соединение.

Область сценария моделирования позволяет выбрать сценарий моделирования с помощью выпадающего списка, а также содержит три кнопки:

- **New** — добавить новый сценарий;
- **Delete** — очистить список пакетов;
- **Toggle PDU List Window** — развернуть или свернуть область отображения результатов моделирования.

Область отображения результатов моделирования служит для вывода сообщений о результатах моделирования процесса передачи пакетов по сети.

При переключении в **режим имитации** (Simulation) вид главного окна программы изменится (рис. 2.2), так как часть рабочего пространства будет закрыта областью управления моделированием.

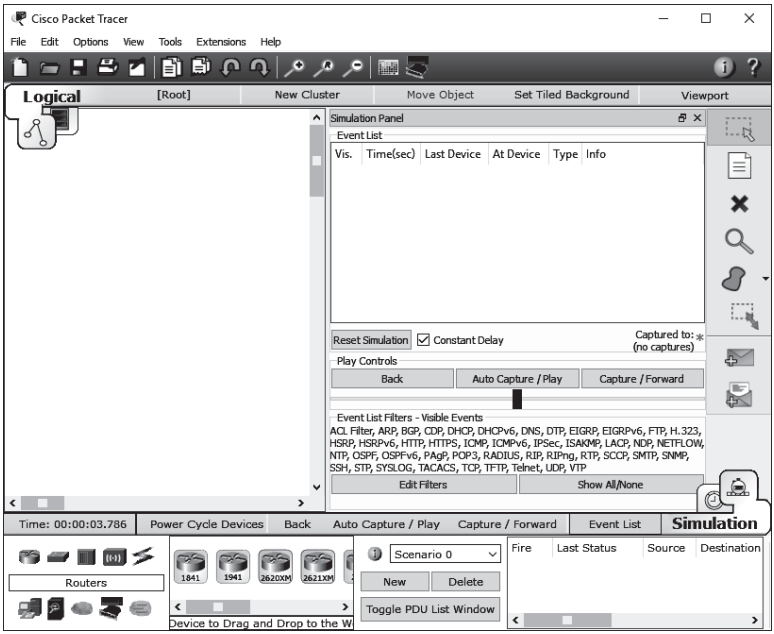

Рис. 2.2. Внешний вид главного окна Cisco Packet Tracer после переключения в режим Simulation

Верхнюю часть области управления моделированием занимает **таблица событий (**Event List), в которой отображается список произошедших в системе событий.

Слева под таблицей Event List находится кнопка **Reset Simulation**, которая позволяет очистить список событий.

После таблицы Event List размещаются область управления моделированием **Play Controls**, в которой размещаются кнопки, предназначенные для управления процессом моделирования:

- **Back** — вернуться на один шаг назад;

- **Auto Capture / Play** — выполнить последовательно все шаги моделирования в автоматическом режиме (без остановок);
- **Capture / Forward** — выполнить очередной шаг моделирования.

Ниже этих кнопок находится регулятор-ползунок, который позволяет управлять скоростью моделирования.

Далее располагается **область фильтрации событий** (Event List Filters), в которой отображается список типов отображаемых событий и имеется две кнопки:

- **Edit Filters** — кнопка для выбора типов пакетов, передача которых будет отображаться в рабочем пространстве и списке событий (по умолчанию отображаются все типы);
- **Show All** — кнопка для включения отображения всех типов пакетов.

На нижней панели инструментов в режиме Simulation также появится дополнительный набор кнопок, дублирующих кнопки из области управления моделированием: Back, Auto Capture / Play и Capture / Forward. Это позволяет при необходимости скрыть область управления.

2.1.1. Ознакомление с основными элементами интерфейса симулятора

В данном упражнении Вам необходимо просто запустить на выполнение симулятор Cisco Packet Tracer и ознакомиться с описанными выше элементами интерфейса этой программы.

После того, как Вы ознакомитесь с элементами интерфейса, завершите работу с Cisco Packet Tracer, закрыв основное окно этой программы.

2.2. Термины и условные обозначения

В симуляторе Cisco Packet Tracer для сетевого оборудования применяются графические условные обозначения, принятые в качестве корпоративного стандарта в Cisco Systems.

В Cisco Packet Tracer используется два типа моделей: модели конкретного оборудования и абстрактные (Generic) модели. Абстрактные модели получены в результате обобщения и упрощения моделей, относящихся к определенному типу оборудования. Такими моделями можно пользоваться на начальном этапе обучения — их легче настраивать, но их возможности сильно ограничены.

Рассмотрим условные обозначения различных устройств, работа которых может моделироваться программой Cisco Packet Tracer.

Условное обозначение, используемое для персонального компьютера (PC), подключаемого к сети в качестве рабочей станции, показано на рисунке 2.3.

Рис. 2.3. Условное обозначение персонального компьютера

Сервер (Server) — это мощный, высокопроизводительный компьютер, выполняющий общественные функции по координации и обслуживанию рабочих станций и распределению ресурсов. Условное обозначение сервера показано на рисунке 2.4.

Рис. 2.4. Условное обозначение сервера

Концентратор (Hub) — сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент. Условное обозначение концентратора показано на рисунке 2.5.

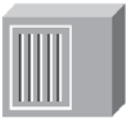

Рис. 2.5. Условное обозначение концентратора

Мост (Bridge) — устройство, которое повторяет приходящий по сети на один из его портов сигнал на все активные порты. Мост обеспечивает ограничение домена коллизий. Условное обозначение моста показано на рисунке 2.6.

Рис. 2.6. Условное обозначение моста

Коммутатор (Switch) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только получателю. Условное обозначение коммутатора показано на рисунке 2.7.

Рис. 2.7. Условное обозначение коммутатора

Многоуровневый коммутатор (Multilayer Switch) — высокопроизводительный коммутатор, способный работать на третьем и четвертом уровнях модели OSI. Условное обозначение многоуровневого коммутатора показано на рисунке 2.8.

Рис. 2.8. Условное обозначение многоуровневого коммутатора

Маршрутизатор (Router) — устройство, которое позволяет соединить локальные сети и подключаться к глобальным сетям. Условное обозначение маршрутизатора показано на рисунке 2.9.

Рис. 2.9. Условное обозначение маршрутизатора

Точка доступа (Access Point) — устройство, которое позволяет подключать беспроводные устройства к уже существующей проводной локальной сети. Точка доступа также позволяет объединить несколько компьютеров в автономную беспроводную локальную сеть, не подключенную к проводной сети. Условное обозначение точки доступа показано на рисунке 2.10.

Рис. 2.10. Условное обозначение точки доступа беспроводной сети Wi-Fi

Точка доступа беспроводной сети может быть встроена прямо в маршрутизатор. Условное обозначение маршрутизатора с точкой доступа показано на рисунке 2.11.

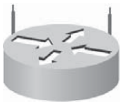

Рис. 2.11. Условное обозначение маршрутизатора с встроенной точкой доступа

Модем (Modem) — устройство, которое применяется в системах связи для физического сопряжения сигнала со средой передачи данных. В компьютерных сетях модемы обычно используются для передачи представленных в цифровой форме компьютерных данных по аналоговым телефонным линиям. Условное обозначение модема показано на рисунке 2.12. В программе Cisco Packet Tracer имеются модели модема для цифровой абонентской линии (DSL-Modem) и кабельного модема (Cable-Modem).

Рис. 2.12. Условное обозначение модема

Для обозначения подключения к внешней сети, построенной по технологии **frame relay**, используется символ в форме облака, показанный на рисунке 2.13.

Рис. 2.13. Внешняя сеть, построенная по технологии frame relay

Для соединения сетевых устройств между собой могут использоваться следующие типы кабелей:

- **Console** — консольный кабель, который подключается к портам RS-232 и используется для подсоединения внешнего терминала. С внешнего терминала можно управлять работой маршрутизатора или интеллектуального коммутатора.
- **Copper Straight-Through** — «прямой» медный кабель Ethernet на основе витой пары (UTP) с разъемами RJ-45 на концах (разводка проводов в разъемах совпадает). Прямой кабель используется для соединения персонального компьютера, сервера или маршрутизатора с концентратором или коммутатором.
- **Copper Cross-Over** — «перекрестный» медный кабель, который отличается от прямого тем, что разводка проводов в разъемах перекрестная (передатчик одного устройства должен быть соединен с приемником другого). Перекрестный кабель используется для непосредственного (без использования концентратора или коммутатора) соединения двух устройств по схеме «точка-точка».
- **Fiber** — оптоволоконный кабель. Оптоволоконный кабель обычно используется для соединения высокопроизводительного оборудования.
- **Phone** — телефонный кабель. Такой кабель может использоваться для соединения модемов.
- **Coaxial** — коаксиальный кабель. Этот тип кабеля применялся в ранних версиях технологии Ethernet.
- **Serial DCE** и **Serial DTE** — отдельные условные обозначения для каждой из сторон соединительного кабеля DCE/DTE. Тот или иной вариант выбирается в зависимости от того, является ли первое из двух соединяемых с помощью кабеля устройств источником или приемником синхросигнала. Порт маршрутизатора, к которому подключен разъем DCE (отмеченный пиктограммой часов), должен выдавать в линию сигнал синхронизации с определенной тактовой частотой, которая задается при настройке параметров порта.

Пункт **Automatically Choose Connection Type**, который идет в списке типов соединений самым первым, обозначает автоматический выбор кабеля в зависимости от того, к какому устройству производится подключение.

2.2.1. Ознакомление с пиктограммами сетевого оборудования

В данном упражнении Вам необходимо запустить на выполнение Cisco Packet Tracer и ознакомиться с пиктограммами различного сетевого оборудования, размещенными в области выбора устройства, после чего можно завершить работу с программой.

2.3. Справочные и учебные материалы

К программе Cisco Packet Tracer прилагаются справочные, учебные и демонстрационные материалы на английском языке.

Для того, чтобы получить доступ к справочным материалам, нужно выбрать пункт Help в главном меню, а затем выбрать пункт Contents в открывшемся подменю, или просто нажать функциональную клавишу **F1**.

Прежде чем вы начнете проводить эксперименты в программе Cisco Packet Tracer, вы можете просмотреть, например, следующие материалы:

- **Getting Started** — краткое руководство для тех, кто только начинает работать с Cisco Packet Tracer;
- **Interface Overview** — обзор интерфейса программы Cisco Packet Tracer;
- **My First PT Lab** — демонстрационная лабораторная работа.
- Ознакомиться с обучающими видеороликами можно, нажав функциональную клавишу **F11** или выбрав пункт **Help** в главном меню, а затем выбрав пункт Tutorials в подменю. Вы можете просмотреть следующие демонстрации:
- **Interface Overview** — обзор интерфейса;
- **Create Network Topology** — демонстрация процесса создания сетевой топологии;
- **Simulation Environment** — описание среды моделирования.

2.4. Задание для самостоятельной работы

Запустите на выполнение симулятор Cisco Packet Tracer, ознакомьтесь с учебными и справочными материалами, после чего завершите работу с программой.

3. ЛОКАЛЬНЫЕ СЕТИ НА БАЗЕ КОММУТАТОРОВ ВТОРОГО УРОВНЯ

Освоение программы Cisco Packet Tracer мы начнем с создания моделей небольших локальных сетей, состоящих из нескольких компьютеров, подключенных к концентратору или коммутатору.

3.1. Простейшая сеть из двух компьютеров

Самую простую локальную сеть можно создать, соединив Ethernet-порты двух компьютеров напрямую друг с другом (рис. 3.1) с помощью перекрестного кабеля UTP. Обычно такую сеть создают как временную — с целью выполнения быстрой передачи большого объема данных с одного компьютера на другой.

Рис. 3.1. Прямое соединение компьютеров перекрестным кабелем

3.1.1. Прямое соединение компьютеров

В этом упражнении от вас требуется создать модель простейшей локальной сети, образованной путем прямого соединения компьютеров, например — персонального компьютера и сервера, как показано на рисунке 3.1.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Выберите группу End Devices (оконечные устройства) щелчком левой кнопки мыши.
   2.2. В группе End Devices выберите устройство PC-PT (типовой персональный компьютер) щелчком левой кнопки мыши по соответствующей пиктограмме. Установите курсор мыши в том месте пространства, где вы поместить устройство, а затем снова щелкните левой кнопки мыши.
   2.3. В группе End Devices выберите устройство Server-PT (типовой сервер) и также поместите его в рабочую пространствоь.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Выберите группу Connections (соединения).
   3.2. В группе Connections выберите пиктограмму Automatically Choose Connection Type (автоматический выбор типа соединения) щелчком левой кнопки мыши, а

затем соедините устройства между собой, как показано на рис. 4.1, щелкнув левой кнопки мыши сначала по одному, а затем — по другому устройству.

4. Настройте компьютер PC0:
   4.1. Выберите в рабочем пространстве персональный компьютер PC0, щелкнув левой кнопкой мыши по пиктограмме компьютера, после чего на экране появится окно для настройки параметров выбранного устройства.
   4.2. Для того чтобы получить возможность настроить параметры Ethernet-соединения на персональном компьютере, выберите вкладку Config и нажмите кнопку FastEthernet.
   4.3. Для соединения FastEthernet выберите статическую конфигурацию IP, установив галочку в пункте Static, задайте адрес **192.168.1.1** и маску **255.255.255.0** (рис. 3.2). Другие параметры на этой вкладке оставьте без изменений.
   4.4. Закройте окно параметров персонального компьютера PC0.

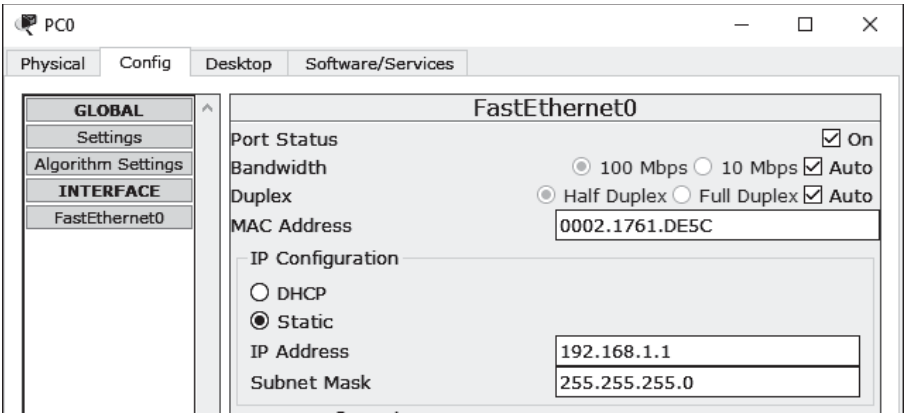

Рис. 3.2. Настройка параметров интерфейса FastEthernet на компьютере PC0

1. Настройте сервер Server0:
   1.1. Выберите в рабочем пространстве сервер Server0, щелкнув левой кнопкой мыши по пиктограмме сервера, после чего на экране появится окно для настройки параметров выбранного устройства.
   1.2. Выберите в окне Server0 вкладку Config и нажмите кнопку FastEthernet.
   1.3. Для соединения FastEthernet выберите статическую конфигурацию IP, задайте адрес **192.168.1.2** и маску **255.255.255.0**.
   1.4. Закройте окно Server0.
2. Проконтролируйте правильность настройки параметров оборудования:
   2.1. На правой панели инструментов нажмите кнопку Inspect, чтобы выбрать инструмент «Увеличительная лупа».
   2.2. Наведите лупу на компьютер PC0 и продержите в таком положении несколько секунд. После этого на экране появиться контекстная подсказка, в которой будет отображаться IP-адрес компьютера.

2.3. Наведите лупу на сервер Server0 и продержите в таком положении несколько секунд. После этого на экране появиться контекстная подсказка, в которой будет отображаться IP-адрес сервера.

3. На правой панели инструментов нажмите кнопку Select, чтобы вернуться в режим выбора устройства.
4. Проверьте состояние точек-индикаторов на концах соединительного кабеля. Эти точки имитируют работу светодиодов сетевых адаптеров, и если соединение между компьютером и сервером установлено, то они будут окрашены в **зеленый** цвет. Если точки на концах кабеля окрашены в красный цвет, то соединение отсутствует и необходимо проверить правильность настройки параметров сетевых адаптеров.
5. Переключите Cisco Packet Tracer из режима реального времени Realtime в режим пошагового моделирования Simulation.
6. Передайте icmp-пакет с компьютера на сервер, для того чтобы проверить исправность сформированного соединения:
   6.1. Нажмите на правой панели кнопку Add Simple PDU, чтобы задать режим передачи простого пакета.
   6.2. Щелкните левой кнопкой мыши по персональному компьютеру PC0, а затем — по серверу Server0, чтобы указать, что PC0 является источником, а Server0 — получателем пакета.
   6.3. Посмотрите на область отображения результатов моделирования, расположенную в правом нижнем углу окна Cisco Packet Tracer. В этой области появится сообщение «In Progress», которое показывает, что процесс передачи пакета был начат, но еще не завершен.
   6.4. Нажмите кнопку Capture / Forward. Если вы правильно настроили параметры компьютера и сервера, то вы сможете наблюдать процесс передачи пакета с компьютера на сервер.
   6.5. Посмотрите на область отображения результатов моделирования — так как процесс передачи пакета еще не завершен, в этой области по прежнему выводится сообщение «In Progress».
   6.6. Снова нажмите Capture / Forward и наблюдайте обратную передачу пакета с сервера на компьютер (передача простого пакета в Cisco Packet Tracer — это на самом деле однократное выполнение команды ping, поэтому на свой запрос PC0 получает от сервера пакет с ответом).
   6.7. Посмотрите на область отображения результатов моделирования: если процесс передачи пакета завершился успешно, в этой области выводится сообщение «Successful», а в противном случае — сообщение «Failed».
7. Посмотрите на список событий Event List — в этом списке в порядке их наступления будут перечислены все события, которые произошли в сети за время моделирования передачи пакета.
8. Просмотрите данные о первом событии в списке Event List:
   8.1. Установите курсор мыши на первую строку списка событий и щелкните левой кнопкой. В результате на экране появится диалоговое окно PDU Information, содержащее информацию о входящем и исходящем сетевых кадрах, которые участвовали в этом событии. На вкладке OSI Model будет показано, как обрабатываются эти кадры на различных уровнях модели OSI, на вкладке Inbound PDU details отображаются заголовки пакетов, вложенных во входящий кадр, а на вкладке Outbound PDU details отображаются заголовки пакетов, вложенных в исходящий кадр. В нашей модели в первом событии на компьютере PC0 участвует только исходящий кадр.
   8.2. Просмотрите информацию на вкладке OSI Model.

8.3. Выберите вкладку Outbound PDU details и просмотрите информацию о заголовках пакетов, инкапсулированных в передаваемый по сети кадр.
8.4. Закройте окно PDU Information.
9. Нажмите на кнопку очистки списка событий Reset Simulation.
10. Повторите моделирование в непрерывном режиме, нажав кнопку Auto Capture / Play.
11. Переключите Cisco Packet Tracer в режим реального времени Realtime.
12. Выберите в рабочем пространстве персональный компьютер PC0, щелкнув левой кнопкой мыши по пиктограмме компьютера.
13. Протестируйте сетевые соединения с помощью диагностических утилит из стека протоколов TCP/IP:
13.1. В окне PC0 выберите вкладку Desktop.
13.2. На вкладке Desktop нажмите кнопку Command Prompt, чтобы открыть окно, имитирующее работу операционной системы компьютера в режиме командной строки.
13.3. Введите команду **ping 192.168.1.2** и просмотрите результат ее выполнения.
13.4. Введите команду **tracert 192.168.1.2** и просмотрите результат ее выполнения (рис. 3.3).
13.5. Закройте окно Command Prompt.
14. Проверьте наличие доступа к информации, размещенной на сервере:
14.1. На вкладке Desktop нажмите кнопку Web Browser, чтобы открыть окно, имитирующее работу браузера Интернет.
14.2. В поле URL браузера введите IP-адрес сервера **http://192.168.1.2** и нажмите расположенную радом с полем URL кнопку Go. В ответ сервер должен выдать сообщение, заданное в его модели по умолчанию (рис. 3.4).
14.3. Закройте окно Web Browser.

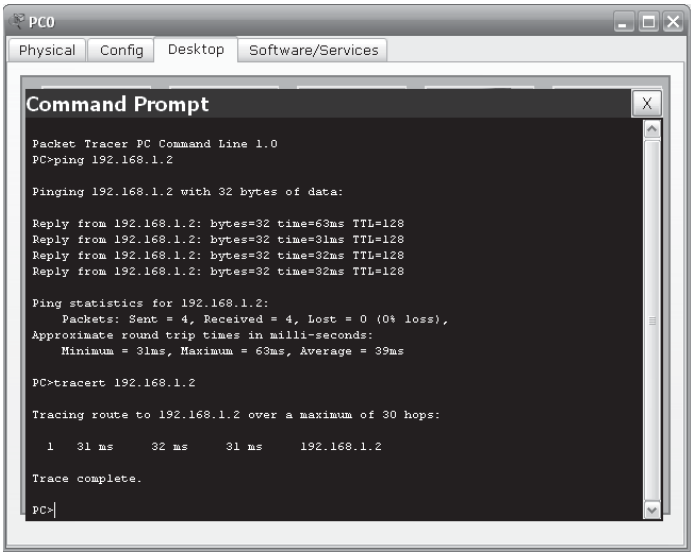

Рис. 3.3. Результаты выполнения команд ping и tracert на компьютере PC0

15. Закройте окно PC0.
16. Выберите в меню пункт File, затем подпункт Save и сохраните модель сети в файле с именем **net_3_1_1**.
17. Завершите работу с Cisco Packet Tracer, закрыв основное окно этой программы.

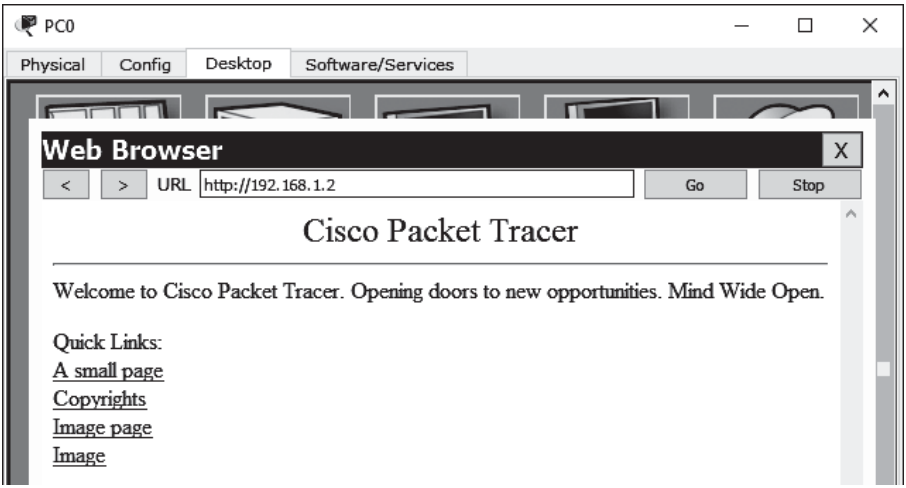

Рис. 3.4. Отображение Интернет-страницы сервера Server0 в браузере компьютера PC0

3.2. Сеть на базе концентратора

Концентратор (хаб) — это сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент. Выпускаются концентраторы со скоростью передачи данных 10 и 100 Мбит/с.

Концентратор работает на физическом уровне сетевой модели OSI, он повторяет приходящий на один порт сигнал на все остальные активные порты. Концентраторы всегда работают в **полудуплексном** режиме.

В случае поступления сигнала на два и более порта одновременно возникает **коллизия**, и передаваемые кадры данных **теряются**. Таким образом, все подключённые к концентратору устройства находятся **в одном домене коллизий**. Для защиты от излишнего количества коллизий концентратор может изолировать порт, к которому подключено неисправное устройство, от общей среды передачи.

Другая проблема, возникающая при использовании концентраторов — опасность перехвата сообщений: все пакеты доходят до всех компьютеров сети, поэтому существует возможность несанкционированного доступа к информации.

И, наконец, ещё одной проблемой является то, что копирование пакетов на все порты концентратора существенно повышает нагрузку на сеть, так как весь трафик сегмента сети поступает к каждому из компьютеров.

3.2.1. Модель сети с концентратором

В этом упражнении от вас требуется создать модель локальной сети, в которой четыре персональных компьютера объединены в сеть при помощи концентратора, как показано на рисунке 3.5.

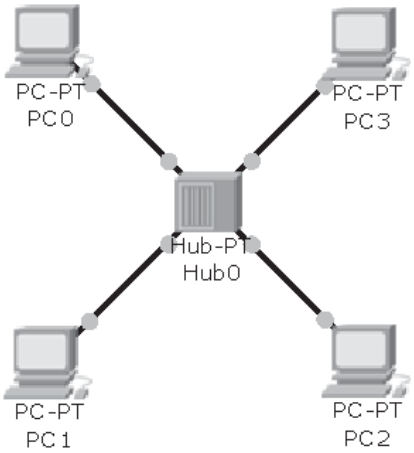

Рис. 3.5. Локальная сеть, построенная с помощью концентратора

Выполните в следующие действия:

1. Запустите Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую пространствоь Cisco Packet Tracer:
   2.1. Выберите группу End Devices. В группе End Devices выберите устройство типа PC-PT и поместите в рабочую пространствоь четыре персональных компьютера PC0-PC3.
   2.2. Выберите группу Hubs. В группе Hubs выберите устройство абстрактную модель концентратора Hub-PT (Generic) и поместите ее в рабочую пространствоь.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Выберите группу Connections.
   3.2. В группе Connections выберите пиктограмму соединительного UDP-кабеля Copper Straight-Through.
   3.3. Щелчком левой кнопки мыши по пиктограмме компьютера PC0 вызовите контекстное меню и выберите пункт FastEthernet, чтобы подключить кабель к соответствующему разъему.

3.4. Щелчком левой кнопки мыши по пиктограмме концентратора вызовите контекстное меню и выберите пункт Port 0, чтобы подключить второй конец кабеля к нулевому порту концентратора.
3.5. Аналогичным образом подключите компьютер PC1 к первому порту концентратора, компьютер PC2 — к второму порту, компьютер PC3 — к третьему порту, чтобы в итоге получилась схема, показанная на рисунке 3.5.

4. Настройте параметры сетевого адаптера на компьютере PC0, используя упрощенный метод:
4.1. Выберите в рабочем пространстве персональный компьютер PC0.
4.2. В окне PC0 выберите вкладку Desktop.
4.3. На вкладке Desktop нажмите кнопку IP Configuration, чтобы открыть окно для настройки параметров IP-соединения.
4.4. В окне IP Configuration задайте статическую конфигурацию IP, адрес **192.168.1.1** и маску **255.255.255.0**, как показано на рис. 3.6.
4.5. Закройте окно IP Configuration.
4.6. Закройте окно PC0.

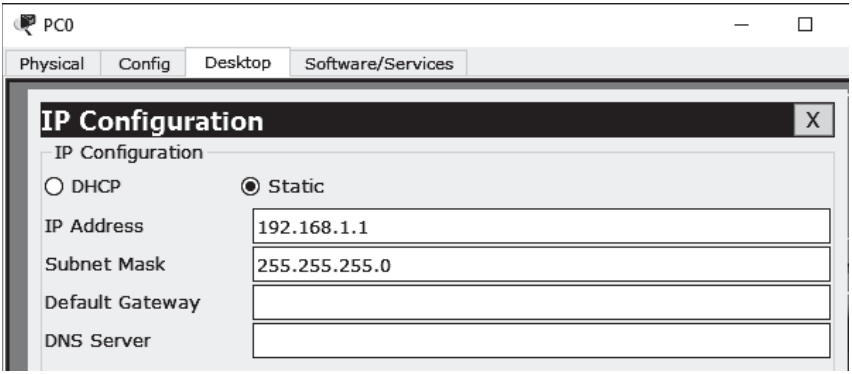

Рис. 3.6. Окно для настройки параметров IP-соединения

5. Настройте компьютер PC1: задайте IP-адрес **192.168.1.2** и маску **255.255.255.0**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.1.3** и маску **255.255.255.0**.
7. Настройте компьютер PC3: задайте IP-адрес **192.168.1.4** и маску **255.255.255.0**.
8. Переключите Cisco Packet Tracer из режима Realtime в режим пошагового моделирования Simulation.
9. Передайте icmp-пакет с компьютера PC0 на компьютер PC2:
9.1. Нажмите на правой панели кнопку Add Simple PDU, чтобы задать режим передачи простого icmp-пакета.
9.2. Щелкните левой кнопкой мыши по персональному компьютеру PC0, а затем — по PC2, чтобы указать, что PC0 является источником, а PC2 — получателем пакета.
9.3. Нажмите кнопку Capture / Forward и наблюдайте процесс передачи пакета с компьютера на концентратор.
9.4. Снова нажмите Capture / Forward и наблюдайте, как концентратор передает пакет по всем портам, кроме того, с которого был принят этот пакет. Пакет бу-

дет отправлен одновременно к компьютерам PC1, PC2 и PC3, но только PC2 сможет его принять (рис. 3.7).

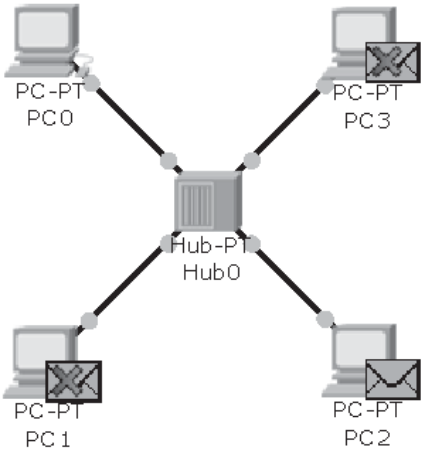

Рис. 3.7. Персональный компьютер PC2 принимает пакет от концентратора

9.5. Нажмите Capture / Forward и наблюдайте ответную передачу пакета с компьютера PC2 на концентратор.
9.6. Нажмите Capture / Forward и наблюдайте передачу пакета с концентратора на компьютеры PC0, PC1 и PC3. Принять этот пакет сможет только персональный компьютер PC0.
9.7. Просмотрите список событий Event List.
9.8. Нажмите кнопку Reset Simulation.
9.9. Повторите моделирование в непрерывном режиме, нажав кнопку Auto Capture / Play.
9.10. Нажмите кнопку Reset Simulation.
9.11. Переведите ползунок регулятора скорости моделирования, расположенный под кнопкой Auto Capture / Play, в крайнее правое положение, чтобы ускорить до максимума процесс прохождения пакетов по модели компьютерной сети.
9.12. Повторите моделирование, нажав кнопку Auto Capture / Play.
10. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
11. Смоделируйте возникновение коллизии в сети:
11.1. Нажмите на правой панели кнопку Add Simple PDU, а затем задайте в качестве источника пакета компьютер PC0, а в качестве получателя пакета — PC1.
11.2. Снова нажмите на кнопку Add Simple PDU. Задайте в качестве источника пакета компьютер PC3, а в качестве получателя пакета — PC2.
11.3. Нажмите кнопку Capture / Forward и наблюдайте коллизию, которая произойдет при попытке одновременной передачи двух пакетов данных (рис. 3.8).
11.4. Снова нажмите кнопку Capture / Forward и наблюдайте, как сигнал о возникновении коллизии передается на все подключенные к сети персональные компьютеры.
12. Сохраните модель сети в файле с именем **net_3_2_1**.
13. Завершите работу с программой Cisco Packet Tracer, закрыв основное окно.

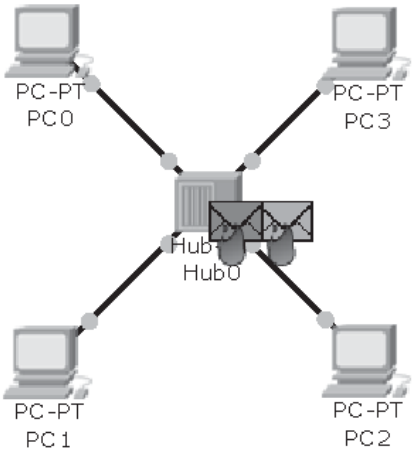

Рис. 3.8. Возникновение коллизия при попытке одновременной передачи данных

3.3. Сеть на базе коммутатора второго уровня

Коммутатор (свитч) — это устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только получателю (исключение составляет широковещательные сообщения всем узлам сети). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости обрабатывать данные, которые им не предназначались.

Коммутатор работает на канальном уровне модели OSI.

Коммутатор хранит в памяти таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры и, определив MAC-адрес узла-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для узла, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес узла-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется.

3.3.1. Модель сети с коммутатором

В этом упражнении от вас требуется создать модель локальной сети, в которой четыре персональных компьютера объединены в одноуровневую сеть при помощи коммутатора, как показано на рисунке 3.9.

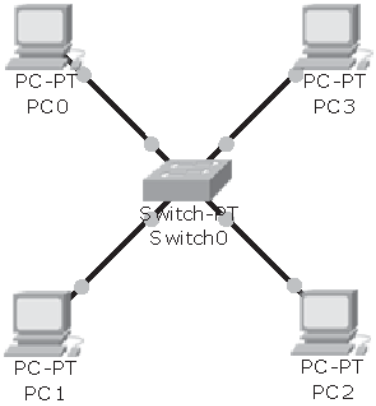

Рис. 3.9. Локальная сеть, построенная с помощью коммутатора

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство персональные компьютеры PC0, PC1, PC2 и PC3.
   2.2. Выберите группу Switches. В группе Switches выберите абстрактную модель коммутатора Switch-PT (Generic) и поместите ее в рабочее пространство.
3. Подключите все компьютеры к коммутатору при помощи прямого медного кабеля.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1** и маску **255.255.255.0**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.1.2** и маску **255.255.255.0**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.1.3** и маску **255.255.255.0**.
7. Настройте компьютер PC3: задайте IP-адрес **192.168.1.4** и маску **255.255.255.0**.
8. Подождите, пока все цветные точки, имитирующие работу светодиодных индикаторов на Ethernet-портах коммутатора, сменят цвет с красного на зеленый, показывая, что коммутатор привел эти порты в рабочее состояние.
9. На правой панели инструментов выберете лупу, наведите ее на коммутатор и продержите в таком положении несколько секунд. После этого на экране появиться контекстная подсказка, в которой отображается состояние портов коммутатора: порты, к которым подключены компьютеры, должны находиться в состоянии Up.
10. Переключите Cisco Packet Tracer из режима реального времени Realtime в режим пошагового моделирования Simulation.
11. Передайте простой пакет с компьютера PC0 на компьютер PC2 и обратно, используя пошаговый режим моделирования.

12. Просмотрите список событий Event List.
13. Нажмите кнопку Reset Simulation.
14. Переведите ползунок регулятора скорости моделирования в крайнее правое положение.
15. Повторите моделирование в непрерывном режиме, нажав кнопку Auto Capture/Play.
16. В области сценария нажмите кнопку Delete, чтобы очистить сценарий моделирования.
17. Передайте с компьютера PC0 ограниченное широковещательное сообщение в сеть:
    17.1. На правой панели инструментов нажмите кнопку Add Complex PDU, чтобы создать сложный пакет, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши. В результате на экране появится диалоговое окно Create Complex PDU.
    17.2. Укажите в списке Outgoing Port (передающий порт) порт **FastEthernet**.
    17.3. В списке Select Application (выбор приложения) укажите **PING**.
    17.4. В поле Destination IP Address (адрес получателя) задайте широковещательный адрес **255.255.255.255**.
    17.5. В поле Source IP Address (адрес источника) задайте IP-адрес компьютера PC0 **192.168.1.1**.
    17.6. В поле времени жизни пакета TTL задайте значение **32**.
    17.7. В поле типа обслуживания TOS задайте используемое протоколом ICMP значение **0**.
    17.8. В поле Sequence Number (номер последовательности) задайте значение **1**.
    17.9. В поле параметров моделирования выберете пункт One Shot (выполнить однократно) и задайте начальное время Time равным 0. В результате окно Create Complex PDU должно иметь вид, показанный на рисунке 3.10.

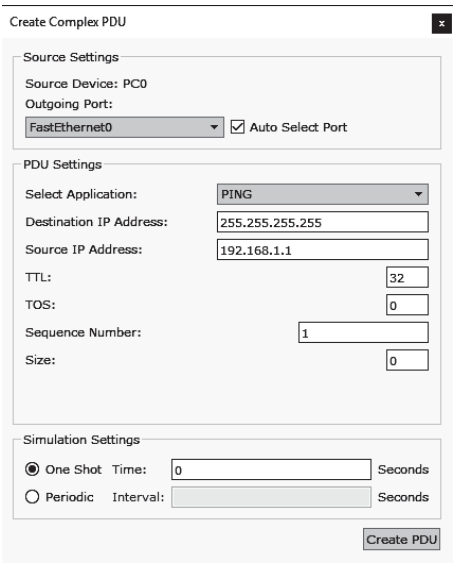

Рис. 3.10. Диалоговое окно для создания сложного пакета

17.10. Нажмите в нижней части окна кнопку Create PDU, чтобы завершить процесс создания пакета.

18. Проследите за тем, как протекает процесс передачи сообщения:
    18.1. Нажмите кнопку Capture/Forward и наблюдайте процесс передачи пакета с компьютера PC0 на коммутатор.
    18.2. Снова нажмите Capture/Forward и наблюдайте одновременную передачу трех копий широковещательного пакета на компьютеры PC1, PC2 и PC3.
    18.3. Нажмите кнопку Capture/Forward и наблюдайте процесс передачи ответных пакетов с компьютеров PC1, PC2 и PC3 на коммутатор. Передать компьютеру PC0 все пакеты одновременно коммутатор не сможет, поэтому они накапливаются в буфере коммутатора (рис. 3.11).
    18.4. Три раза подряд нажимайте кнопку Capture/Forward и наблюдайте поочередную передачу пакетов с коммутатора на компьютер PC0.

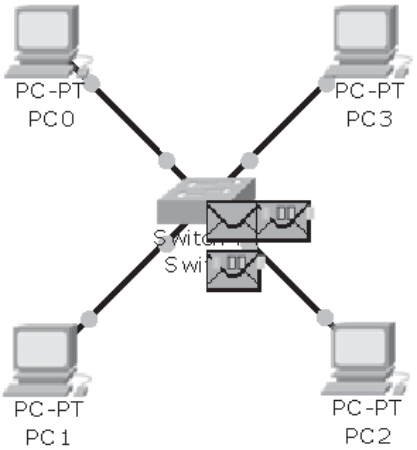

Рис. 3.11. Накопление пакетов в буфере коммутатора

19. В области сценария нажмите кнопку Delete, чтобы очистить сценарий моделирования.
20. Разделите сеть на две логические части:
    20.1. Измените IP-адрес компьютера PC2, задав значение **192.168.2.1**.
    20.2. Измените IP-адрес компьютера PC3, задав значение **192.168.2.2**. Теперь компьютеры PC0 и PC1 находятся в одной подсети, а компьютеры PC2 и PC3 — в другой. Подсети в этом случае оказываются изолированными друг от друга, и между ними будут передаваться только широковещательные пакеты.
21. Передайте простой пакет с компьютера PC0 на компьютер PC1.
22. Передайте простой пакет с компьютера PC2 на компьютер PC3.
23. Попытайтесь передать простой пакет с компьютера PC0 на компьютер PC2 (попытка должна завершиться неудачей, так как эти компьютеры теперь находятся в разных подсетях).

24. В области сценария нажмите кнопку Delete, чтобы очистить сценарий моделирования.
25. Повторите эксперимент с передачей пакета с компьютера PC0 в ограниченном широковещательном режиме. Пакет должен дойти до компьютеров PC1, PC2 и PC3, но принять его и послать ответ сможет только компьютер PC1, который входит в ту же подсеть, что и компьютер PC0.
26. Просмотрите список событий Event List.
27. Нажмите кнопку Capture / Forward и снова посмотрите на список событий. В списке событий кроме используемых в данном примере пакетов ICMP могут наблюдаться также пакеты, автоматически рассылаемые самим сетевым оборудованием, например — пакеты протоколов ARP, STP, CDP и DTP.
28. Для того чтобы посторонние пакеты не отображались на экране и в списке событий, нужно настроить режим фильтрации пакетов:
    28.1. Нажмите кнопку Edit Filters (редактирование фильтров).
    28.2. В открывшемся безымянном диалоговом окне снимите галочку в пункте Show All/None.
    28.3. Установите галочку в пункте ICMP.
    28.4. Переместите курсор за пределы диалогового окна.
    28.5. Закройте диалоговое окно щелчком левой или правой кнопки мыши.
29. Нажмите кнопку Reset Simulation.
30. Повторите моделирование в непрерывном режиме, нажав кнопку Auto Capture / Play. Теперь события, связанные с передачей посторонних пакетов, не имеющих отношения к протоколу ICMP, в списке событий отображаться не будут, но они продолжают накапливаться в буфере событий.
31. Если сразу после завершения передачи пакета вы не остановите процесс моделирования (путем повторного нажатия кнопки Auto Capture / Play), то через некоторое время буфер событий будет переполнен — вы увидите на экране сообщение «The maximum number of events has been reached». Если вы получили подобное сообщение, то в окне сообщения нажмите кнопку View Previous Events.
32. Сохраните модель сети в файле с именем **net_3_3_1**.
33. Завершите работу с программой Cisco Packet Tracer.

3.4. Древовидная топология связей

Выше мы рассматривали простые сети, которые можно использовать, когда количество соединяемых компьютеров невелико (измеряется десятками) и они расположены на небольшом расстоянии друг от друга в одном помещении или нескольких смежных помещениях.

Для того, чтобы создать более крупную сеть, ее приходится разделять на части, подключать каждую из частей к отдельному коммутатору, а коммутаторы соединять друг с другом высокоскоростными линиями связи. Концентраторы для создания крупных сетей в настоящее время уже не используются, так как не выгодно держать в одном домене коллизий большое количество компьютеров.

В крупных сетях для соединения коммутаторов используются многоуровневые структуры с древовидной топологией связей: на нижнем уровне размещаются дешевые коммутаторы со сравнительно низкой пропускной способностью, к которым подключаются персональные компьютеры, а для объединения этих коммутаторов в единую сеть используются мощные дорогие устройства, обладающие высокой пропускной спо-

собностью и способные работать на третьем уровне модели OSI (коммутаторы третьего уровня).

В настоящее время обычно применяется иерархическая модель сети, показанная на рисунке 3.12. Эта модель включает в себя три логических уровня:

- уровень доступа;
- уровень распределения;
- уровень ядра.

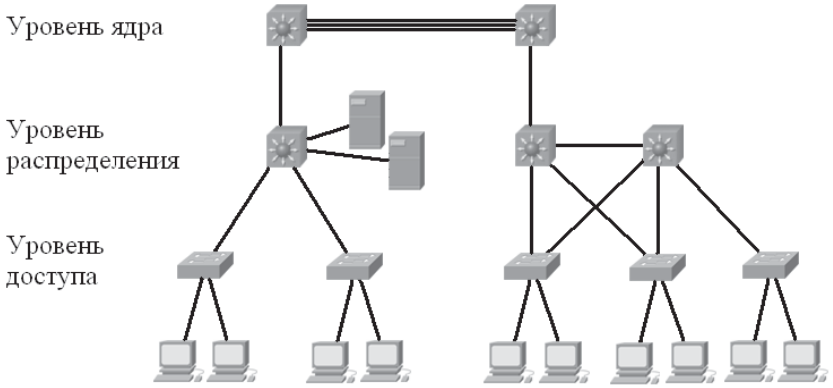

Рис. 3.12. Трехуровневая иерархическая модель сети

Каждый уровень выполняет строго определенные функции:

- уровень доступа управляет доступом пользователей к ресурсам сети;
- уровень распределения служит связующим звеном между уровнями доступа и ядра;
- уровень ядра находится в верхней части иерархии и отвечает за надежную и быструю передачу больших объемов данных.

3.5. Создание резервных линия связи между коммутаторами

Если обрыв кабеля между компьютером и коммутатором приводит к отключению от локальной сети только этого конкретного компьютера, то обрыв кабеля, соединяющего коммутаторы между собой, приводит к тому, что сеть распадается на отдельные изолированные сегменты и компьютеры из разных сегментов не могут связаться друг с другом.

Основным приемом защиты сети от обрыва кабелей является создание **резервных соединений**, однако в сетях, построенных на базе коммутаторов, при добавлении резервных соединений образуются петли, в которых передаваемые по сети пакеты будут зацикливаться. Поэтому в коммутаторы встроена защита от зацикливания пакетов, которая блокирует передачу данных по резервным линиям до тех пор, пока основные линии связи сохраняют работоспособность.

Для предотвращения образования петель коммутаторы используют **протокол остовного дерева** (Spanning Tree Protocol, сокращенно **STP**) — сетевой протокол, работающий на втором уровне модели OSI. Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии. Происходит это путём автоматического блокирования избыточных связей.

Протокол STP описан в стандарте IEEE 802.1D. Принцип действия протокола STP следующий:

1) В сети выбирается один корневой мост.
2) Далее каждый, отличный от корневого, мост просчитывает кратчайший путь к корневому мосту. Соответствующий этому пути порт называется корневым. У любого не корневого коммутатора может быть только один корневой порт.
3) После этого для каждого сегмента сети просчитывается кратчайший путь к корневому порту. Мост, через который проходит этот путь, становится назначенным для этой сети, а непосредственно подключенный к сети порт моста — назначенным портом.
4) Далее на всех мостах блокируются все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура с вершиной в виде корневого коммутатора.

Корневым назначается коммутатор с самым низким значением идентификатора Bridge ID (BID). Если BID у двух коммутаторов одинаков, то корневым станет коммутатор с наименьшим MAC-адресом.

3.5.1. Сеть с резервной линией связи

В этом упражнении от вас требуется создать модель локальной сети, в которой три коммутатора соединены друг с другом, как показано на рисунке 3.13.

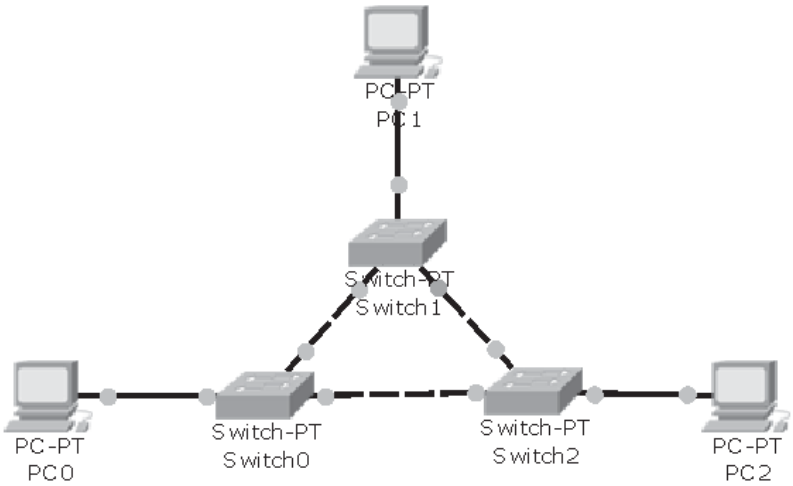

Рис. 3.13. Локальная сеть, в которой все коммутаторы соединены друг с другом

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Создайте сеть, состоящую из трех компьютеров и трех коммутаторов (рис. 3.13).
3. Настройте параметры компьютера PC0: задайте IP-адрес **192.168.1.1** и маску **255.255.255.0**.
4. Настройте параметры компьютера PC1: задайте IP-адрес **192.168.1.2** и маску **255.255.255.0**.
5. Настройте параметры компьютера PC2: задайте IP-адрес **192.168.1.3** и маску **255.255.255.0**.
6. Нажмите кнопку Fast Forward Time, размещенную под рабочим пространством, чтобы временно ускорить процесс моделирования.
7. Проверьте состояние портов коммутаторов: на всех портах, кроме одного, должны появиться зеленые сигналы.
8. Сохраните модель сети в файле с именем **net_3_5_1**.
9. Переключите Cisco Packet Tracer из режима Realtime в режим Simulation.
10. Проверьте все сетевые соединения путем поочередной передачи в пошаговом режиме простых пакетов с компьютера PC0 на компьютер PC1, с компьютера PC1 на компьютер PC2 и с компьютера PC2 на компьютер PC0. По какому маршруту пойдет каждый из этих пакетов?
11. Нажмите на правой панели инструментов кнопку Delete (красный крестик).
12. Наведите крестик на одну из активных линий связи между коммутаторами (оба конца активной линии отмечены зелеными точками), и щелкните левой кнопкой мыши, чтобы разорвать эту связь.
13. Перейдите в режим Realtime и дождитесь завершения активации резервной линии связи.
14. Вернитесь в режим Simulation.
15. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
16. Повторите поочередную передачу пакетов с PC0 на PC1, с PC1 на PC2 и с PC2 на PC0.
17. Завершите работу с программой Cisco Packet Tracer.

3.6. Динамическое распределение IP-адресов

Если к локальной сети подключены сотни компьютеров, то присвоение компьютерам IP-адресов вручную становится для администратора сети трудоемкой задачей.

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, сокращенно **DHCP**) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Протокол DHCP работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- Ручное распределение: администратор сети сопоставляет аппаратному адресу (MAC-адресу) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной

настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

- Автоматическое распределение: каждому компьютеру в постоянное пользование выделяется произвольный свободный IP-адрес из определённого администратором диапазона адресов.
- Динамическое распределение: свободный IP-адрес выдаётся компьютеру не на постоянное пользование, а в аренду на определённый срок. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Часто используются следующие опции:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

В качестве DHCP-сервера в локальной сети может использоваться маршрутизатор или сервер.

3.6.1. Настройка сервиса DHCP на сервере

В этом упражнении от вас требуется создать модель локальной сети, в которой за распределение IP-адресов отвечает сервер (рис. 3.14).

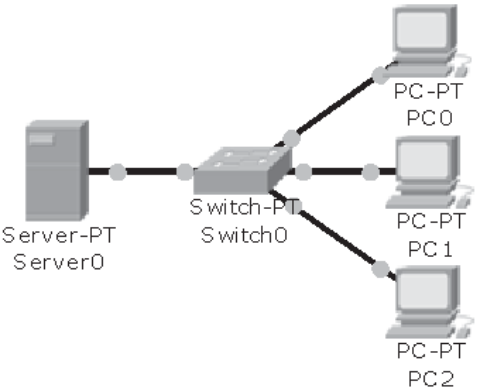

Рис. 3.14. Локальная сеть, в которой за распределение IP-адресов отвечает сервер

Выполните в следующие действия:

1. Создайте модель локальной сети, состоящую из сервера, коммутатора и трех компьютеров PC0-PC2, соединенных между собой показанным на рисунке 3.14 способом.
2. Настройте параметры сервера:

2.1. Выберите в рабочем пространстве сервер Server0.
2.2. Выберите в окне Server0 вкладку Config и нажмите кнопку FastEthernet.
2.3. Для соединения FastEthernet выберите статическую конфигурацию IP, задайте адрес **192.168.1.1** и маску **255.255.255.0**.
2.4. Выберите в окне Server0 вкладку Services.
2.5. На вкладке Services нажмите кнопку DHCP.
2.6. Настройте параметры сервиса DHCP: задайте начальный IP-адрес (Start IP Address) **192.168.1.10**, маску подсети **255.255.255.0**, максимальное число пользователей (Maximum number of users) — **200**, а затем нажмите кнопку Save. В результате выполнения указанных действий изображение в окне Server0 должно иметь вид, показанный на рисунке рис. 3.15.
2.7. Закройте окно Server0.

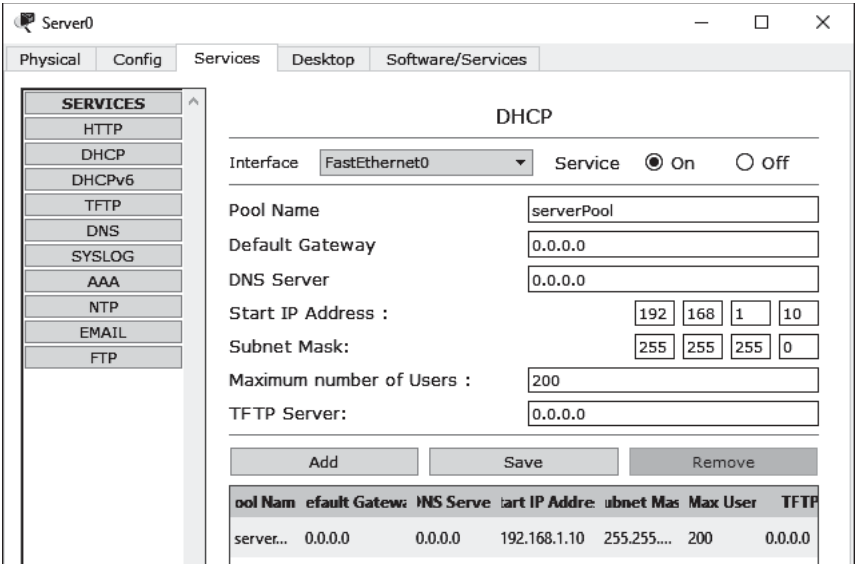

Рис. 3.15. Диалоговое окно для настройки сервиса DHCP на сервере

3. Настройте параметры компьютера PC0:
3.1. Выберите в рабочем пространстве компьютер PC0.
3.2. В окне PC0 выберите вкладку Config и нажмите кнопку FastEthernet.
3.3. Задайте сетевому адаптеру режим конфигурирования IP-адреса с помощью DHCP, установив соответствующий флажок, как показано на рисунке 3.16.
3.4. Закройте окно PC0.

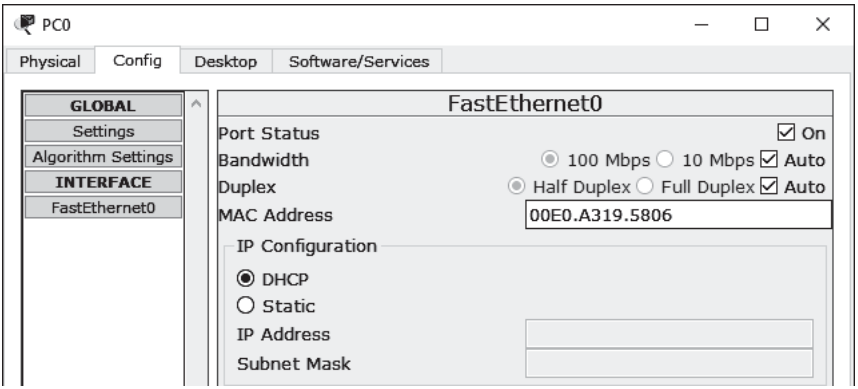

Рис. 3.16. Настройка сетевого адаптера компьютера на использование DHCP

4. Аналогичным образом настройте на использование DHCP сетевые адаптеры компьютеров PC1 и PC2.
5. Нажмите кнопку Fast Forward Time, размещенную под рабочим пространством, чтобы временно ускорить процесс моделирования. Наведите курсор мыши поочередно на каждый компьютер, подождите до появления всплывающей подсказки и проверьте значение IP-адреса.
6. Переключитесь в режим Simulation.
7. Проверьте сетевые соединения путем поочередной передачи простых пакетов с каждого из компьютеров на сервер.
8. Передайте с компьютера PC0 широковещательное сообщение в сеть:
   8.1. На правой панели инструментов нажмите кнопку Add Complex PDU, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши. В результате на экране появится диалоговое окно Create Complex PDU.
   8.2. Укажите в списке Outgoing Port порт **FastEthernet**.
   8.3. В списке Select Application укажите **PING**.
   8.4. В поле Destination IP Address задайте широковещательный адрес **192.168.1.255**.
   8.5. В поле времени жизни пакета TTL задайте значение **32**.
   8.6. В поле типа обслуживания TOS задайте значение **0**.
   8.7. В поле Sequence Number задайте значение **1**.
   8.8. В поле параметров моделирования выберете пункт One Shot и задайте начальное время Time равным 0.
   8.9. Нажмите кнопку Create PDU, чтобы завершить процесс создания пакета.
9. В пошаговом режиме проследите за рассылкой сообщения.
10. Повторите предыдущий эксперимент, используя адрес **255.255.255.255** для рассылки ограниченного широковещательного сообщения.
11. Переключите Cisco Packet Tracer в режим Realtime.
12. Выберите в рабочем пространстве компьютер PC0.
13. Откройте вкладку Physical, установите курсор мыши на красную кнопку (рис. 3.17), изображающую выключатель питания на модели корпуса системного блока и щелчком левой кнопки мыши имитируйте отключение питания компьютера (светодиод над кнопкой должен погаснуть), после чего закройте окно PC0.
14. Аналогичным образом отключите питание компьютеров PC1 и PC2.

15. Включите питание компьютеров в следующем порядке: вначале питание PC2, затем — PC1, затем — PC0.
16. Нажмите кнопку Fast Forward Time, чтобы временно ускорить процесс моделирования.
17. Используя лупу, определите, какие IP-адреса присвоены компьютерам. Какой способ распределения адресов использует в данном случае DHCP-сервер?
18. Проверьте соединение — передайте простой пакет с PC0 на PC2.
19. Сохраните модель сети в файле с именем **net_3_6_1**.
20. Завершите работу с программой Cisco Packet Tracer.

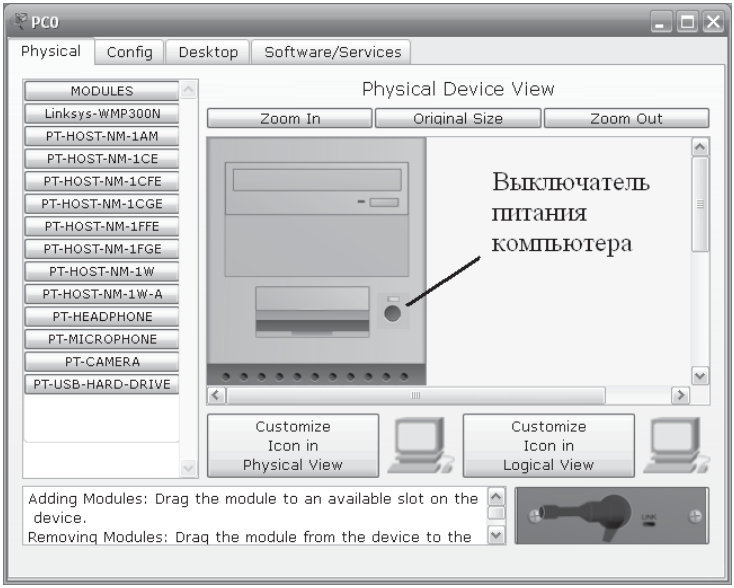

Рис. 3.17. Расположение выключателя питания на модели корпуса компьютера

3.7. Задание для самостоятельной работы

Создайте и настройте модель локальной сети, состоящей из четырех компьютеров и двух коммутаторв (рисунок 3.18).

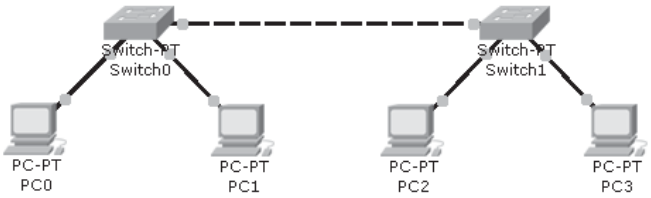

Рис. 3.18. Сеть, состоящая из четырех компьютеров и двух коммутаторов

4. УПРОЩЕННЫЙ РЕЖИМ НАСТРОЙКИ МОДЕЛЕЙ МАРШРУТИЗАТОРОВ

Главным препятствием для создания большой компьютерной сети с помощью одних только коммутаторов является быстрый рост объёма широковещательного трафика при увеличении количества подключенных к сети устройств, так как подобная сеть представляет собой единый широковещательный домен. Для решения данной проблемы необходимо разделить сеть на подсети и соединить их в единое целое с помощью маршрутизаторов.

Маршрутизатор представляет собой **многофункциональное устройство**, в задачи которого входит построение таблиц маршрутизации, определение маршрута, буферизация, фрагментация и фильтрация поступающих пакетов, поддержка сетевых интерфейсов. Маршрутизатор обеспечивает соединение на сетевом уровне модели OSI.

Маршрутизаторы позволяют соединять компьютерные сети с одинаковыми или разными средами передачи данных. Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры.

4.1. Настройка параметров в окне модели маршрутизатора

Для создания простых моделей компьютерных сетей необходимо настроить только несколько основных параметров работы портов маршрутизатора. В этом случае Cisco Packet Tracer позволяет обходиться без использования команд операционной системы Cisco IOS и настраивать порты в упрощенном режиме, используя вкладку Config в окне модели маршрутизатора.

Следует, однако, иметь в виду, что такой способ настройки доступен только для моделей, а в реальных устройствах настройка параметров выполняется с помощью команд Cisco IOS.

4.1.1. Модель сети с маршрутизатором

В этом упражнении от вас требуется настроить сеть из двух компьютеров, подключенных к разным портим маршрутизатора (рис. 4.1).

Рис. 4.1. Сеть, состоящая из маршрутизатора и двух компьютеров

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство компьютеры PC0 и PC1.
   2.2. В группе Routers выберите абстрактную модель маршрутизатора Router-PT (Generic) и поместите ее в рабочем пространстве между компьютерами.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet1/0 маршрутизатора Router0.
4. Настройте компьютер PC0:
   4.1. Выберите в рабочем пространстве компьютер PC0.
   4.2. В окне PC0 выберите вкладку Config. На этой вкладке по умолчанию должна открыться область настройки глобальных параметров Global Settings.
   4.3. Задайте статический режим настройки шлюза (установив для этого переключатель Gateway/DNS в положение Static) и введите адрес шлюза **192.168.1.1** (рис. 4.2).
   4.4. На вкладке Config нажмите кнопку FastEthernet.
   4.5. Задайте для адаптера сети Fast Ethernet статическую конфигурацию IP, адрес **192.168.1.2** и маску **255.255.255.0**.
   4.6. Закройте окно PC0.

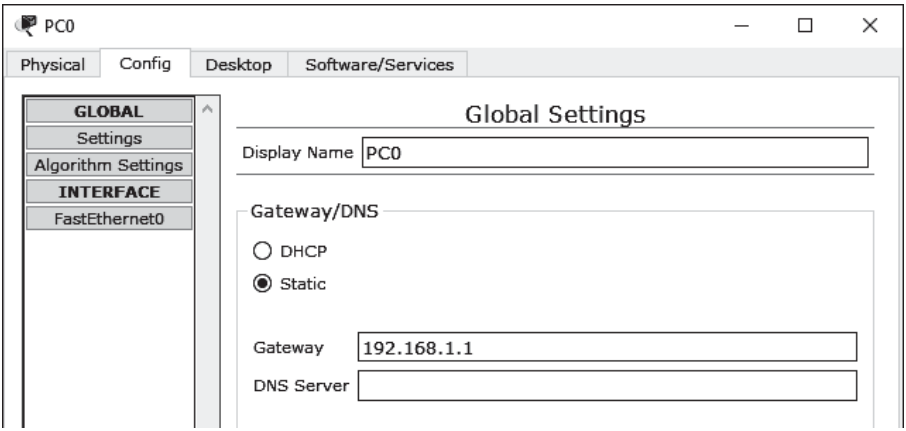

Рис. 4.2. Настройка глобальных параметров для компьютера PC0

5. Настройте параметры сетевого адаптера на компьютере PC1, используя упрощенный метод:
   5.1. Выберите в рабочем пространстве персональный компьютер PC1.
   5.2. В окне PC1 выберите вкладку Desktop.
   5.3. На вкладке Desktop нажмите кнопку IP Configuration.

5.4. В окне IP Configuration задайте статическую конфигурацию IP, IP-адрес **192.168.2.2**, маску **255.255.255.0** и адрес шлюза **192.168.2.1**.
5.5. Закройте окно IP Configuration.
5.6. Закройте окно PC1.

6. Настройте маршрутизатор Router0:
6.1. Выберите в рабочем пространстве маршрутизатор Router0.
6.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
6.3. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.1.1** и маску **255.255.255.0** (рис. 4.3).
6.4. В окне Router0 нажмите кнопку FastEthernet1/0.
6.5. Для интерфейса FastEthernet1/0 задайте статус порта On, адрес **192.168.2.1** и маску **255.255.255.0**.
6.6. Закройте окно Router0.

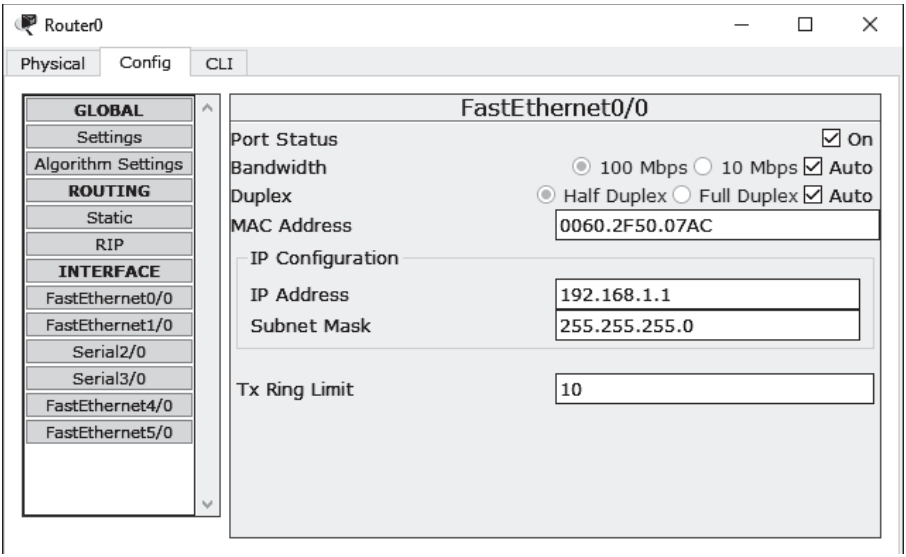

Рис. 4.3. Окно настройки параметров порта маршрутизатора

7. Проверьте таблицу маршрутизации:
7.1. На правой панели инструментов нажмите кнопку Inspect.
7.2. Наведите лупу на маршрутизатор и щелкните левой кнопкой мыши, для того чтобы вызвать контекстное меню.
7.3. Выберете в меню пункт Routing Table, чтобы открыть таблицу маршрутизации.
7.4. Просмотрите таблицу маршрутизации: в таблице должны присутствовать строки, описывающие сети **192.168.1.0** и **192.168.2.0**.
7.5. Закройте окно Routing Table for Router0.

8. Проверьте таблицу ARP:
8.1. Наведите лупу на маршрутизатор и щелкните левой кнопкой мыши, чтобы вызвать контекстное меню.

8.2. Выберете в меню пункт ARP Table, для того чтобы открыть таблицу ARP.
8.3. Просмотрите таблицу ARP.
8.4. Закройте окно ARP Table for Router0.
9. Переключите Cisco Packet Tracer в режим Simulation.
10. Проверьте соединение между компьютерами путем передачи простого пакета с PC0 на PC1 в режиме Auto Capture / Play.
11. Если первая попытка передачи оказалась неудачной (завершилась сообщением Failed), так как маршрутизатор не успел построить путь из одной сети в другую, то нажмите кнопку Reset Simulation, а затем повторите передачу пакета, снова нажав кнопку Auto Capture / Play.
12. Сохраните модель сети в файле с именем **net_4_1_1**.
13. Завершите работу с программой Cisco Packet Tracer.

4.1.2. Модель сети с маршрутизатором и двумя коммутаторами

Рассмотрим пример использования маршрутизатора для объединения двух подсетей. Для начала создадим сеть без маршрутизатора, состоящую из двух коммутаторов и четырех компьютеров (рис. 4.4).

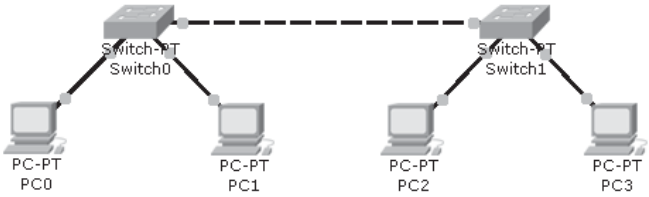

Рис. 4.4. Сеть, состоящая из двух коммутаторов и четырех компьютеров

Выполните в следующие действия:
1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую пространствоь Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство компьютеры PC0, PC1, PC2 и PC3.
   2.2. В группе Switches выберите модель коммутатора Switch-PT (Generic) и поместите в рабочее пространство коммутаторы Switch0 и Switch1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите прямым кабелем компьютер PC0 к порту FastEthernet0/1 коммутатора Switch0.
   3.2. Подключите прямым кабелем компьютер PC1 к порту FastEthernet1/1 коммутатора Switch0.
   3.3. Подключите прямым кабелем компьютер PC2 к порту FastEthernet0/1 коммутатора Switch1.
   3.4. Подключите прямым кабелем компьютер PC3 к порту FastEthernet1/1 коммутатора Switch1.
   3.5. Подключите перекрестным кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet2/1 коммутатора Switch1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1** и маску **255.255.255.0**.

5. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2** и маску **255.255.255.0**.
6. Настройте компьютер PC0: задайте IP-адрес **192.168.2.1** и маску **255.255.255.0**.
7. Настройте компьютер PC0: задайте IP-адрес **192.168.2.2** и маску **255.255.255.0**.
8. Нажмите кнопку Fast Forward Time, чтобы ускорить процесс самонастройки коммутаторов.
9. Проверьте состояние коммутаторов: на всех портах должны появиться зеленые сигналы.
10. Сохраните модель сети в файле с именем **net_4_1_2a**.
11. Передайте простой пакет с PC0 на PC1.
12. Передайте простой пакет с PC2 на PC3.
13. Попытайтесь передайте простой пакет с PC0 на PC3 — пакет в этом случае передаваться не должен.
14. Переключите Cisco Packet Tracer в режим пошагового моделирования Simulation.
15. Передайте с компьютера PC0 ограниченное широковещательное сообщение в сеть:
    15.1. На правой панели инструментов нажмите кнопку Add Complex PDU, чтобы создать сложный пакет, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши.
    15.2. В окне Create Complex PDU укажите в списке Outgoing Port порт **FastEthernet**.
    15.3. В списке Select Application укажите **PING**.
    15.4. В поле Destination IP Address задайте широковещательный адрес **255.255.255.255**.
    15.5. В поле Source IP Address задайте адрес компьютера PC0 **192.168.1.1**.
    15.6. В поле времени жизни пакета TTL задайте значение **32**.
    15.7. В поле типа обслуживания TOS задайте значение **0**.
    15.8. В поле Sequence Number задайте значение **1**.
    15.9. В поле параметров моделирования выберете пункт One Shot и задайте начальное время Time равным **0**.
    15.10. Нажмите кнопку Create PDU, чтобы завершить процесс создания пакета.
    15.11. В пошаговом режиме проследите за рассылкой сообщения.
16. Попробуйте повторить предыдущий эксперимент, используя адрес 192.168.2.255 для рассылки широковещательного сообщения с компьютера PC0 в сеть 192.168.2.0. Что в результате произойдет и почему?
17. Установите между коммутаторами маршрутизатор:
    17.1. Нажмите на правой панели инструментов кнопку Delete. Наведите крестик на кабель, соединяющий коммутаторы, и удалите его, чтобы разорвать соединение.
    17.2. В группе Routers выберите модель Router-PT (Generic) и поместите ее в рабочее пространство между коммутаторами, как показано на рисунке 4.5.
    17.3. Подключите прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
    17.4. Подключите прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet1/0 маршрутизатора Router0.

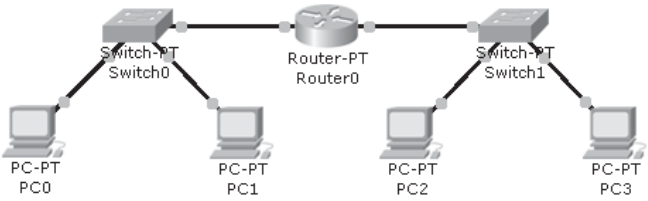

Рис. 4.5. Модель сети после подключения маршрутизатора

18. Настройте маршрутизатор:
    18.1. Выберите в рабочем пространстве маршрутизатор Router0.
    18.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
    18.3. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.1.254** и маску **255.255.255.0**.
    18.4. В окне Router0 нажмите кнопку FastEthernet1/0.
    18.5. Для интерфейса FastEthernet1/0 задайте статус порта On, адрес **192.168.2.254** и маску **255.255.255.0**, а затем закройте окно Router0.
19. Проведите дополнительную настройку компьютеров: для PC0 задайте адрес шлюза **192.168.1.254**, для PC1 задайте адрес шлюза **192.168.1.254**, для PC2 задайте адрес шлюза **192.168.2.254**, для PC3 задайте адрес шлюза **192.168.2.254**
20. Нажмите кнопку Fast Forward Time, чтобы ускорить процесс самонастройки маршрутизатора.
21. Проверьте таблицу маршрутизации:
    21.1. На правой панели инструментов нажмите кнопку Inspect.
    21.2. Наведите лупу на маршрутизатор и щелкните левой кнопкой мыши, чтобы вызвать меню.
    21.3. Выберете в меню пункт Routing Table, чтобы просмотреть таблицу маршрутизации.
    21.4. Просмотрите таблицу маршрутизации: в таблице должны присутствовать строки, описывающие сети 192.168.1.0 и 192.168.2.0.
    21.5. Закройте окно Routing Table for Router0.
22. Проверьте соединение между компьютерами путем передачи простого пакета с PC0 на PC3. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет. Если и второй пакет не передается — проверьте правильность настройки параметров маршрутизатора и персональных компьютеров.
23. Передайте с компьютера PC0 широковещательное сообщение в сеть:
    23.1. На правой панели инструментов нажмите кнопку Add Complex PDU, чтобы создать сложный пакет, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши.
    23.2. В окне Create Complex PDU укажите в списке Outgoing Port порт **FastEthernet**.
    23.3. В списке Select Application укажите **PING**.
    23.4. В поле Destination IP Address задайте широковещательный адрес **192.168.2.255**.
    23.5. В поле Source IP Address задайте адрес компьютера PC0 **192.168.1.1**.
    23.6. В поле времени жизни пакета TTL задайте значение **32**.
    23.7. В поле типа обслуживания TOS задайте значение **0**.

23.8. В поле Sequence Number задайте значение **1**.
23.9. В поле параметров моделирования выберете пункт One Shot и задайте начальное время Time равным **0**.
23.10. Нажмите кнопку Create PDU, чтобы завершить процесс создания пакета.
24. В пошаговом режиме проследите за рассылкой широковещательного сообщения. Пакет будет доходить только до порта маршрутизатора, ведущего в сеть 192.168.2.0, после чего маршрутизатор сам сформирует ответный пакет.
25. Сохраните модель сети в файле с именем **net_4_1_2b**.
26. Завершите работу с программой Cisco Packet Tracer.

4.2. Протокол маршрутизации RIP

Если количество маршрутизаторов в невелико, то они обычно используют для обмена маршрутной информацией самый простой из протоколов маршрутизации — дистанционно-векторный протокол **сбора маршрутной информации** (Routing Information Protocol, сокращенно — **RIP**).

При использовании этого протокола для настройки маршрутизации достаточно указать только сети, непосредственно примыкающие к маршрутизатору.

4.2.1. Модель сети с двумя маршрутизаторами

Рассмотрим упрощенный способ настройки RIP через окно параметров модели маршрутизатора, для чего мы создадим сеть, состоящую из двух маршрутизаторов и двух компьютеров (рис. 4.6).

Рис. 4.6. Сеть, состоящая из двух маршрутизаторов и двух компьютеров

Выполните в следующие действия:
1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство компьютеры PC0 и PC1.
   2.2. Поместите в рабочее пространство маршрутизаторы Router0 и Router1 типа Router-PT.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем компьютер PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем компьютер PC1 к порту FastEthernet0/0 маршрутизатора Router1.
   3.3. Соедините перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 и порт FastEthernet1/0 маршрутизатора Router1.

4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1**, маску **255.255.255.0**. и шлюз **192.168.1.254**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**. и шлюз **192.168.2.254**.
6. Настройте маршрутизатор Router0:
   6.1. Выберите в рабочем пространстве маршрутизатор Router0.
   6.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   6.3. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.1.254** и маску **255.255.255.0**.
   6.4. На вкладке Config нажмите кнопку FastEthernet1/0.
   6.5. Для интерфейса FastEthernet1/0 задайте статус порта On, адрес **192.168.3.1** и маску **255.255.255.0**.
   6.6. На вкладке Config нажмите кнопку RIP, после чего должна открыться область для настройки параметров протокола маршрутизации RIP Routing.
   6.7. В поле Network введите номер сети **192.168.1.0** и нажмите кнопку Add.
   6.8. В поле Network введите номер сети **192.168.3.0** и нажмите кнопку Add. После этого окно Router0 должно иметь вид, изображенный на рисунке 4.7.
   6.9. Закройте окно Router0.

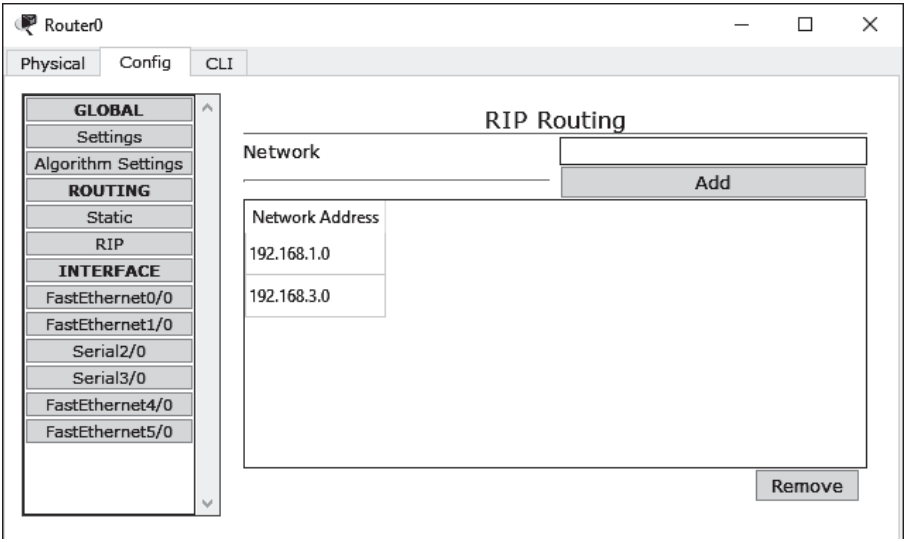

Рис. 4.7. Настройка параметров протокола RIP

7. Настройте маршрутизатор Router1:
   7.1. Выберите в рабочем пространстве маршрутизатор Router1.
   7.2. В окне Router1 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   7.3. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.2.254** и маску **255.255.255.0**.

7.4. На вкладке Config нажмите кнопку FastEthernet1/0.
7.5. Для интерфейса FastEthernet1/0 задайте статус порта On, адрес **192.168.3.2** и маску **255.255.255.0**.
7.6. На вкладке Config нажмите кнопку RIP.
7.7. В поле Network введите номер сети **192.168.2.0** и нажмите кнопку Add, затем введите номер сети **192.168.3.0** и снова нажмите кнопку Add.
7.8. Закройте окно Router1.

8. Используя лупу, проверьте таблицу маршрутизации на маршрутизаторе Router0: в таблице должны присутствовать сети **192.168.1.0**, **192.168.2.0** и **192.168.3.0**, а окно с таблицей должно иметь вид, показанный на рисунке 4.8.

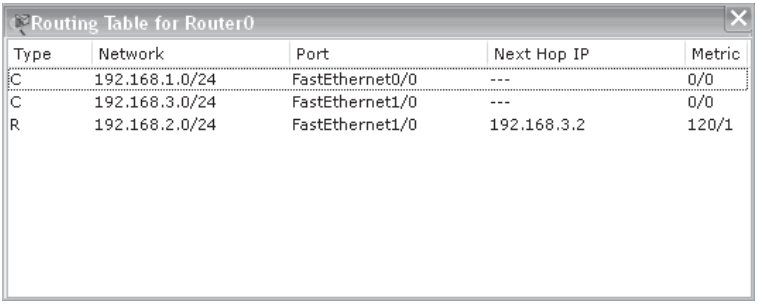

Рис. 4.8. Таблица маршрутизации протокола RIP

9. Используя лупу, проверьте таблицу маршрутизации на маршрутизаторе Router1: в таблице также должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0.
10. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет. Если и второй пакет не передается — проверьте правильность настройки параметров маршрутизаторов и компьютеров.
11. Сохраните модель сети в файле с именем **net_4_2_1**.
12. Выделите сразу два объекта: установите курсор мыши над маршрутизатором Router1, нажмите левую кнопку мыши, и, удерживая ее, переместите курсор таким образом, чтобы он оказался под компьютером PC1, после чего отпустите кнопку мыши.
13. Нажмите на верхней панели инструментов кнопку New Cluster, чтобы сгруппировать выделенные объекты в кластер Cluster0 (рис. 4.9).
14. Установите курсор мыши на кластер Cluster0 и щелкните левой кнопкой, чтобы развернуть кластер в рабочем пространстве и посмотреть на состав входящего в него оборудования.
15. Нажмите на верхней панели инструментов кнопку Back, чтобы снова свернуть кластер.
16. Завершите работу с программой Cisco Packet Tracer.

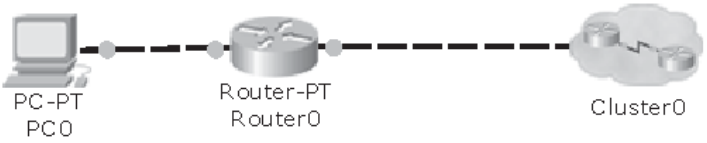

Рис. 4.9. Объединение объектов в кластер

4.3. Петлевидные соединения между маршрутизаторами

Использование резервных линий связи порождает в компьютерных сетях проблему петель, в которых могут зацикливаться передаваемые по сети пакеты.

Маршрутизаторы, в отличие от концентраторов и коммутаторов, выстраивают для передачи пакетов определенный, по возможности — оптимальный маршрут, и проблема зацикливания актуальна только для пакетов, содержащих маршрутную информацию. Чтобы предотвратить зацикливание таких пакетов, используется метод расщепления горизонта, который заключается в том, что информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается тому маршрутизатору, от которого она получена.

4.3.1. Модель сети с петлевидным соединением маршрутизаторов

В качестве примера рассмотрим сеть, в которой три маршрутизатора соединены друг с другом (рис. 4.10).

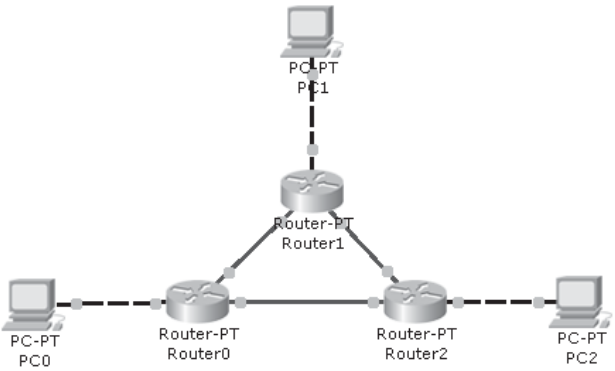

Рис. 4.10. Сеть с петлевидным соединением маршрутизаторов

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:

2.1. Поместите в рабочее пространство маршрутизаторы типа Router-PT Router0, Router1 и Router2.
2.2. Поместите в рабочее пространство компьютеры PC0, PC1 и PC2.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
3.1. Подключите перекрестным кабелем компьютер PC0 к порту FastEthernet0/0 маршрутизатора Router0.
3.2. Подключите перекрестным кабелем компьютер PC1 к порту FastEthernet0/0 маршрутизатора Router1.
3.3. Подключите перекрестным кабелем компьютер PC2 к порту FastEthernet0/0 маршрутизатора Router2.
3.4. В группе Connections выберите пиктограмму оптоволоконного кабеля Fiber. Подключите оптоволоконным кабелем порт FastEthernet4/0 маршрутизатора Router0 к порту FastEthernet5/0 маршрутизатора Router1.
3.5. Подключите оптоволоконным кабелем порт FastEthernet4/0 маршрутизатора Router1 к порту FastEthernet5/0 маршрутизатора Router2.
3.6. Подключите оптоволоконным кабелем порт FastEthernet4/0 маршрутизатора Router2 к порту FastEthernet5/0 маршрутизатора Router0.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1**, маску **255.255.255.0**. и шлюз **192.168.1.254**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**. и шлюз **192.168.2.254**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.3.1**, маску **255.255.255.0**. и шлюз **192.168.3.254**.
7. Настройте маршрутизатор Router0:
7.1. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.1.254** и маску **255.255.255.0**.
7.2. Для интерфейса FastEthernet4/0 задайте статус порта On, адрес **192.168.4.1** и маску **255.255.255.0**.
7.3. Для интерфейса FastEthernet5/0 задайте статус порта On, адрес **192.168.6.1** и маску **255.255.255.0**.
7.4. Для протокола RIP добавьте в таблицу RIP Routing сети **192.168.1.0**, **192.168.4.0** и **192.168.6.0**.
8. Настройте маршрутизатор Router1:
8.1. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.2.254** и маску **255.255.255.0**.
8.2. Для интерфейса FastEthernet4/0 задайте статус порта On, адрес **192.168.5.1** и маску **255.255.255.0**.
8.3. Для интерфейса FastEthernet5/0 задайте статус порта On, адрес **192.168.4.2** и маску **255.255.255.0**.
8.4. Для интерфейса FastEthernet5/0 задайте статус порта **On**, адрес **192.168.4.2** и маску **255.255.255.0**.
8.5. Для протокола RIP добавьте в таблицу RIP Routing сети **192.168.2.0**, **192.168.4.0** и **192.168.5.0**.
9. Настройте маршрутизатор Router2:
9.1. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.3.254** и маску **255.255.255.0**.
9.2. Для интерфейса FastEthernet4/0 задайте статус порта On, адрес **192.168.6.2** и маску **255.255.255.0**.
9.3. Для интерфейса FastEthernet5/0 задайте статус порта On, адрес **192.168.5.2** и маску **255.255.255.0**.

9.4. Для протокола RIP добавьте в таблицу RIP Routing сети **192.168.3.0**, **192.168.4.0** и **192.168.6.0**.

10. Используя лупу, проверьте таблицы маршрутизации: в таблице каждого из маршрутизаторов должны присутствовать сети 192.168.1.0–192.168.6.0 (к некоторым сетям в таблице может быть указано по два маршрута). Если какая-то из таблиц неполна, то нажмите кнопку Fast Forward Time и повторите проверку. Если повторная проверка по-прежнему выявляет неполноту таблиц маршрутизации, то нужно проверить настройку маршрутизаторов.
11. Переключите Cisco Packet Tracer в режим Simulation.
12. Для того чтобы проверить работоспособность сети, в пошаговом режиме поочередно передайте простые пакеты с компьютера PC0 на компьютер PC1, с компьютера PC1 на компьютер PC2 и с компьютера PC2 на компьютер PC0. Пакеты должны перемещаться по кратчайшим маршрутам. Если в процессе передачи пакета происходит сбой, то нажмите кнопку Reset Simulation и повторите передачу. Если же и повторная попытка завершилась неудачей — проверьте настройку оборудования.
13. Для того чтобы очистить сценарий моделирования, в области сценария нажмите кнопку Delete.
14. Нажмите кнопку Delete на правой панели инструментов, наведите крестик на оптоволоконную линию связи между маршрутизаторами Router0 и Router2 и удалите ее.
15. Сразу после разрыва соединения в пошаговом режиме попробуйте передать простой пакет с компьютера PC2 на компьютер PC0. Маршрутизатор Router2 обнаружит обрыв линии связи, передаст компьютеру PC2 сообщение о потере пакета и начнет строить новый маршрут к сети 192.168.1.0.
16. Для того, чтобы ускорить процесс построения нового маршрута, нажмите кнопку Fast Forward Time.
17. В пошаговом режиме повторите передачу простого пакета с компьютера PC2 на компьютер PC0 — на этот раз пакет должен пройти по маршруту, проложенному маршрутизаторами в обход разорванной линии связи.
18. Сохраните модель сети в файле с именем **net_4_3_1**.
19. Завершите работу с программой Cisco Packet Tracer.

4.4. Настройка параметров последовательных портов

Последовательные каналы связи обычно применяются для передачи данных на большие расстояния.

Когда маршрутизаторы соединяются последовательным каналом непосредственно друг с другом, без использования промежуточного оборудования, следует учитывать, что такое соединение не является симметричным — на одном из концов кабеля должен находиться тактовый генератор, задающий скорость передачи данных по каналу и обеспечивающий синхронизацию. Ведущее устройство, обеспечивающее синхронизацию передачи данных на последовательном канале, обозначается как DCE (Data Circuit Equipment), а ведомое устройство — как DTE (Data Terminal Equipment).

4.4.1. Настройка последовательного канала связи

В качестве примера рассмотрим сеть, в которой два маршрутизатора соединены друг с другом последовательным каналом связи (рис. 4.11).

Рис. 4.11. Непосредственное соединение маршрутизаторов с помощью последовательного канала связи

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство персональные компьютеры PC0 и PC1.
   2.2. Поместите в рабочее пространство маршрутизаторы Router0 и Router1 типа Router-PT.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем компьютер PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем компьютер PC1 к порту FastEthernet0/0 маршрутизатора Router1
   3.3. В группе Connections выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial2/0 маршрутизатора Router0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1**, маску **255.255.255.0**. и шлюз **192.168.1.254**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**. и шлюз **192.168.2.254**.
6. Настройте маршрутизатор Router0:
   6.1. Выберите в рабочем пространстве маршрутизатор Router0.
   6.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   6.3. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.1.254** и маску **255.255.255.0**.
   6.4. В окне Router0 нажмите кнопку Serial2/0.
   6.5. Для интерфейса Serial2/0 задайте статус порта On, частоту тактового генератора передатчика (Clock Rate) **56000**, адрес **192.168.3.1** и маску **255.255.255.0** (рис. 4.12).
   6.6. В окне Router0 нажмите кнопку RIP, после чего должна открыться область для настройки параметров протокола маршрутизации RIP Routing.
   6.7. В поле Network введите номер сети **192.168.1.0** и нажмите кнопку Add, затем введите номер сети **192.168.3.0** и нажмите кнопку Add.
   6.8. Закройте окно Router0.
7. Настройте маршрутизатор Router1:
   7.1. Для интерфейса FastEthernet0/0 задайте статус порта On, адрес **192.168.2.254** и маску **255.255.255.0**.
   7.2. Для интерфейса Serial2/0 задайте статус порта On, скорость передачи Not set (скорость не задана), адрес **192.168.3.2** и маску **255.255.255.0**.

7.3. Для протокола RIP добавьте в таблицу RIP Routing сети **192.168.2.0** и **192.168.3.0**.

8. Проверьте таблицы маршрутизации на маршрутизаторах Router0 и Router1: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0.
9. Переключите Cisco Packet Tracer в режим Simulation.
10. В пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1.
11. Сохраните модель сети в файле с именем **net_4_4_1**.
12. Завершите работу с программой Cisco Packet Tracer.

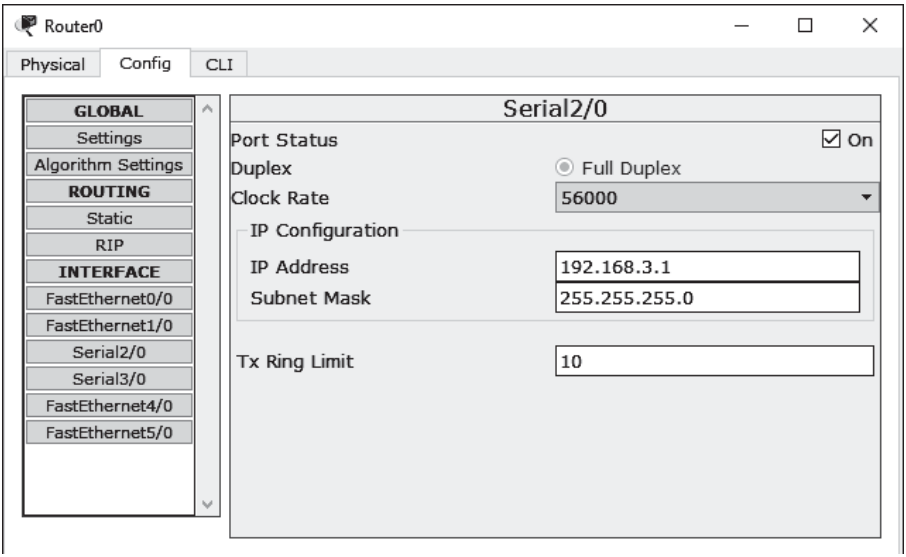

Рис. 4.12. Окно для настройки параметров последовательного интерфейса

4.5. Задание для самостоятельной работы

В целях тренировки попробуйте самостоятельно создать и наладить модель сети, изображенной на рисунке 4.13 (сеть должна состоять из пяти компьютеров и пяти маршрутизаторов типа Router-PT, маршрутизаторы должны быть соединены последовательными каналами связи).

Проведите проверку работоспособности построенной вами модели сети. Когда модель будет отлажена, сохраните ее в файле с именем net_4_5.

Разорвите одно из соединений между маршрутизаторами и убедитесь, что в сети будет построен обходной маршрут

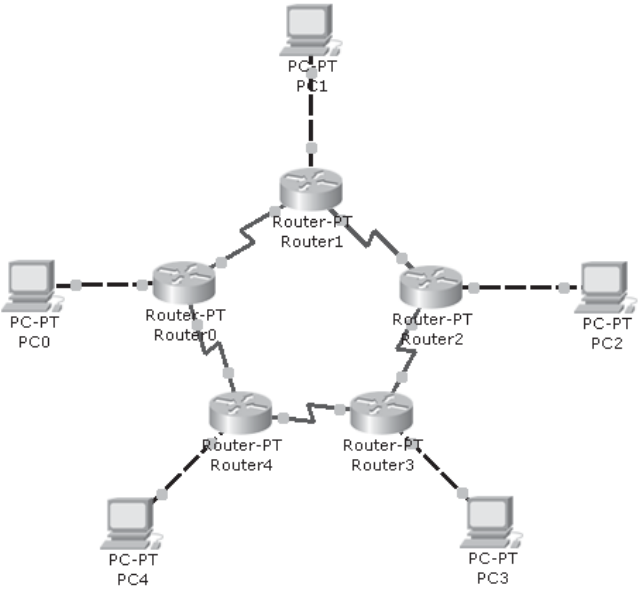

Рис. 4.13. Задание для самостоятельной работы

5. ЗНАКОМСТВО С CISCO IOS

С помощью упрощенного оконного интерфейса в программе Cisco Packet Tracer можно настроить только некоторые (самые важные) параметры модели устройства. Возможность настройки любых параметров сетевого оборудования может быть реализована только путем подачи управляющих команд специализированной операционной системы Cisco IOS.

5.1. Командный интерпретатор Exec

Cisco Internetwork Operating System (**IOS**) — операционная система, работающая на управляемых коммутаторах и маршрутизаторах Cisco. Она содержит полный набор инструментов, необходимых администратору для настройки сетевого оборудования. Один из этих инструментов, командный интерпретатор Exec, служит основой, на которой выполняется Cisco IOS.

Командный интерпретатор Cisco IOS имеет два уровня. Нижний уровень, выполняющий основную интерпретацию команд, называется **интерпретатором пользовательского режима**. Верхний уровень — это **интерпретатор привилегированного режима**.

Пользовательский интерфейс Cisco IOS включает в себя четыре основных компонента: сообщения о состоянии, запросы на ввод, приглашение IOS на ввод команды и курсор.

Приглашение на ввод в командной строке Cisco IOS подразделяется на две логических части: имя устройства и индикатор режима. Имя присваивается сетевому устройству администратором, оно произвольно и время от времени может меняться.

Вторая часть приглашения на ввод — это индикатор режима. Символ «>» показывает, что администратор вошел в систему в пользовательском режиме, а для обозначения привилегированного режима используется символ «#».

Когда пользователь регистрируется на коммутаторе или маршрутизаторе Cisco, по умолчанию он находится в пользовательском режиме. Доступ к устройству в пользовательском режиме не требует пароля. В этом режиме пользователь может выполнить большинство основных команд, таких как просмотр характеристик устройства или временное изменение настроек терминала.

Второй уровень доступа — это привилегированный режим работы интерпретатора Exec. В привилегированном режиме администратор может получить доступ ко всем функциям сетевого устройства. Этот режим дает ему доступ к средствам, позволяющим конфигурировать интерфейсы, соединяться с внешними источниками, загружать протоколы, перемещать и удалять файлы. В целях обеспечения безопасности доступ к привилегированному режиму командного интерпретатора может быть закрыт паролем.

Если приглашение на ввод команды между именем устройства и индикатором режима содержит слова в скобках, то эти слова указывают на используемый подрежим конфигурирования:

- config — подрежим глобального конфигурирования;
- config-if — подрежим конфигурирования интерфейса;
- config-subif — подрежим конфигурирования подинтерфейса;
- config-router — подрежим конфигурирования маршрутизатора.

Интерпретатор Exec позволяет сокращать длинные слова в командах, как правило — до двух символов, Ввод каждой команды завершается нажатием клавиши Enter.

Если какая-либо команда выдает большой объем информации, который не помещается на экране, то информация будет отображаться порциями, а в конце каждой порции будет выводиться запрос «--More--» на вывод следующей порции. В ответ на этот запрос можно нажать клавишу Enter, чтобы вывести следующую строку данных, или клавишу Space (пробел), чтобы вывести следующую страницу данных.

Командный интерпретатор позволяет использовать в командной строке для редактирования вводимого текста следующие **управляющие клавиши** и **комбинации клавиш**:

- нажатие клавиши ↑ переводит курсор в конец предыдущей строки в предыстории команд;
- нажатие клавиши ↓ переводит курсор в конец следующей строки в предыстории команд;
- нажатие клавиши ← переводит курсор на одну позицию влево;
- нажатие клавиши → переводит курсор на одну позицию вправо;
- нажатие клавиши Back Space позволяет удалить символ слева от курсора;
- нажатие клавиши Tab позволяет автоматически дополнить сокращенную форму команды до ее полной формы (например, если после ввода команды conf нажать клавишу Tab, то эта команда в командной строке будет преобразована в полную форму — configure);
- нажатие комбинации клавиш Ctrl+A возвращает курсор к началу строки;
- нажатие комбинации клавиш Ctrl+E перемещает курсор в конец строки;
- нажатие комбинации клавиш Ctrl+R приводит к повторному отображению командной строки (повторное отображение нужно в тех случаях, когда выводимые устройством сообщения мешают вводить команду);
- нажатие комбинации клавиш Ctrl+U приводит к полной очистке строки;
- нажатие комбинации клавиш Ctrl+Z позволяет выйти из текущего режима конфигурирования на более высокий уровень.

5.2. Справочная система IOS

В Cisco IOS встроена всеобъемлющая справочная система. Чтобы получить доступ к основным функциям справочной системы, введите **help** в ответ на приглашение на ввод команды.

Возвращаемое командой help сообщение показывает, что существует два уровня помощи. Первый уровень называют полной справкой. Полная справка используется, когда требуется определить, какие команды могут быть выполнены в командной строке, а также для того, чтобы узнать, какие команды можно выполнять совместно с другими командами.

Обратиться за помощью можно в любом месте команды, введя знак вопроса.

Предусмотрены два типа справки:

- **Полная справка** доступна, когда вы вводите символ «?» вместо аргумента команды (например, «show ?») и хотите получить описание всех возможных аргументов.
- **Частичная справка** предоставляется, когда вы вводите неполное название аргумента и хотите узнать, какие аргументы совпадают с вводом (например, «show pr?»).

5.2.1. Использование справочной системы

В этом упражнении от вас требуется войти в пользовательский режим работы Cisco IOS и получить подсказку по системе команд коммутатора.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите в рабочее пространство коммутатор Switch0 типа Switch-PT и выберите его щелчком левой кнопки мыши.
3. В окне Switch0 выберете вкладку CLI, чтобы войти в режим имитации настройки параметров коммутатора с внешнего терминала.
4. Если коммутатор находится в состоянии загрузки операционной системы после включения питания, то необходимо дождаться ее окончания.
5. В ответ на запрос «Press RETURN to get started!» («Нажмите Enter для начала работы!») нажмите клавишу Enter.
6. Когда в командной строке появится приглашение Switch>, введите знак вопроса и нажмите клавишу Enter, после чего просмотрите список команд коммутатора, который будет выеден на экран.
7. В командной строке введите текст **show ?** и нажмите клавишу Enter, после чего просмотрите список всех аргументов команды show.
8. В командной строке введите текст **show t?** и нажмите клавишу Enter, после чего просмотрите список аргументов команды show, название которых начинается с буквы «t».
9. Закройте окно Switch0.
10. Завершите работу с программой Cisco Packet Tracer.

5.3. Команды IOS для базовой настройки оборудования

Настройка коммутаторов и маршрутизаторов Cisco должна выполняться в привилегированном режиме работы командной оболочки.

Для перехода из пользовательского режима исполнения команд в привилегированный используется команда **enable** (сокращенно — **en**), которая имеет следующий формат:

enable [*privilege-level*]

где *privilege-level* — уровень привилегий, который может иметь значение в диапазоне от 1 до 15.

Уровень привилегий с номером 1 соответствует пользовательскому режиму исполнения команд, а уровень с номером 15 — привилегированному режиму. Параметр privilege-level не является обязательным, и если он не указан, то устанавливается максимальное значение кода уровня привилегий и устройство после выполнения команды enable переходит в привилегированный режим.

Для того чтобы выйти из привилегированного режима после завершения настройки устройства применяется команда **disable** (сокращенно — **disa**), которая имеет следующий формат:

disable [*privilege-level*]

где *privilege-level* — уровень привилегий.

Обычно команды enable и disable используются без параметров — для входа в привилегированный режим исполнения команд и для выхода из привилегированного режима соответственно.

Для того чтобы войти в режим глобального конфигурирования, в привилегированном режиме требуется подать команду **configure terminal** (сокращенно — **conf t**).

В процессе изготовления оборудования всем маршрутизаторам Cisco присваивается один и тот же символьный псевдоним Router, а коммутаторам присваивается псевдоним Switch. Для того, чтобы можно было настраивать сетевые устройства дистанционно, их нужно как-то различать друг от друга. Присвоить новый псевдоним устройству можно с помощью команды **hostname** (сокращенно — **ho**), которая имеет следующий формат:

```
hostname name
```

где *name* — символьный псевдоним, который должен быть присвоен устройству. Длина псевдонима может составлять от 1 до 254 символов. В псевдониме допускается использование латинских символов, арабских цифр, тире и подчеркивания. Пробелы внутри псевдонима не допускаются.

Оборудование от изготовителей к потребителям поступает с «заводскими» настройками, при использовании которых пароли на доступ к этому оборудованию не заданы. Для того чтобы ограничить доступ к устройству через консоль, нужно в режиме конфигурирования ввести последовательность команд:

```
line con 0
password password
login
```

где *password* — пароль длиной от 1 до 80 символов (допускается использование любых символов, включая пробел, но при этом пароль не должен начинаться с цифры и пробел не может следовать за цифрой).

После ввода этой последовательности команд при каждой попытке подключения через консоль устройство будет запрашивать у пользователя указанный в команде password пароль.

Если устройство выводит свои сообщения на консоль во время ввода команды, то процесс ввода нарушается, что очень неудобно для пользователей. Для того чтобы прерванная команда автоматически повторно выводилась в командной строке, нужно добавить к приведенной выше последовательности команду logging synchronous (сокращенно — logg syn).

При использовании заводских настроек доступ к командной строке разрешен только через консоль. Если необходимо организовать дистанционный доступ к устройству по протоколам Telnet или SSH, то администратор должен задать пароль для виртуальных линий связи (vty). Обычно задают общий пароль сразу для всех доступных виртуальных линий (с номерами от 0 до 15) при помощи следующей последовательности команд:

```
line vty 0 15
password password
login
```

где *password* — пароль длиной от 1 до 80 символов.

По умолчанию пароли для доступа к устройству хранятся в памяти этого устройства в незашифрованном виде. Для того чтобы включить режим шифрования паролей, нужно подать команду service password-encryption (сокращенно — serv pas).

Для того чтобы предупредить пользователей о том, что несанкционированный доступ к устройству запрещен, перед запросом на ввод пароля на экран полагается выводить соответствующее сообщение (баннер). Для вывода баннера применяется команда **banner motd** (сокращенно — **ban mo**), которая имеет следующий формат:

```
banner motd message
```

где *message* — текстовая строка, содержащая выводимое на экран сообщение и ограниченная с двух сторон символами-разделителями (в качестве разделителей можно использовать одинаковые символы, которые не встречаться внутри строки).

Для того чтобы предотвратить несанкционированное изменение настройки оборудования посторонними лицами, доступ к привилегированному режиму исполнения команд администратор также должен защитить паролем. Такой пароль может храниться в памяти устройства в виде незашифрованной или зашифрованной текстовой строки.

Незашифрованный пароль для доступа к привилегированному режиму можно задать с помощью команды enable password (сокращенно — **ena pas**), которая имеет следующий формат:

```
enable password password
```

где *password* — пароль длиной от 1 до 25 символов (допускается использование любых символов, включая пробел, но при этом пароль не должен начинаться с цифры).

Хранить пароль в виде незашифрованной строки опасно. Для того чтобы пароль сохранялся в зашифрованном виде, вместо команды enable password нужно использовать команду enable secret (сокращенно — **ena sec**), которая имеет следующий формат:

```
enable secret password
```

где password — пароль длиной от 1 до 25 символов.

Если для доступа к привилегированному режиму был задан пароль, то устройство будет запрашивать его после подачи команды enable.

При вводе паролей следует учитывать, что интерпретатор Exec различает заглавные и строчные символы. В процессе ввода пароли в командной строке не отображаются, то есть совершенно невидимы ни для администратора, ни для сторонних наблюдателей.

Для того чтобы выйти из режима (или любого подрежима) конфигурирования в привилегированный режим, нужно подать команду **end**.

Проверить правильность настройки параметров можно с помощью команды **show running-config** (сокращенно — **sh run**).

После завершения настройки нужно сохранить новую конфигурацию параметров устройства в энергонезависимой памяти (NVRAM) путем копирования файла текущей конфигурации в файл стартовой конфигурации, для чего требуется подать команду **copy running-config startup-config** (сокращенно — **copy run sta**). Когда устройство выдаст запрос на ввод имени файла для сохранения конфигурации «Destination filename [startup-config]?», можно в ответ просто нажать клавишу Enter и информация будет записана в файл, используемый по умолчанию.

Для того, чтобы полностью завершить работу с устройством и разорвать соединение с ним, в пользовательском режиме требуется подать команду **exit** (сокращенно — **ex**).

Команду exit также можно использовать для того, чтобы выйти из текущего режима на более высокий уровень (например, из привилегированного режима перейти в пользовательский),

5.3.1. Ограничение доступа к маршрутизатору

В этом упражнении от вас требуется присвоить маршрутизатору имя и установить пароли для доступа к маршрутизатору с консоли и виртуальных терминалов.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите в рабочее пространство маршрутизатор Router0 типа Router-PT и выберите его щелчком левой кнопки мыши.
3. В окне Router0 выберите вкладку CLI, чтобы использовать интерфейс командной строки CLI для настройки параметров маршрутизатора.
4. Если маршрутизатор находится в состоянии загрузки операционной системы после включения питания, то необходимо дождаться ее окончания.
5. Если на экране выведен запрос «Continue with configuration dialog? [yes/no]:» («Продолжить настройку параметров в диалоговом режиме?»), то с клавиатуры введите символ n и нажмите клавишу Enter.
6. В ответ на запрос «Press RETURN to get started!» («Нажмите Enter для начала работы!») нажмите клавишу Enter.
7. Когда в командной строке появится приглашение Router>, введите команду **enable** и нажмите клавишу Enter, для того чтобы включить привилегированный режим настройки маршрутизатора.
8. Когда в командной строке появится приглашение Router#, введите команду **configure terminal** и нажмите клавишу Enter, для того чтобы включить режим конфигурирования маршрутизатора с внешнего терминала.
9. Когда в командной строке появится приглашение Router(config)#, введите команду **hostname R0** и нажмите клавишу Enter, для того чтобы присвоить маршрутизатору имя R0.
10. Когда в командной строке появится приглашение R0(config)#, введите команду **service password-encryption** и нажмите клавишу Enter, для того чтобы включить шифрование паролей доступа к устройству.
11. Когда в командной строке появится приглашение R0(config)#, введите команду **line con 0** и нажмите клавишу Enter, чтобы войти в режим настройки линии связи с консолью.
12. Когда в командной строке появится приглашение R0(config-line)#, введите команду **password pas1** и нажмите клавишу Enter, чтобы задать пароль для доступа с консоли.
13. Когда в командной строке появится приглашение R0(config-line)#, введите команду **login** и нажмите клавишу Enter, чтобы разрешить использование введенного выше пароля для аутентификации пользователя.
14. Когда в командной строке появится приглашение R0(config-line)#, введите команду **exit** и нажмите клавишу Enter, чтобы вернуться в режим конфигурирования устройства.

15. Когда в командной строке появится приглашение R0(config)#, введите команду **line vty 0** 15 и нажмите клавишу Enter, чтобы войти в режим настройки линий связи с виртуальными терминалами.
16. Когда в командной строке появится приглашение R0(config-line)#, введите команду **password pas2** и нажмите клавишу Enter, чтобы задать пароль для доступа к маршрутизатору с виртуальных терминалов.
17. Когда в командной строке появится приглашение R0(config-line)#, введите команду **login** и нажмите клавишу Enter, чтобы разрешить использование введенного выше пароля для аутентификации пользователя.
18. Когда в командной строке появится приглашение R0(config-line)#, введите команду **exit** и нажмите клавишу Enter, чтобы вернуться в режим конфигурирования устройства.
19. Когда в командной строке появится приглашение R0(config)#, введите команду **enable secret pas3** и нажмите клавишу Enter, чтобы задать пароль для доступа к привилегированному режиму.
20. Когда в командной строке появится приглашение R0(config)#, введите команду **banner motd #Unauthorized access prohibited!#** и нажмите клавишу Enter, чтобы создать предупреждение о том, что неавторизованный доступ к устройству запрещен.
21. Когда в командной строке появится приглашение R0(config)#, введите команду **end** и нажмите клавишу Enter, чтобы выйти из режима конфигурирования.
22. Когда в командной строке появится приглашение R0#, введите команду **copy running-config startup-config** и нажмите клавишу Enter, чтобы сохранить настройку параметров.
23. Когда устройство выдаст запрос на ввод имени файла для сохранения конфигурации «Destination filename [startup-config]?», нажмите клавишу Enter
24. Когда в командной строке появится приглашение R0#, введите команду **disable** и нажмите клавишу Enter, чтобы выйти из привилегированного режима.
25. Когда в командной строке появится приглашение R0>, введите команду **exit** и нажмите клавишу Enter, чтобы выйти из пользовательского режима и разорвать соединение.
26. В ответ на запрос «Press RETURN to get started!» нажмите клавишу Enter.
27. В ответ на запрос «Password:» введите пароль **pas1** и нажмите клавишу Enter.
28. Когда в командной строке появится приглашение R0>, введите команду **en** и нажмите клавишу Enter, для того чтобы включить привилегированный режим настройки маршрутизатора.
29. В ответ на запрос «Password:» введите пароль **pas3** и нажмите клавишу Enter.
30. Когда в командной строке появится приглашение R0#, введите команду show running-config и нажмите клавишу Enter, чтобы проверить конфигурацию параметров. В ответ на запрос «--More--» нажимайте пробел до тех пор, пока не появится приглашение на ввод следующей команды.
31. Когда в командной строке появится приглашение R0#, введите команду **disable** и нажмите клавишу Enter, чтобы выйти из привилегированного режима.
32. Когда в командной строке появится приглашение R0>, введите команду **exit** и нажмите клавишу Enter, чтобы выйти из пользовательского режима и разорвать соединение.
33. Закройте окно Router0.
34. Завершите работу с программой Cisco Packet Tracer.

5.4. Команды IOS для настройки интерфейсов

Для того чтобы настроить параметры какого-либо интерфейса сетевого устройства, нужно войти в режим конфигурирования интерфейса с помощью команды interface (сокращенно — **int**), которая имеет следующий формат:

```
interface type slot/port
```

где *type* — тип интерфейса, *slot* — номер слота, *port* — номер порта в слоте.

В Cisco IOS приняты следующие обозначения типов интерфейсов:

- async — асинхронный интерфейс для связи с модемом;
- atm — интерфейс, используемый для соединения с коммутатором сети ATM;
- bri — интерфейс ISDN BRI;
- fastethernet — интерфейс Fast Ethernet;
- fddi — интерфейс FDDI;
- gigabitethernet — интерфейс Gigabit Ethernet;
- loopback — локальный интерфейс петли обратной связи;
- null — нулевой интерфейс;
- serial — последовательный интерфейс для соединения с устройствами CSU/DSU.

Интерфейсы типов null и loopback являются программными, все остальные интерфейсы — аппаратные.

Нулевой интерфейс используется для фильтрации трафика: пакеты, направленные на этот интерфейс, просто уничтожаются.

Петлевой интерфейс используется в качестве виртуального интерфейса, на который можно направлять пакеты. В отличие от аппаратных интерфейсов петлевой интерфейс включен постоянно.

Петлевому интерфейсу может быть присвоен любой доступный IP-адрес. Например, чтобы присвоить петлевому интерфейсу с номером 0 адрес 192.168.1.1 и маску 255.255.255.252, нужно подать последовательность команд:

```
interface loopback 0
ip address 192.168.1.1 255.255.255.252
```

Некоторые протоколы маршрутизации, например, OSPF и BGP, могут использовать адрес петлевого интерфейса в качестве идентификатора маршрутизатора.

При подаче команды можно сокращать обозначение типа интерфейса до двух символов, а в некоторых случаях — до одного символа. Пробел между обозначением типа интерфейса и номером слота не является обязательным. Например, вместо interface serial 2/0 можно писать сокращенно int s2/0.

По умолчанию все интерфейсы маршрутизатора выключены (находятся в неактивном состоянии). Для того чтобы перевести интерфейс в активное состояние, нужно подать команду **no shutdown** (сокращенно — **no shut**). Соответственно, отключить интерфейс при необходимости можно, используя команду **shutdown** (сокращенно — **shut**).

Иногда, например, после сбоя, возникает необходимость перезапустить интерфейс. В этом случае интерфейс нужно выключить, а затем — снова включить путем подачи последовательности команд:

```
shutdown
no shutdown
```

Для того чтобы включить на последовательном интерфейсе режим инкапсуляции пакетов, нужно использовать команду **encapsulation** (сокращенно — **en**), которая имеет следующий формат:

encapsulation *encapsulation-type*

где *encapsulation-type* — символьное обозначение используемого метода инкапсуляции.

В Cisco IOS приняты следующие обозначения методов инкапсуляции:

- frame-relay — инкапсуляция Frame Relay,
- hdlc — инкапсуляция HDLC,
- lapb — инкапсуляция LAPB,
- ppp — инкапсуляция PPP,
- slip — инкапсуляция SLIP,
- smds — инкапсуляция SMDS.

При подаче команды обозначение метода инкапсуляции можно сократить до двух символов. Например, вместо encapsulation frame-relay можно писать сокращенно — **en fr**.

Один интерфейс может поддерживать несколько виртуальных каналов, каждый из которых может рассматриваться в качестве отдельного интерфейса, называемого **подинтерфейсом** или **субинтерфейсом**. Польза от применения концепции подинтерфейсов заключается в возможности назначать каждому подинтерфейсу различные характеристики сетевого уровня.

На одном физическом интерфейсе можно задать неограниченное количество подинтерфейсов. Для задания подинтерфейса используется команда interface следующего формата:

interface *type slot/port.number*

где *type* — тип интерфейса, *slot* — номер слота, *port* — номер порта, number — номер подинтерфейса.

Существуют два типа подинтерфейсов: двухточечные и многоточечные. Двухточечные подинтерфейсы применяются тогда, когда два маршрутизатора соединяются между собой одним виртуальным каналом, многоточечные подинтерфейсы используются, если маршрутизатор является центральным узлом виртуальных каналов с топологией «звезда».

Задать для интерфейса или подинтерфейса IP-адрес и маску подсети можно с помощью команды **ip address** (сокращенно — **ip ad**), которая имеет следующий формат:

ip address *ip-address mask*

где *ip-address* — IP-адрес интерфейса или подинтерфейса, *mask* — маска подсети.

Для того чтобы выйти из режима конфигурирования интерфейса, нужно подать команду exit.

После завершения процесса конфигурирования можно проверить правильность настройки устройства с помощью команды **show interfaces** (сокращенно — **sh int**), которая позволяет просмотреть статистику по всем сконфигурированным интерфейсам. Эта команда имеет следующий формат:

```
show interfaces [type]
```

где *type* — символьное обозначение типа интерфейса.

Параметр type в команде show interfaces является необязательным. Если этот параметр задан, то выводится информация по интерфейсам указанного типа, а если опущен — по всем сконфигурированным интерфейсам.

5.5. Команды IOS для настройки параметров протокола RIP

Настройку динамической маршрутизации надлежит производить в режиме конфигурирования маршрутизатора. Для перехода в режим конфигурирования маршрутизатора используется команда **router** (сокращенно — **ro**), которая в обобщенном виде имеет следующий формат:

```
router protocol-type
```

где *protocol-type* — символьное обозначение типа протокола.

В данном разделе мы рассмотрим команды, предназначенные для настройки параметров протокола RIP. Переход в режим конфигурирования маршрутизатора в этом случае выполняется с помощью команды **router rip** (сокращенно — **ro rip**).

Для того, чтобы точно указать, какую версию протокола RIP должен использовать маршрутизатор, нужно подать команду **version** (сокращенно — **ver**), которая имеет следующий формат:

```
version {1|2}
```

Команда **version 1** практически не применяется, так как первая версия RIP (RIPv1) используется по умолчанию. Команда **version 2** запускает вторую версию RIP (RIPv2), в которой поддерживается передача информации о масках сетей.

Если на маршрутизаторе применяется протокол RIP, то для настройки маршрутизации достаточно перечислить адреса соседних сетей (сетей, к которым непосредственно подключен маршрутизатор) с помощью команды **network** (сокращенно — **net**), которая имеет следующий формат:

```
network ip-address
```

где *ip-address* — адрес сети.

Для того, чтобы запретить маршрутизацию с помощью протокола RIP для определенной соседней сети, используется команда no network, которая имеет следующий формат:

no network *ip-address*

где *ip-address* — адрес сети.

Если требуется перенастроить маршрутизатор на использование какого-то другого протокола маршрутизации, то работу протокола RIP нужно остановить путем подачи команды **no router rip**.

Для того чтобы выйти из режима конфигурирования маршрутизатор, нужно подать команду **exit**.

После завершения процесса конфигурирования можно проверить правильность настройки параметров протокола RIP с помощью команд **show ip rip database** (сокращенно — **sh ip rip dat**) и **show ip route** (сокращенно — **sh ip ro**).

Команда show ip route, которая отображает на экран текущее состояние таблицы маршрутизации, имеет следующий формат:

show ip route [*protocol*]

где *protocol* — символьное обозначение типа протокола.

Если тип протокола в команде show ip route не указан, то отображаются все записи таблицы маршрутизации. Для того чтобы отображались только записи, имеющие отношение к протоколу RIP, нужно подать команду **show ip route rip** (сокращенно — **sh ip ro rip**).

5.6. Особенности реализации утилит ping и traceroute

Реализация утилит ping и traceroute, относящихся к стандарному набору утилит стека TCP/IP, в Cisco IOS имеет ряд отличий от реализации в MS Windows.
В Cisco IOS команда **ping** имеет следующий формат:

ping {*host-name* | *system-address*}

где *host-name* — имя узла назначения, *system-address* — IP-адрес узла назначения (может быть указан в формате IPv4 или IPv6).

В отличие от реализации в MS Windows, реализация утилиты ping в Cisco IOS предпринимает не четыре, а пять попыток связаться с адресатом, а результаты своей работы выдает в закодированном виде.

Коды ответов команды ping:

- ! — получен ответ,
- . — ответ не был получен,
- & — истекло время жизни пакета;
- U — получено сообщение о недостижимости узла,
- N — получено сообщение о недостижимости сети,
- M — получено сообщение о невозможности фрагментации.

Утилита трассировки маршрута в Cisco IOS, в отличие от Windows, носит название **traceroute** (сокращенно — **tr**). Для запуска этой утилиты используется команда следующего формата:

```
traceroute destination
```

где *destination* — имя или адрес узла назначения.

5.7. Настройка сетевого оборудования с внешнего терминала

В процессе создания моделей сложных компьютерных сетей настройку сетевого оборудования (маршрутизаторов и управляемых коммутаторов) нужно проводить в консольном режиме с использованием команд Cisco IOS.

В программе Cisco Packet Tracer реализовано два способа настройки сетевого оборудования:

- в упрощенном режиме — с вкладки CLI, расположенной в окне модели устройства;
- в режиме полной имитации — с внешнего терминала (консоли).

5.7.1. Настройка маршрутизатора с вкладки CLI и с консоли

На примере модели сети, показанной на рисунке 5.1, в этом упражнении мы поочередно рассмотрим оба способа настройки: вначале с вкладки CLI, а затем — с консоли.

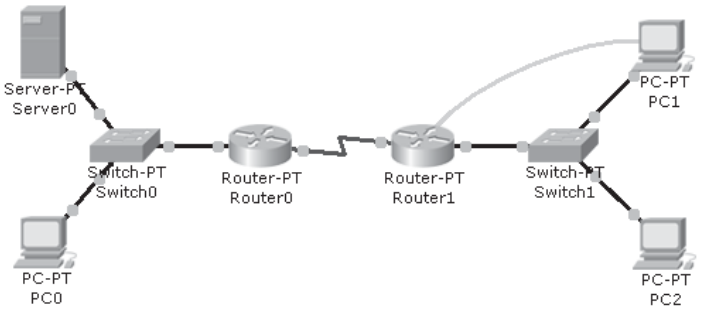

Рис. 5.1. Модель сети для демонстрации двух способов настройки оборудования

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. В группе Routers выберите модель Router-PT и поместите в рабочее пространство маршрутизаторы Router0 и Router1.

2.2. В группе Switches выберите модель Switch-PT и поместите в рабочее пространство коммутаторы Switch0 и Switch1.
2.3. Поместите в рабочее пространство компьютеры PC0, PC1 и PC2.
2.4. Поместите в рабочее пространство сервер Server0.

3. Соедините между собой устройства, размещенные в рабочем пространстве:
3.1. Подключите прямым кабелем компьютер PC0 к порту FastEthernet1/1 коммутатора Switch0.
3.2. Подключите прямым кабелем компьютер PC1 к порту FastEthernet0/1 коммутатора Switch1.
3.3. Подключите прямым кабелем компьютер PC2 к порту FastEthernet1/1 коммутатора Switch1.
3.4. Подключите прямым кабелем сервер Server0 к порту FastEthernet0/1 коммутатора Switch0.
3.5. Подключите прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
3.6. Подключите прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet0/0 маршрутизатора Router1.
3.7. В группе Connections выберите пиктограмму консольного кабеля Console. Подсоедините один конец консольного кабеля к порту RS 232 компьютера PC1, а другой конец — к порту Console маршрутизатора Router1.
3.8. В группе Connections выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial2/0 маршрутизатора Router0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router1.

4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0**, адрес шлюза **192.168.1.254** и адрес сервера DNS **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**, адрес шлюза **192.168.2.254** и адрес сервера DNS **192.168.1.1**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.2.2**, маску **255.255.255.0**, адрес шлюза **192.168.2.254** и адрес сервера DNS **192.168.1.1**.
7. Настройте сервер Server0:
7.1. Выберите в рабочем пространстве сервер Server0.
7.2. В окне Server0 выберите вкладку Config.
7.3. В области настройки глобальных параметров Global Settings задайте статический режим настройки шлюза и адрес шлюза **192.168.1.254**.
7.4. В окне Server0 выберите вкладку Services.
7.5. На вкладке Services нажмите кнопку HTTP.
7.6. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On** (рис. 5.2).
7.7. На вкладке Services нажмите кнопку DHCP.
7.8. В области настройки параметров протокола DHCP установите переключатель Service в положение **Off** (рис. 5.3), для того чтобы отключить динамическое распределение IP-адресов.

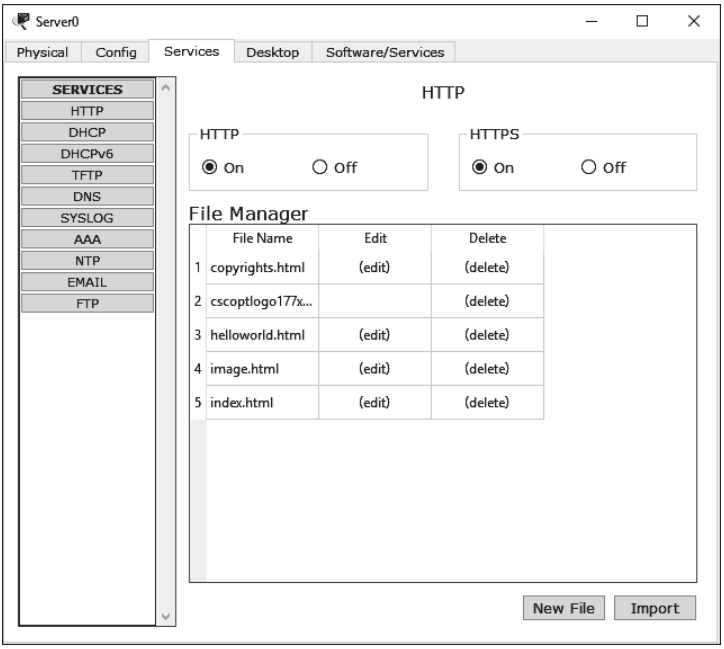

Рис. 5.2. Включение поддержки протокола HTTP на сервере Server0

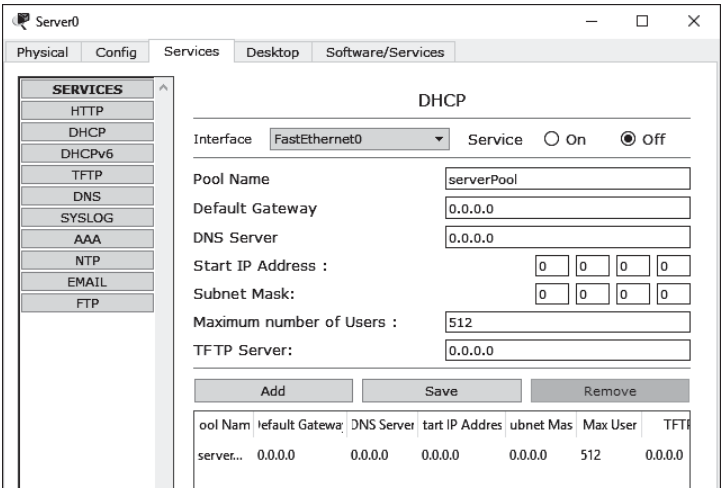

Рис. 5.3. Отключение поддержки протокола DHCP на сервере Server0

7.9. На вкладке Services нажмите кнопку DNS.
7.10. В области настройки параметров DNS установите переключатель DNS Service в положение **On**, для того чтобы включить поддержку сервиса DNS.
7.11. В поле Name задайте для сервера имя serv0.ru, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.1.1**, после чего нажмите кнопку Add. В результате в таблице DNS должна появиться одна запись (рис. 5.4).
7.12. На вкладке Config нажмите кнопку FastEthernet.
7.13. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.1.1** и маску **255.255.255.0**.
7.14. Закройте окно Server0.

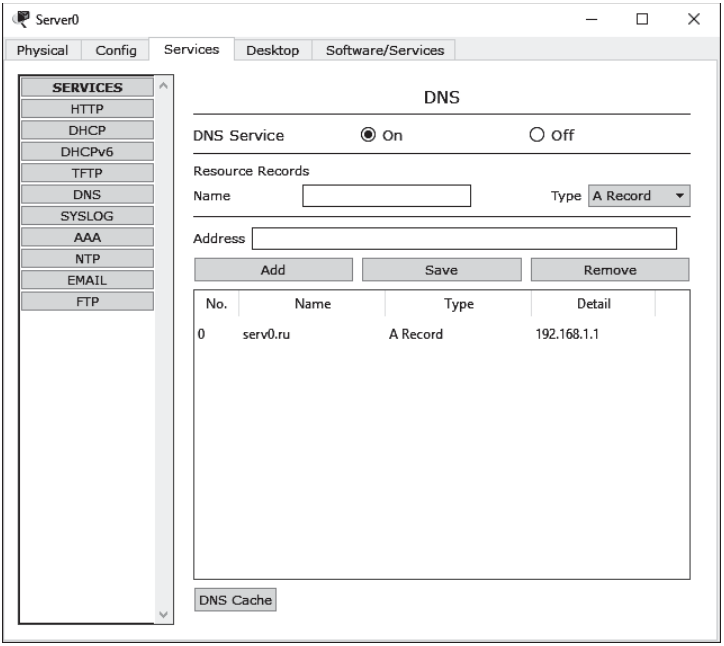

Рис. 5.4. Включение сервиса DNS на сервере Server0

8. Настройте маршрутизатор Router0 с вкладки CLI:
   8.1. Выберите в рабочем пространстве маршрутизатор Router0.
   8.2. В окне Router0 выберите вкладку CLI, чтобы использовать интерфейс командной строки CLI для настройки параметров маршрутизатора.
   8.3. Если на экране выведен запрос «Continue with configuration dialog? [yes/no]:», то с клавиатуры введите символ **n** и нажмите клавишу Enter.
   8.4. В ответ на запрос «Press RETURN to get started!» нажмите клавишу Enter.
   8.5. Когда в командной строке появится приглашение Router>, введите команду **en**.

8.6. Когда в командной строке появится приглашение Router#, введите команду **conf t**.
8.7. Когда в командной строке появится приглашение Router(config)#, введите команду **hostname Router0**, чтобы присвоить маршрутизатору имя Router0.
8.8. Когда в командной строке появится приглашение Router0(config)#, введите команду **int fa0/0**, чтобы начать настройку параметров интерфейса FastEthernet0/0.
8.9. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **ip address 192.168.1.254 255.255.255.0**, для того чтобы задать IP-адрес и маску для интерфейса FastEthernet0/0.
8.10. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **no shutdown**, для того чтобы после завершения процесса настройки маршрутизатора порт интерфейса FastEthernet0/0 оставался в активном состоянии. В ответ на эту команду вы должны получить подтверждение «Interface FastEthernet0/0, changed state to up», которое сообщает, что порт был переведен в активное состояние (поднят), и сообщение «Line protocol on Interface FastEthernet0/0, changed state to up», которое гласит, что для обслуживания порта был активирован соответствующий протокол.
8.11. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **int se2/0**, чтобы начать настройку параметров интерфейса Serial2/0.
8.12. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **ip ad 192.168.3.1 255.255.255.0**, для того чтобы задать IP-адрес и маску для интерфейса Serial2/0.
8.13. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **clock rate 56000**, для того чтобы задать скорость передачи данных по последовательному каналу.
8.14. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **no shut**, для того чтобы порт интерфейса Serial2/0 оставался в активном состоянии.
8.15. Когда в командной строке появится приглашение Router0(config-if)#, введите команду **exit**, чтобы завершить процесс настройки интерфейсов.
8.16. Когда в командной строке появится приглашение Router0(config)#, введите команду **router rip**, чтобы начать настройку параметров протокола маршрутизации RIP.
8.17. Когда в командной строке появится приглашение Router0(config-router)#, введите команду **network 192.168.1.0**, для того чтобы указать, что сеть 192.168.1.0 для маршрутизатора является соседней.
8.18. Когда в командной строке появится приглашение Router0(config-router)#, введите команду **ne 192.168.3.0**, для того чтобы указать, что сеть 192.168.3.0 для маршрутизатора является соседней.
8.19. Когда в командной строке появится приглашение Router0(config-router)#, введите команду **end**, чтобы завершить процесс настройки параметров и выйти из режима конфигурирования.
8.20. Когда в командной строке появится приглашение Router0#, введите команду **copy run sta** и нажмите клавишу Enter, чтобы сохранить настройку параметров в энергонезависимой памяти.
8.21. Когда в командной строке появится приглашение Router0#, введите команду **exit**, для того чтобы завершить работу в привилегированном режиме.
8.22. На этом процесс настройки маршрутизатора можно считать завершенным. Закройте окно маршрутизатора Router0.

9. Настройте маршрутизатор Router1 с внешнего терминала:
   9.1. Для того, чтобы приступить к использованию второго способа настройки оборудования, выберите в рабочем пространстве персональный компьютер PC1.
   9.2. В окне PC1 выберите вкладку Desktop и нажмите кнопку Terminal.
   9.3. В окне Terminal configuration нажмите кнопку OK, чтобы принять заданные по умолчанию параметры терминала. На экране должно открыться окно Terminal.
   9.4. Если в окне Terminal выведен запрос «Continue with configuration dialog? [yes/no]:», то с клавиатуры введите n и нажмите клавишу Enter.
   9.5. В ответ на запрос «Press RETURN to get started!» нажмите клавишу Enter.
   9.6. Введите в окне терминала последовательность команд:

```
Router>en
Router#conf t
Router#ho Router1
Router1(config)#int fa0/0
Router1(config-if)#ip ad 192.168.2.254 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#int se2/0
Router1(config-if)#ip ad 192.168.3.2 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#ro rip
Router1(config-router)#net 192.168.2.0
Router1(config-router)#net 192.168.3.0
Router1(config-router)#end
Router1#copy run sta
Router1#exit
```

   9.7. На этом процесс настройки маршрутизатора с терминала можно считать завершенным. Закройте окно Terminal, а затем закройте окно PC1.
10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: во всех таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0.
11. Переключите Cisco Packet Tracer в режим Simulation.
12. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC1.
13. Переключите Cisco Packet Tracer в режим Realtime.
14. Выберите в рабочем пространстве компьютер PC0.
15. Используя утилиты стека TCP/IP, проверьте связь между компьютером PC0 и сервером:
   15.1. В окне PC0 выберите вкладку Desktop.
   15.2. На вкладке Desktop нажмите кнопку Command Prompt, для того чтобы войти в режим, имитирующий работу командного процессора операционной системы персонального компьютера.
   15.3. Когда в командной строке появится приглашение PC>, введите команду **ping 192.168.1.1**, для того чтобы проверить наличие связи с сервером Server0. Просмотрите результаты выполнения этой команды.
   15.4. Когда в командной строке появится приглашение PC>, введите команду **tracert serv0.ru**, дождитесь завершения выполнения команды и просмотрите результат ее выполнения.
   15.5. Закройте окно Command Prompt.

16. Проверьте наличие доступа с компьютера PC0 к интернет-странице на сервере:
    16.1. Нажмите кнопку Web Browser на вкладке Desktop.
    16.2. В окне браузера наберите в поле URL адрес **serv0.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера.
    16.3. Закройте окно Web Browser.
17. Закройте окно PC0.
18. Выберите в рабочем пространстве компьютер PC2.
19. Используя утилиты стека TCP/IP, проверьте связь между компьютером PC2 и сервером.
20. Проверьте наличие доступа с компьютера PC2 к интернет-странице на сервере.
21. Закройте окно PC2.
22. Проверьте связь между маршрутизатором Router0 и компьютерами:
    22.1. Выберите в рабочем пространстве маршрутизатор Router0.
    22.2. В окне Router0 выберите вкладку CLI,.
    22.3. Когда в командной строке появится приглашение Router0>, введите команду **en**.
    22.4. Когда в командной строке появится приглашение Router0#, введите команду **ping 192.168.1.1**, чтобы проверить связь с компьютером PC0.
    22.5. Когда в командной строке появится приглашение Router0#, введите команду **ping 192.168.2.2**, чтобы проверить связь с компьютером PC2.
    22.6. Когда в командной строке появится приглашение Router0#, введите команду **traceroute 192.168.2.2**, чтобы определить маршрут к компьютеру PC2.
    22.7. Когда в командной строке появится приглашение Router0#, введите команду **exit**.
    22.8. Когда в командной строке появится приглашение Router0>, введите команду **exit**.
    22.9. Закройте окно маршрутизатора Router0.
23. Сохраните модель сети в файле с именем **net_5_7_1**.
24. Завершите работу с программой Cisco Packet Tracer.

5.8. Настройка статических маршрутов

Записи о статических маршрутах вносятся в таблицу маршрутизации в режиме глобального конфигурирования при помощи команды ip route (сокращенно — **ip ro**), которая имеет следующий формат:

ip route *prefix mask* {*ip-address*|*interface-type interface-number*}

где *prefix* — адрес сети назначения, *mask* — маска сети назначения, *ip-address* — IP-адрес шлюза, *interface-type* — тип интерфейса, *interface-number* — номер интерфейса.

Параметр ip-address задает IP-адрес шлюза, через который будет осуществляться маршрутизация к указанной сети. Например, команда

```
ip route 10.9.8.0 255.255.255.0 172.20.30.1
```

указывает маршрутизатору, что все пакеты, предназначенные для сети 10.9.8.0, должны передаваться через шлюз 172.20.30.1.

Команда ip route позволяет задать **маршрут по умолчанию**, который будет использоваться маршрутизатором в том случае, когда ему неизвестен конкретный шлюз до системы назначения. В этом случае в качестве адреса сети назначения задается значение 0.0.0.0 и в качестве маски сети назначения также задается значение 0.0.0.0.

Например, команда

```
ip route 0.0.0.0 0.0.0.0 4.3.2.1
```

указывает маршрутизатору, что все пакеты, для которых нет известного маршрута, должны передаваться шлюзу 4.3.2.1.

Если маршрутизатор сам выполняет роль шлюза, то в команде ip route вместо адреса шлюза по умолчанию можно указать тип и номер интерфейса, на который должен по умолчанию направляться трафик.

Например, команда

```
ip route 0.0.0.0 0.0.0.0 serial 2/0
```

указывает маршрутизатору, что трафик по умолчанию должен передаваться через интерфейс serial 2/0.

После завершения процесса конфигурирования можно проверить правильность настройки статических маршрутов с помощью команды **show ip route static** (сокращенно — **sh ip ro st**).

5.9. Команды IOS для настройки сервиса DHCP

Для включения на маршрутизаторе сервиса DHCP используется команда **service dhcp**, а отключить его можно с помощью команды **no service dhcp**.

По умолчанию сервис DHCP на маршрутизаторах Cisco включен.

После включения сервиса DHCP адреса компьютерам-клиентам будут выдаваться из так называемого пула адресов.

Пул адресов можно создать с помощью команды **ip dhcp pool**, которая имеет следующий формат:

```
ip dhcp pool name
```

где *name* — символическое имя пула.

После создания пула нужно присвоить сети номер и маску, используя команду **network**:

```
network network-number [mask]
```

где *network-number* — номер сети, *mask* — маска сети (необязательный параметр).

Для того, чтобы исключить из пула определенные адреса (например, адрес шлюза, используемого по умолчанию), применяется команда **ip dhcp excluded-address** (сокращенно — **ip dhcp ex**), которая имеет следующий формат:

```
ip dhcp excluded-address low-address [high-address]
```

где *low-address* — нижняя граница исключаемой области адресов, *high-address* — верхняя граница области адресов (необязательный параметр).

Кроме своей основной функции — раздачи клиентам IP-адресов, встроенный в маршрутизатор DHCP-сервер обеспечивает также ряд дополнительных возможностей: позволяет задавать адрес шлюза по умолчанию, адрес сервера DNS и т.д.

Команда **domain-name**, которая задает имя домена для клиента DHCP, имеет следующий формат:

```
domain-name domain
```

где *domain* — имя домена.

Команда **dns-server** (сокращенно — **dn**), которая позволяет присвоить IP-адрес серверу DNS, имеет следующий формат:

```
dns-server address
```

где *address* — IP-адрес сервера DNS.

Адрес шлюза, используемого по умолчанию, можно задать с помощью команды **default-router** (сокращенно — **de**), которая имеет следующий формат:

```
default-router address
```

где *address* — IP-адрес шлюза, используемого по умолчанию.

5.9.1. Настройка статических маршрутов и сервиса DHCP

Рассмотрим настройку статических маршрутов и сервиса DHCP на примере сети, изображенной на рисунке 5.5.

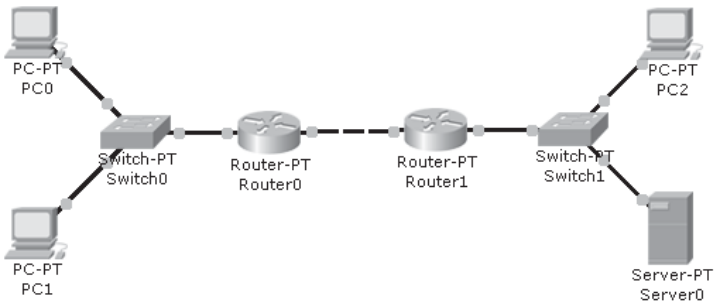

Рис. 5.5. Модель сети для демонстрации настройки сервиса DHCP

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве два коммутаторы Switch0 и Switch1 типа Switch-PT, маршрутизаторы Router0 и Router1 типа Router-PT, компьютеры PC0–PC2 и сервер Server0 так, как показано на рисунке 5.5.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   - 3.1. Присоедините прямым кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/1 коммутатора Switch0.
   - 3.2. Присоедините прямым кабелем порт FastEthernet компьютера PC1 к порту FastEthernet1/1 коммутатора Switch0.
   - 3.3. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
   - 3.4. Присоедините прямым кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/1 коммутатора Switch1.
   - 3.5. Присоедините прямым кабелем порт FastEthernet сервера Server0 к порту FastEthernet1/1 коммутатора Switch1.
   - 3.6. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet0/0 маршрутизатора Router1.
   - 3.7. Присоедините перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet1/0 маршрутизатора Router1.
4. Настройте компьютер PC0:
   - 4.1. Выберите в рабочем пространстве персональный компьютер PC0.
   - 4.2. В окне PC0 выберите вкладку Config.
   - 4.3. Задайте режим настройки шлюза с помощью DHCP, установив в соответствующее положение переключатель Gateway/DNS (рис. 5.6).
   - 4.4. Закройте окно PC0.

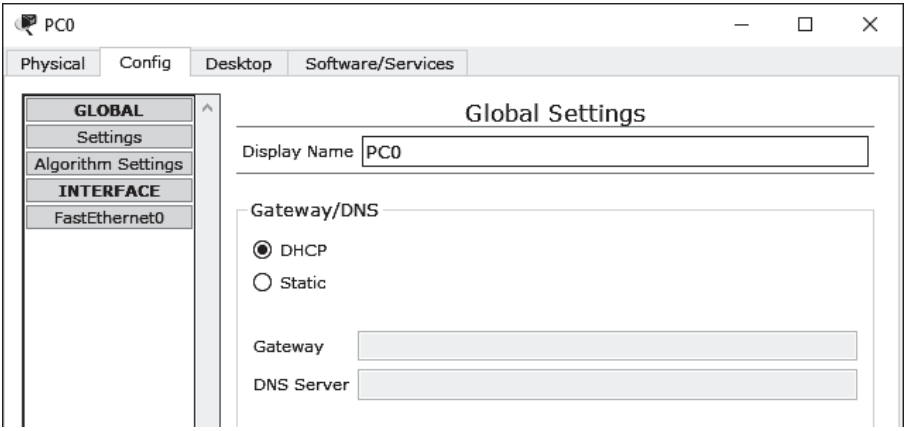

Рис. 5.6. Переключение компьютера PC0 в режим клиента DHCP

5. Аналогичным образом задайте режим настройки шлюза с помощью DHCP на компьютерах PC1 и PC2.

6. Настройте сервер Server0:
   6.1. Выберите в рабочем пространстве сервер Server0.
   6.2. В окне Server0 выберите вкладку Config.
   6.3. В области настройки глобальных параметров Global Settings установите статический режим настройки шлюза, задайте адрес шлюза **192.168.2.1** и адрес сервера DNS **192.168.2.2**.
   6.4. На вкладке Config нажмите кнопку FastEthernet.
   6.5. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.2.2** и маску **255.255.255.0**.
   6.6. В окне Server0 выберите вкладку Services.
   6.7. На вкладке Services нажмите кнопку HTTP.
   6.8. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
   6.9. На вкладке Services нажмите кнопку DHCP.
   6.10. В области настройки параметров протокола DHCP установите переключатель Service в положение **Off**, для того чтобы отключить динамическое распределение IP-адресов сервером.
   6.11. На вкладке Services нажмите кнопку DNS.
   6.12. В области настройки параметров DNS установите переключатель DNS Service в положение **On**, для того чтобы включить поддержку сервиса DNS.
   6.13. В поле Name задайте для сервера имя **serv0.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.2.2**, после чего нажмите кнопку Add. В результате в таблице DNS должна появиться одна запись.
   6.14. Закройте окно Server0.
7. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router#ho Router0
Router0(config)#ip dhcp excluded-address 192.168.1.1
Router0(config)#ip dhcp pool net1
Router0(config-pool)#net 192.168.1.0 255.255.255.0
Router0(config-pool)#default-router 192.168.1.1
Router0(config-pool)#dns-server 192.168.2.2
Router0(config)#int fa0/0
Router0(config-if)#ip ad 192.168.1.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#int fa1/0
Router0(config-if)#ip ad 192.168.3.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#ro rip
Router0(config-router)#net 192.168.1.0
Router0(config-router)#net 192.168.3.0
Router0(config-router)#end
Router0#copy run sta
Router0#exit
```

8. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router#ho Router1
Router1(config)#ip dhcp ex 192.168.2.1 192.168.2.2
Router1(config)#ip dhcp pool net2
Router1(config-pool)#net 192.168.2.0 255.255.255.0
Router1(config-pool)#de 192.168.2.1
Router1(config-pool)#dn 192.168.2.2
Router1(config)#int fa0/0
Router1(config-if)#ip ad 192.168.2.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#int fa1/0
Router1(config-if)#ip ad 192.168.3.2 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#ro rip
Router1(config-router)#net 192.168.2.0
Router1(config-router)#net 192.168.3.0
Router1(config-router)#end
Router1#copy run sta
Router1#exit
```

9. Подождите до завершения процесса самонастройки коммутаторов (на всех портах должны появиться зеленые сигналы).
10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0.
11. Проверьте исправность сетевых соединений:
    11.1. Передайте простой пакет с компьютера PC0 на компьютер PC1.
    11.2. Передайте простой пакет с компьютера PC2 на сервер Server0.
    11.3. Передайте простой пакет с компьютера PC0 на сервер Server0. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
12. Используя утилиты стека TCP/IP, проверьте связь между компьютером PC0 и сервером.
13. Проверьте наличие доступа с компьютера PC0 к интернет-странице на сервере.
14. Сохраните модель сети в файле с именем **net_5_9_1**.
15. Завершите работу с программой Cisco Packet Tracer.

5.10. Сброс настроек оборудования в исходное состояние

Если в процессе настройки оборудования были допущены ошибки, то в некоторых случаях удобнее и быстрее выполнить настройку заново, а не искать и исправлять ошибки по одной.

Если ошибочные настройки еще не были сохранены в энергонезависимой памяти, то можно просто перезагрузить устройство. Для перезагрузки коммутатора или маршрутизатора нужно в привилегированном режиме подать команду **reload** (сокра-

щенно — **rel**). В ответ на запрос подтверждения операции «Proceed with reload? [confirm]» нужно просто нажать клавишу Enter.

Сбросить не сохраненные в энергонезависимой памяти настройки можно и другим способом — путем имитации перезагрузки устройства после отключения и обратного включения питания. На моделях корпусов маршрутизаторов в Cisco Packet Tracer обычно присутствуют выключатели питания: выключив, а затем — снова включив питание маршрутизатора, можно вызвать перезагрузку его операционной системы.

В Cisco Packet Tracer имеется также возможность выполнения одновременной перезагрузки всех сетевых устройств путем имитации общего сброса по питанию: для этой цели предназначена кнопка Power Cycle Down, размещенная под рабочим пространством. Настройки персональных компьютеров и серверов при отключении питания не сбрасываются.

Если ошибочно заданные значения параметров уже были сохранены в файле стартовой конфигурации, то перед перезагрузкой устройства необходимо стереть этот файл путем подачи в привилегированном режиме команды **erase startup-config** (сокращенно — **er sta**). В ответ на запрос подтверждения операции «Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]» нужно нажать клавишу Enter.

В коммутаторах для полного сброса настроек в исходное (заводское) состояние необходимо проделать перед перезагрузкой еще одну операцию — стереть из энергонезависимой памяти файл vlan.dat, в котором сохраняются настройки виртуальных сетей. Для стирания указанного файла нужно подать в привилегированном режиме команду **delete vlan.dat** (сокращенно — **del vlan.dat**).Таким образом, для коммутатора последовательность подачи команд будет следующей:

```
erase startup-config
delete vlan.dat
reload
```

5.11. Задание для самостоятельной работы

В целях тренировки попробуйте самостоятельно создать и наладить модель сети, изображенной на рисунке 5.7. Сеть должна состоять из пяти компьютеров, сервера, трех коммутаторов типа Switch-PT и трех маршрутизаторов типа Router-PT. Маршрутизаторы должны быть соединены последовательными каналами связи.

Для настройки параметров маршрутизаторов используйте вкладку CLI, расположенную в окне модели маршрутизатора.

В процессе настройки оборудования протоколируйте свои действия — периодически делайте скриншоты и сохраняйте их в файлах на диске. Подобный протокол может понадобиться для поиска ошибок, которые могут быть допущены в процессе наладки оборудования.

Проведите проверку работоспособности построенной вами модели сети. Когда модель будет отлажена, сохраните ее в файле с именем **net_5_11**.

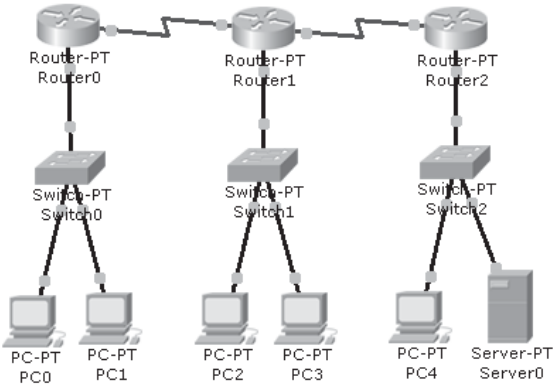

Рис. 5.7. Задание для самостоятельной работы

6. БЕСКЛАССОВАЯ АДРЕСАЦИЯ

Традиционная схема деления IP-адреса на номер сети и номер узла разрабатывалась в то время, когда понятия «персональный компьютер» еще не существовало, и не была рассчитана на то, что в мире появятся миллиарды компьютеров. В результате сети, построенные по стандарту IPv4, стали сталкиваться с различными проблемами, так как ширина пространства адресов оказалось недостаточной для присвоения уникального IP-адреса каждому компьютеру, подключенному к всемирной сети.

6.1. Маска подсети

В течение некоторого периода времени проблему «нехватки адресов» удавалось решать за счет различных приемов и трюков, делающих систему адресации более гибкой.

Одним из способов повышения гибкости системы адресации является использование масок.

Маска — это число, которое используется в паре с IP-адресом. Двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети (последовательность единиц в маске должна быть непрерывной, но количество единиц может быть не кратным 8).

Например, если адрес 189.76.54.123 ассоциировать с маской 255.255.255.0, то номером сети будет 189.76.54.0, а не 189.76.0.0, как это определено системой классов.

Для стандартных классов сетей маски имеют следующие значения:

- для класса A — 11111111.00000000.00000000.00000000 (255.0.0.0);
- для класса B — 11111111.11111111.00000000.00000000 (255.255.0.0);
- для класса C — 11111111.11111111.11111111.00000000 (255.255.255.0).

6.2. Использование масок

Если снабжать IP-адреса масками, то можно отказаться от понятий классов адресов, поэтому адресация с использованием масок называется **бесклассовой**.

Маска позволяет разделить сеть определенного класса на части — подсети (subnets). При выполнении такого разделения следует учитывать ограничения, создаваемые наличием особых IP-адресов:

- адреса узлов, состоящие из двоичных единиц, зарезервированы для широковещания;
- адреса узлов, состоящие из двоичных нулей, зарезервированы для всей подсети.

Непрерывная последовательность единиц, с которой начинается маска, называется **префиксом подсети**.

Длину префикса указывают, отделяя косой чертой от IP-адреса. Например, запись «192.168.1.2/28» показывает, что в подсети используется маска 255.255.255.240.

С точки зрения адресации, подсети являются расширением сетевого номера. Использование подсетей никак не отражается на том, как внешний мир видит эту сеть, но в пределах организации подсети рассматриваются как дополнительные структуры.

Маршрутизатор определяет сеть назначения, используя адрес подсети, тем самым ограничивая объем трафика в других сегментах сети.

Адрес подсети включает номера сети, подсети и узла. Для того чтобы создать адрес подсети, сетевой администратор заимствует биты из поля, выделенного для адреса узла, и переопределяет их в качестве поля подсети.

В таблице 6.1 в качестве примера приведены возможные варианты деления класса С на подсети в зависимости от количества заимствованных бит.

Таблица 6.1. Варианты деления сети класса С на подсети

Количество заимствованных бит	Маска подсети	Количество подсетей	Количество узлов
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

6.2.1. Разделение локальной сети на подсети

В этом упражнении от вас требуется разделить локальную сеть, показанную на рисунке 6.1, на две независимые подсети, используя маски.

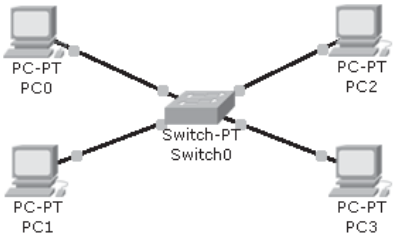

Рис. 6.1. Сеть, которая должна быть разделена на две подсети

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Соберите модель сети, изображенной на рисунке 6.1. Сеть должна состоять из четырех компьютеров и коммутатора типа Switch-PT, соединенных прямыми медными кабелями на основе витой пары.
3. Настройте компьютер PC0: задайте IP-адрес **192.168.1.5** и маску **255.255.255.252**.
4. Настройте компьютер PC1: задайте IP-адрес **192.168.1.6** и маску **255.255.255.252**.
5. Настройте компьютер PC2: задайте IP-адрес **192.168.1.9** и маску **255.255.255.252**.
6. Настройте компьютер PC3: задайте IP-адрес **192.168.1.10** и маску **255.255.255.252**.
7. Переключите Cisco Packet Tracer в режим Simulation.
8. Передайте простой пакет с компьютера PC0 на компьютер PC1.
9. Передайте простой пакет с компьютера PC2 на компьютер PC3.
10. Попытайтесь передать пакет с компьютера PC0 на компьютер PC3. Что произойдет и почему?

11. Сохраните модель сети в файле с именем **net_6_2_1**.
12. Завершите работу с программой Cisco Packet Tracer.

6.2.2. Моделирование взаимодействия подсетей

В предыдущем упражнении локальная сеть была образована вокруг единственного коммутатора. Компьютеры, относящиеся к различным подсетям, в подобной сети не могут общаться между собой. Для того, чтобы обеспечить взаимодействие подсетей друг с другом, в локальную сеть нужно добавить маршрутизатор.

Схема подобной сети показана на рисунке 6.2.

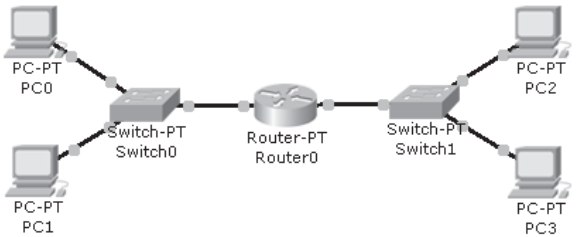

Рис. 6.2. Сеть, объединенная маршрутизатором

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве коммутаторы Switch0 и Switch1 типа Switch-PT, маршрутизатор Router0 типа Router-PT и четыре компьютера PC0–PC3 так, как показано на рисунке 6.2.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Присоедините прямым кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/1 коммутатора Switch0.
   3.2. Присоедините прямым кабелем порт FastEthernet компьютера PC1 к порту FastEthernet1/1 коммутатора Switch0.
   3.3. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.4. Присоедините прямым кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/1 коммутатора Switch1.
   3.5. Присоедините прямым кабелем порт FastEthernet компьютера PC3 к порту FastEthernet1/1 коммутатора Switch1.
   3.6. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet1/0 маршрутизатора Router1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.10**, маску **255.255.255.248** и адрес шлюза **192.168.1.9**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.1.11**, маску **255.255.255.248** и адрес шлюза **192.168.1.9**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.1.18**, маску **255.255.255.248** и адрес шлюза **192.168.1.17**.

7. Настройте компьютер PC3: задайте IP-адрес **192.168.1.19**, маску **255.255.255.248** и адрес шлюза **192.168.1.17**.
8. Настройте маршрутизатор Router0:
   8.1. Выберите в рабочем пространстве маршрутизатор Router0.
   8.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   8.3. Для интерфейса FastEthernet0/0 задайте статус порта **On**, адрес **192.168.1.9** и маску **255.255.255.248**.
   8.4. На вкладке Config нажмите кнопку FastEthernet1/0.
   8.5. Для интерфейса FastEthernet1/0 задайте статус порта **On**, адрес **192.168.1.17** и маску **255.255.255.248**.
   8.6. Закройте окно Router0.
9. Подождите до завершения процесса самонастройки коммутаторов (на всех портах должны появиться зеленые сигналы).
10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу на маршрутизатор, щелкните левой кнопкой мыши, для того чтобы вызвать меню, и выберете в меню пункт Routing Table, чтобы просмотреть таблицу маршрутизации. В таблице должны присутствовать подсети 192.168.1.8 и 192.168.1.16. Какой префикс имеют эти подсети?
11. Переключите Cisco Packet Tracer в режим Simulation.
12. Передайте простой пакет с компьютера PC0 на компьютер PC1.
13. Передайте простой пакет с компьютера PC2 на компьютер PC3.
14. Передайте простой пакет с компьютера PC0 на компьютер PC3.
15. Сохраните модель сети в файле с именем **net_6_2_2**.
16. Завершите работу с программой Cisco Packet Tracer.

6.3. Задание для самостоятельной работы

Измениете приведенную на рисунке 6.3 модель таким образом, чтобы в каждой подсети было по пять компьютеров. Какую маску подсети нужно использовать в этом случае?

7. КОНФИГУРИРОВАНИЕ ВИРТУАЛЬНОЙ СЕТИ

Если строить крупную сеть, используя только коммутаторы, то широковещательные запросы будут существенно ее загружать, снижая полезную пропускную способность каналов связи. Чтобы решить проблему перегруженности сети широковещательными запросами, ее делят на подсети, передачу данных между которыми выполняют с помощью маршрутизаторов.

7.1. Виртуальные локальные сети

Виртуальная локальная сеть (Virtual Local Area Network, сокращенно — **VLAN**) представляет собой совокупность портов одного или более коммутаторов.

Метод виртуальных сетей позволяют логически разбить исходную локальную сеть на несколько независимых сетей. При использовании этого метода администратор сети должен указать на каждом коммутаторе, к какой виртуальной сети относится тот или иной порт. По умолчанию все порты коммутатора относятся к виртуальной сети с номером 1. Максимальное число виртуальных сетей в коммутаторе равно общему числу его портов.

Основной целью создания виртуальных сетей является повышение безопасности работы пользователей: метод виртуальных сетей позволяет полностью изолировать подсети друг от друга и вести для разных подсетей различную политику безопасности.

Помимо обеспечения безопасности создание виртуальных сетей позволяет также решить проблему избыточного широковещательного трафика.

Порт управляемого коммутатора может работать либо в режиме **доступа**, либо в **магистральном** режиме. Соответственно связь, подсоединённая к порту, является либо связью доступа, либо магистральной связью.

В режиме доступа порт принадлежит только одной виртуальной сети. Порт доступа присоединяется к оконечному устройству: компьютеру, серверу или концентратору, а кадры, проходящие через порт доступа, являются обычными кадрами сети Ethernet.

Для обмена информацией о виртуальных сетях коммутаторы используют магистральный (транковый) протокол. Для того, чтобы такой обмен информацией стал возможным, между коммутаторами нужно создать магистральные связи.

Магистральный порт — это порт, используемый для передачи информации о виртуальной сети в другие сетевые устройства, присоединенные к этому порту. Обычные порты не передают информацию о виртуальной сети, но любой порт управляемого коммутатора может быть перенастроен для работы в качестве магистрального порта.

Одна магистральная связь способна поддерживать несколько виртуальных сетей. Виртуальные сети на различных коммутаторах связываются через магистральный протокол. Магистральные порты не принадлежат определённой виртуальной сети и используются для подсоединения к другим коммутаторам, маршрутизаторам или серверам. Если порт находится в магистральном режиме, то он может быть настроен для транспорта всех или только некоторых виртуальных сетей.

Магистрали могут расширить виртуальную сеть по всей локальной сети. Без магистральных связей для каждой из виртуальных сетей потребовалось бы создать отдельную связь доступа, а такой подход дорог и неэффективен.

Для магистральных целей назначают высокоскоростные порты коммутаторов. Для передачи пакетов по магистральному каналу используется либо протокол ISL (Inter-Switch Link) корпорации Cisco, либо стандарт IEEE 802.1Q.

7.2. Конфигурирование статических сетей

Статическая виртуальная сеть — это совокупность портов на коммутаторе, которую администратор сети при конфигурировании интерфейса задает вручную с помощью команд Cisco IOS [14].

Для того, чтобы переключить коммутатор в режим настройки конфигурации виртуальной локальной сети, нужно использовать команду **vlan database** (сокращенно — **vl da**). После выполнения этой команды в командной строке за именем устройства будет следовать индикатор режима конфигурирования vlan, помещенный в круглые скобки.

Для включения виртуальной сети в базу данных применяется команда **vlan** (сокращенно — **vl**), которя имеет следующий формат:

```
vlan vlan-id [name vlan-name]
```

где *vlan-id* — номер виртуальной сети, *vlan-name* — символическое имя сети длиной не более 32 символов.

Параметр name в команде vlan не является обязательным. Если имя виртуальной сети в команде не указано, то оно формируется из номера сети с приставкой VLAN. Например, последовательность команд

```
Switch#vlan database
Switch(vlan)#vlan 33
```

создает на коммутаторе Switch пустую сеть с номером 33 и именем VLAN0033.

Команда **switchport mode** (сокращенно — **sw mo**) используется для установки интерфейса в динамический режим (dynamic), режим доступа (access) или режим магистрали (trunk). Команда имеет следующий формат:

```
switchport mode access|dynamic|trunk
```

Для того, чтобы связать интерфейс с виртуальной сетью, в режиме настройки интерфейса нужно подать команду **switchport access vlan** (сокращенно — **sw ac vl**), которая имеет следующий формат:

```
switchport access vlan number
```

где *number* — номер виртуальной сети, с которой должен быть связан данный интерфейс.

Команда **interface range** (сокращенно — **int ra**) определяет диапазон интерфейсов для последующей конфигурации. Например, порты с третьего по седьмой могут быть помещены в виртуальную сеть 19 с помощью последовательности команд

```
interface range fa0/3 - 7
switchport access vlan 19
```

Для того чтобы переключить интерфейс в магистральный режим, используется команда **switchport mode trunk** (сокращенно — **sw mo tr**).

По умолчанию все магистральные порты принимают и передают трафик со всех виртуальных сетей. Однако если какие-то виртуальные сети не используется на другом конце магистрали, то можно не разрешать передачу трафика этих сетей, чтобы подавить лишние широковещательные запросы. Для сокращения магистрального трафика можно использовать команду **switchport trunk allowed vlan** (сокращенно — **sw tr al vl**), которая имеет следующий формат:

```
switchport trunk allowed vlan vlan-list
```

где *vlan-list* — номер виртуальной сети или диапазон номеров виртуальных сетей, для которых разрешена передача трафика через данный интерфейс.

Например, последовательность команд

```
switchport trunk allowed vlan 3
switchport trunk allowed vlan 8-15
```

разрешает передачу по магистрали трафика виртуальной сети 3 и трафика виртуальных сетей с 8 по 15.

После завершения настройки сети правильность ее выполнения можно проверить с помощью команд **show vlan** (сокращенно — **sh vl**) и **show vlan brief** (сокращенно — **sh vl br**).

Для того чтобы определить, передача трафика каких сетей разрешена на данной магистрали, можно использовать команду **show running-config** (сокращенно — **sh ru**).

7.2.1. Сеть на базе управляемых коммутаторов

Для начала рассмотрим порядок настройки простой сети, построенную на основе двух управляемых коммутаторов (рис. 7.1).

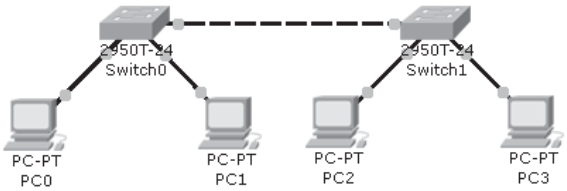

Рис. 7.1. Сеть, построенная на основе двух управляемых коммутаторов

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве два коммутатора типа 2950T-24 Switch0 и Switch1, и четыре компьютера PC0–PC3 так, как показано на рисунке 7.1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:

3.1. Присоедините прямым кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/1 коммутатора Switch0.
3.2. Присоедините прямым кабелем порт FastEthernet компьютера PC1 к порту FastEthernet1/1 коммутатора Switch0.
3.3. Присоедините прямым кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/1 коммутатора Switch1.
3.4. Присоедините прямым кабелем порт FastEthernet компьютера PC3 к порту FastEthernet1/1 коммутатора Switch1.
3.5. Подсоедините перекрестным кабелем порт GigabitEthernet0/1 коммутатора Switch0 к порту GigabitEthernet0/1 коммутатора Switch1.
4. Настройте компьютер PC0: задайте IP-адрес **172.16.10.1** и маску **255.255.0.0**.
5. Настройте компьютер PC1: задайте IP-адрес **172.16.20.1** и маску **255.255.0.0**.
6. Настройте компьютер PC2: задайте IP-адрес **172.16.10.2** и маску **255.255.0.0**
7. Настройте компьютер PC3: задайте IP-адрес **172.16.20.2** и маску **255.255.0.0**
8. Подождите до завершения процесса самонастройки коммутаторов (на всех портах должны появиться зеленые сигналы).
9. Для того, чтобы проверить работоспособность сети, передайте простой пакет с компьютера PC0 на компьютер PC2, а затем передайте пакет с компьютера PC1 на компьютер PC3.
10. Попытайтесь передать пакет с PC0 на PC3 — пакет передаваться не должен.
11. Переключите Cisco Packet Tracer в режим Simulation.
12. Передайте с компьютера PC0 ограниченное широковещательное сообщение в сеть:
12.1. На правой панели инструментов нажмите кнопку Add Complex PDU, чтобы создать сложный пакет, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши.
12.2. В окне Create Complex PDU укажите в списке Outgoing Port порт **FastEthernet**.
12.3. В списке Select Application укажите **PING**.
12.4. В поле Destination IP Address задайте широковещательный адрес **255.255.255.255**.
12.5. В поле Source IP Address задайте адрес компьютера PC0 **172.16.10.1**.
12.6. В поле времени жизни пакета TTL задайте значение **32**.
12.7. В поле типа обслуживания TOS задайте значение **0**.
12.8. В поле Sequence Number задайте значение **1**.
12.9. В поле параметров моделирования выберете пункт **One Shot** и задайте начальное время Time равным **0**.
12.10. Нажмите кнопку Create PDU, чтобы завершить процесс создания пакета.
12.11. В пошаговом режиме проследите за рассылкой сообщения.
13. Настройте виртуальные сети на коммутаторе Switch0, для чего введите на вкладке CLI последовательность команд:

```
Switch>en
Switch#vl da
Switch(vlan)#vlan 10
Switch(vlan)#vlan 20
Switch(vlan)#exit
Switch#conf t
Switch(config)#int fa0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/2
```

```
Switch(config-if)#sw ac vl 20
Switch(config-if)#int gi0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#exit
Switch#show vlan brief
Switch#exit
```

14. Настройте аналогичным образом VLAN на коммутаторе Switch1 (повторите весь набор команд, использованных при настройке коммутатора Switch0).
15. Для того, чтобы проверить работоспособность сети, передайте простой пакет с компьютера PC0 на компьютер PC2, а затем передайте пакет с компьютера PC1 на компьютер PC3.
16. Переключите Cisco Packet Tracer в режим Simulation.
17. Передайте с компьютера PC0 ограниченное широковещательное сообщение в сеть:
    - 17.1. На правой панели инструментов нажмите кнопку Add Complex PDU, чтобы создать сложный пакет, а затем установите курсор на компьютер PC0 и щелкните левой кнопкой мыши.
    - 17.2. В окне Create Complex PDU укажите в списке Outgoing Port порт **FastEthernet**.
    - 17.3. В списке Select Application укажите **PING**.
    - 17.4. В поле Destination IP Address задайте широковещательный адрес **255.255.255.255**.
    - 17.5. В поле Source IP Address задайте адрес компьютера PC0 **172.16.10.1**.
    - 17.6. В поле времени жизни пакета TTL задайте значение **32**.
    - 17.7. В поле типа обслуживания TOS задайте значение **0**.
    - 17.8. В поле Sequence Number задайте значение **1**.
    - 17.9. В поле параметров моделирования выберете пункт **One Shot** и задайте начальное время Time равным **0**.
    - 17.10. Нажмите кнопку Create PDU, чтобы завершить процесс создания пакета.
    - 17.11. В пошаговом режиме проследите за рассылкой сообщения. Если раньше широковещательное сообщение доходило до всех компьютеров, то теперь оно должно распространяться только внутри одной виртуальной локальной сети.
18. На всех четырех компьютерах PC0–PC3 измените маску интерфейса Fast Ethernet на **255.255.255.0**, но оставьте без изменений IP-адреса.
19. Сохраните модель сети в файле с именем **net_7_2_1**.
20. Завершите работу с программой Cisco Packet Tracer.

7.2.2. Первый способ объединения виртуальных сетей

После разделения сети на VLAN мы получим несколько локальных сетей, которые далее необходимо объединить в единое целое с помощью маршрутизаторов.

Рассмотрим первый способ объединения VLAN в единую сеть, который предполагает, что все коммутаторы подключены к маршрутизатору.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Загрузите из файла с именем **net_7_2_1** модель сети, созданную в предыдущем упражнении.

3. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
4. Сохраните модель сети в файле с именем **net_7_2_2**.
5. В группе Routers выберите модель маршрутизатора Router-PT и поместите маршрутизатор Router0 в рабочее пространство, расположив его так, как показано на рисунке 7.2.

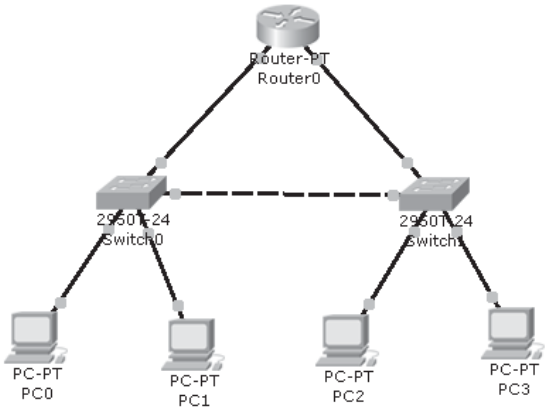

Рис. 7.2. Первый способ объединения виртуальных сетей

6. Присоедините прямым кабелем порт FastEthernet0/0 маршрутизатора Router0 к порту FastEthernet0/3 коммутатора Switch0.
7. Присоедините прямым кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet0/3 коммутатора Switch1.
8. Проведите дополнительную настройку параметров компьютеров:
   8.1. Для PC0 задайте шлюз **172.16.10.254**.
   8.2. Для PC1 задайте шлюз **172.16.20.254**.
   8.3. Для PC2 задайте шлюз **172.16.10.254**.
   8.4. Для PC3 задайте шлюз **172.16.20.254**.
9. Настройте порт FastEthernet0/3 на коммутаторе Switch0 для работы в режиме доступа, для чего введите на вкладке CLI последовательность команд:

```
Switch>en
Switch#conf t
Switch(config)#int fa0/3
Switch(config-if)#sw ac vl 10
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#exit
Switch#exit
```

10. Настройте порт FastEthernet0/3 на коммутаторе Switch1 для работы в режиме доступа, для чего введите на вкладке CLI последовательность команд:

```
Switch>en
Switch#conf t
Switch(config)#int fa0/3
Switch(config-if)#sw ac vl 20
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#exit
Switch#exit
```

11. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 172.16.10.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa1/0
Router(config-if)#ip ad 172.16.20.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
Router#exit
```

12. Переключите Cisco Packet Tracer в режим Simulation.
13. В пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC3. Если операция завершилась неудачно, нажмите кнопку Reset Simulation, а затем попробуйте повторить передачу пакета.
14. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
15. В пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1. Если операция завершилась неудачно, нажмите кнопку Reset Simulation, а затем попробуйте повторить передачу пакета. По какому маршруту пойдет этот пакет?
16. Сохраните модель сети в файле с именем **net_7_2_2**.
17. Завершите работу с программой Cisco Packet Tracer.

7.2.3. Второй способ объединения виртуальных сетей

Второй способ объединения VLAN предполагает, что только один из коммутаторов подключен к маршрутизатору (рис.7.3). При использовании этого способа подключенный к коммутатору интерфейс маршрутизатора должен быть настроен как магистральный порт и на нем должны быть созданы подинтерфейсы.

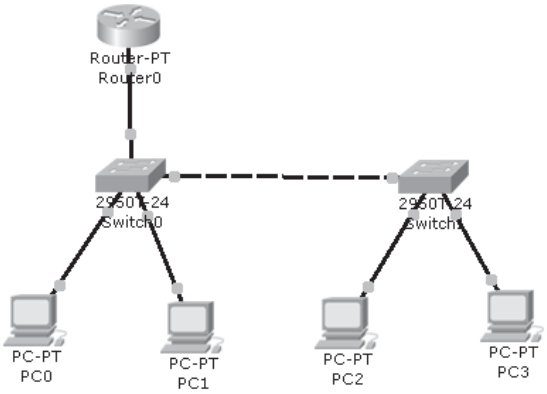

Рис. 7.3. Второй способ объединения виртуальных сетей

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Загрузите из файла с именем **net_7_2_1** модель сети, созданную в упражнении 7.2.1.
3. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
4. Сохраните модель сети в файле с именем **net_7_2_3**.
5. В группе Routers выберите модель Router-PT и поместите маршрутизатор Router0 в рабочее пространство, расположив его так, как показано на рисунке 7.3..
6. Присоедините прямым кабелем порт FastEthernet0/0 маршрутизатора Router0 к порту FastEthernet0/3 коммутатора Switch0.
7. Проведите дополнительную настройку параметров компьютеров:
   7.1. Для PC0 задайте шлюз **172.16.10.254**.
   7.2. Для PC1 задайте шлюз **172.16.20.254**.
   7.3. Для PC2 задайте шлюз **172.16.10.254**.
   7.4. Для PC3 задайте шлюз **172.16.20.254**.
8. Подождите до завершения процесса самонастройки коммутаторов (на всех портах должны появиться зеленые сигналы).
9. Настройте порт FastEthernet0/3 коммутатора Switch0 для работы в магистральном режиме, для чего введите на вкладке CLI последовательность команд:

```
Switch>en
Switch#conf t
Switch(config)#int fa0/3
Switch(config-if)#sw mo tr
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#exit
Switch#exit
```

10. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip ad 172.16.10.254 255.255.255.0
Router(config-subif)#int fa0/0.20
Router(config-subif)#en dot1q 20
Router(config-subif)#ip ad 172.16.20.254 255.255.255.0
Router(config-subif)#int fa0/0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
```

11. Проверьте наличие подсетей 172.16.10.0 и 172.16.20.0 в таблице маршрутизации, при помощи команды **sh ip route**. После этого введите команду exit и закройте окно Router0.
12. Передайте простой пакет с компьютера PC0 на компьютер PC3. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
13. Передайте простой пакет с компьютера PC2 на компьютер PC3. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
14. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
15. Переключите Cisco Packet Tracer в режим Simulation.
16. В пошаговом режиме передайте простой пакет с компьютера PC2 на компьютер PC3. По какому маршруту пойдет этот пакет?
17. Сохраните модель сети в файле с именем **net_7_2_3**.
18. Завершите работу с программой Cisco Packet Tracer.

7.3. Задание для самостоятельной работы

Добавьте к приведенной на рисунке 7.3 модели еще два компьютера и один коммутатор таким образом, чтобы к каждому коммутатору было подключено по два компьютера, принадлежащих к различным подсетям.

8. ПРОТОКОЛ EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) — улучшенный протокол маршрутизации внутреннего шлюза. Протокол EIGRP появился в 1994 году в результате усовершенствования протокола IGRP, который был разработан фирмой Cisco для многопротокольных маршрутизаторов еще в 80-х годах прошлого века.

В литературе, описывающей протокол EIGRP, используются следующие специфические термины:

- **Таблица соседства** — таблица, в которой маршрутизатор хранит список соседних маршрутизаторов.
- **Топологическая таблица** — таблица, в которой маршрутизатор хранит уже известные маршруты к получателям.
- **Преемник** — это первичный маршрут, который используется для достижения получателя.
- **Вероятный преемник** — это сосед, который находится на пути к получателю. Через вероятного преемника прокладывается резервный путь к получателю. Топологическая таблица может хранить множество вероятных преемников.

В протоколе EIGRP используются следующие типы пакетов:

- Пакет **hello** (приветствие) используется для поиска соседей. Такие пакеты рассылаются в широковещательном режиме и имеют номер подтверждения, равный нулю.
- Пакет **update** (обновление) используется для пересылки данных о маршрутах. При обнаружении нового маршрута или при завершении процедуры сходимости пакеты обновления рассылаются в широковещательном режиме; для синхронизации топологических таблиц обновления рассылаются соседям в симплексном режиме.
- Пакеты **queries** (запросы) маршрутизатор посылает соседям, когда не может найти вероятного приемника. Путем использования запросов маршрутизатор пытается выяснить у соседей, имеется ли у кого-либо из них вероятный приемник к получателю.
- Пакет **replies** (ответ) посылается маршрутизатором в ответ на пакет запроса.
- Пакет **ACK** (подтверждение) используется для подтверждения получения пакета обновления, запроса или ответа. Пакеты подтверждения представляют собой пакеты hello, которые рассылаются в симплексном режиме и имеют номер подтверждения, отличный от нуля.

8.1. Команды Cisco IOS для настройки EIGRP

Для того чтобы на маршрутизаторе заработал протокол EIGRP, необходимо настроить интерфейсы, на которых будет использоваться EIGRP, включить процесс EIGRP и указать подсети, с которыми этот процесс должен взаимодействовать.

Включение процесса EIGRP выполняется по команде **router eigrp** (сокращенно — **ro eigrp**), которая имеет следующий формат:

`router eigrp` ***`autonomous-system-number`***

где *autonomous-system-number* — номер, идентифицирующий автономную систему (целое число в диапазоне от 1 до 65535). Значение идентификатора автономной системы должно совпадать у всех маршрутизаторов сети.

Для того чтобы указать подсеть, которая является частью сети EIGRP, используется команда **network** (сокращенно — **ne**), которая имеет следующий формат:

`network` ***`network-number`***

где *network-number* — адрес подсети.

При использовании в сети последовательных каналов, например, Frame Relay или SMDS, необходимо указывать пропускную способность каналов для интерфейсов, которые к ним присоединены. Если значение пропускной способности явно не задано, то протокол EIGRP будет считать его равным пропускной способности какала T1. В том случае, когда последовательный канал работает медленнее, чем T1, использование заданного по умолчанию значения пропускной способности может привести к нарушению процесса маршрутизации.

Для того чтобы указать пропускную способность интерфейса, используется команда **bandwidth** (сокращенно — **ba**), которая имеет следующий формат:

`bandwidth` ***`kilobits`***

где *kilobits* — пропускная способность канала, указанная в килобитах в секунду.

Для включения журналирования (логгирования) изменений состояния соединений используется команда **eigrp log-neighbor-changes**

Для проверки правильности работы протокол EIGRP можно использовать следующие команды:

- команда **show ip route eigrp** (сокращенно — **sh ip ro eigrp**) отображает общую информацию о работе протокола EIGRP;
- команда **show ip eigrp neighbors** (сокращенно — **sh ip eigrp ne**) отображает информацию о соседних сетях;
- команда **show ip eigrp topology** (сокращенно — **sh ip eigrp to**) отображает информацию о топологии сети;
- команда **show ip eigrp traffic** (сокращенно — **sh ip eigrp tra**) отображает статистику отправки, приема и пересылки служебных пакетов.

8.1.1. Настройка маршрутизаторов для работы по протоколу EIGRP

Рассмотрим процесс настройки маршрутизаторов для работы по протоколу EIGRP на примере сети, изображенной на рисунке 8.1.

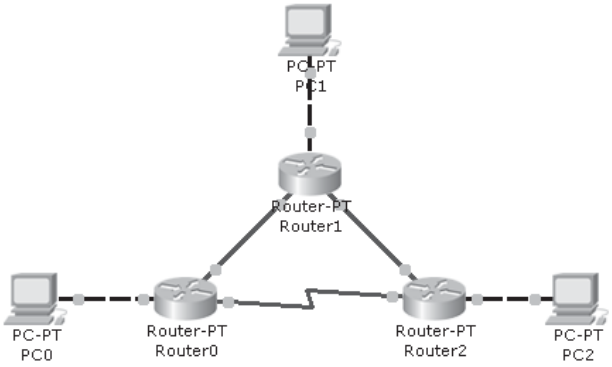

Рис. 8.1. Схема сети для упражнения по настройке EIGRP

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую область Cisco Packet Tracer:
   2.1. В группе Routers выберите абстрактную модель маршрутизатора Router-PT и поместите в рабочую область маршрутизаторы Router0, Router1 и Router2
   2.2. Поместите в рабочую компьютеры PC0, PC1 и PC2.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet0/0 маршрутизатора Router1.
   3.3. Подключите перекрестным кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/0 маршрутизатора Router2.
   3.4. Подключите оптоволоконным кабелем порт FastEthernet4/0 маршрутизатора Router0 к порту FastEthernet4/0 маршрутизатора Router1.
   3.5. Подключите оптоволоконным кабелем порт FastEthernet5/0 маршрутизатора Router1 к порту FastEthernet4/0 маршрутизатора Router2.
   3.6. Выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial2/0 маршрутизатора Router0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router2.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.2**, маску **255.255.255.0** и адрес шлюза **192.168.2.1**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.3.2**, маску **255.255.255.0** и адрес шлюза **192.168.3.1**.
7. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
```

```
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa4/0
Router(config-if)#ip ad 192.168.4.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#ip ad 192.168.6.1 255.255.255.0
Router(config-if)#clock rate 56000
Router(config-if)#bandwidth 56
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.4.0
Router(config-router)#net 192.168.6.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

8. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa4/0
Router(config-if)#ip ad 192.168.4.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa5/0
Router(config-if)#ip ad 192.168.5.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.4.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

9. Настройте маршрутизатор Router2 для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.3.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa4/0
Router(config-if)#ip ad 192.168.5.2 255.255.255.0
```

```
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#ip ad 192.168.6.2 255.255.255.0
Router(config-if)#ba 56
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.5.0
Router(config-router)#net 192.168.6.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0, 192.168.5.0 и 192.168.6.0. Если в одной из таблиц отсутствует какая-либо сеть — немного подождите.
11. Проверьте сетевые соединения:
    11.1. Передайте простой пакет с компьютера PC0 на компьютер PC1. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
    11.2. Передайте простой пакет с компьютера PC1 на компьютер PC2.
    11.3. Передайте простой пакет с компьютера PC2 на компьютер PC0.
12. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
13. Переключите Cisco Packet Tracer в режим Simulation.
14. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC2. По какому маршруту будет передаваться пакет?
15. Переключите Cisco Packet Tracer в режим Realtime.
16. Проверьте настройку маршрутизатора Router0 с помощью команд Cisco IOS:
    16.1. Выберите в рабочем пространстве маршрутизатор Router0.
    16.2. В окне Router0 выберите вкладку CLI.
    16.3. Если на экране отсутствует приглашение для ввода команды, то нажмите клавишу Enter.
    16.4. Когда в командной строке появится приглашение Router>, введите команду **en**.
    16.5. Когда в командной строке появится приглашение Router#, введите команду **sh ip route**, для того чтобы вывести на экран таблицу маршрутизации.
    16.6. Введите команду **sh ip route eigrp**, чтобы вывести на экран общую информацию о работе протокола EIGRP.
    16.7. Введите команду **sh ip eigrp neighbors**, чтобы вывести на экран информацию о соседних сетях.
    16.8. Введите команду **sh ip eigrp topology**, чтобы вывести на экран информацию о топологии сети.
    16.9. Введите команду **sh ip eigrp traffic**, чтобы вывести на экран статистику отправки, приема и пересылки служебных пакетов.
    16.10. Введите команду **exit**, чтобы завершить работу в привилегированном режиме.
    16.11. Закройте окно Router0.
17. Протестируйте соединение между компьютерами с помощью диагностических утилит из стека протоколов TCP/IP:
    17.1. Выберите в рабочем пространстве компьютер PC0.

17.2. В окне PC0 выберите вкладку Desktop.
17.3. На вкладке Desktop нажмите кнопку Command Prompt, чтобы открыть окно, имитирующее работу в режиме командной строки.
17.4. Введите команду **ping 192.168.3.2** и просмотрите результат ее выполнения.
17.5. Введите команду **tracert 192.168.3.2** и просмотрите результат ее выполнения.
17.6. Закройте окно Command Prompt.
17.7. Закройте окно PC0.
18. Сохраните модель сети в файле с именем **net_8_1_1**.
19. Нажмите на правой панели инструментов кнопку Delete, наведите крестик на оптоволоконную линию связи между маршрутизаторами Router0 и Router1 и щелкните левой кнопкой мыши, чтобы разорвать эту связь.
20. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов. Что изменилось в таблицах маршрутизации после разрыва линии связи?
21. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
22. Переключите Cisco Packet Tracer в режим Simulation.
23. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC2, чтобы проверить медленный последовательный резервный канал связи между маршрутизаторами Router0 и Router2.
24. Завершите работу с программой Cisco Packet Tracer.

8.2. Распределение нагрузки

Распределение нагрузки — это способность маршрутизатора распределять трафик через все сетевые порты, имеющие одно и то же расстояние до адреса назначения.

Распределение нагрузки повышает пропускную способность сети за счет увеличения процента использования сетевых сегментов.

По умолчанию Cisco IOS допускает распределение трафика между четырьмя путями, имеющими равные характеристики стоимости, однако максимальное количество путей можно при необходимости увеличить, используя команду **maximum-path**.

8.2.1. Моделирование распределения нагрузки

Рассмотрим в качестве примера распределение нагрузки между двумя путями в сети, изображенной на рисунке 8.2.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую область Cisco Packet Tracer:
   2.1. Поместите в рабочую область маршрутизаторы Router0, Router1, Router2 и Router3 типа Router-PT.
   2.2. Поместите в рабочее пространство компьютеры PC0 и PC1.

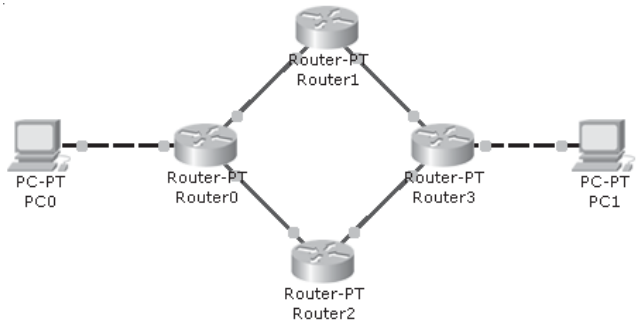

Рис. 8.2. Сеть с двумя равноценными путями между маршрутизаторами Router0 и Router3

3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet0/0 маршрутизатора Router3.
   3.3. Подключите оптоволоконным кабелем порт FastEthernet4/0 маршрутизатора Router0 к порту FastEthernet4/0 маршрутизатора Router1.
   3.4. Подключите оптоволоконным кабелем порт FastEthernet5/0 маршрутизатора Router0 к порту FastEthernet4/0 маршрутизатора Router2.
   3.5. Подключите оптоволоконным кабелем порт FastEthernet5/0 маршрутизатора Router1 к порту FastEthernet4/0 маршрутизатора Router3.
   3.6. Подключите оптоволоконным кабелем порт FastEthernet5/0 маршрутизатора Router2 к порту FastEthernet5/0 маршрутизатора Router3.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.2**, маску **255.255.255.0** и адрес шлюза **192.168.2.1**.
6. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa4/0
Router(config-if)#ip ad 192.168.3.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa5/0
Router(config-if)#ip ad 192.168.4.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.3.0
```

```
Router(config-router)#net 192.168.4.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

7. Настройте маршрутизатор Router1, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa4/0
Router(config-if)#ip ad 192.168.3.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa5/0
Router(config-if)#ip ad 192.168.5.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

8. Настройте маршрутизатор Router2, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa4/0
Router(config-if)#ip ad 192.168.4.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa5/0
Router(config-if)#ip ad 192.168.6.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.4.0
Router(config-router)#net 192.168.6.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

9. Настройте маршрутизатор Router3, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa4/0
Router(config-if)#ip ad 192.168.5.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int fa5/0
Router(config-if)#ip ad 192.168.6.1 255.255.255.0
```

```
Router(config-if)#no shut
Router(config-if)#ro eigrp 100
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.5.0
Router(config-router)#net 192.168.6.0
Router(config-router)#exit
Router(config)#exit
Router#exit
```

10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0–192.168.6.0. Если в одной из таблиц отсутствует какая-либо сеть — немного подождите.
11. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить наличие соединения. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
12. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
13. Проверьте настройку маршрутизатора Router0 с помощью команд Cisco IOS.
14. Протестируйте соединение между компьютерами с помощью диагностических утилит из стека протоколов TCP/IP:
    14.1. Выберите в рабочем пространстве компьютер PC0.
    14.2. В окне PC0 выберите вкладку Desktop.
    14.3. На вкладке Desktop нажмите кнопку Command Prompt.
    14.4. Введите команду **ping 192.168.2.2** и просмотрите результат ее выполнения.
    14.5. Введите команду **tracert 192.168.2.2** и просмотрите результат ее выполнения.
    14.6. Закройте окно Command Prompt.
    14.7. Закройте окно PC0.
15. Переключите Cisco Packet Tracer в режим Simulation.
16. В пошаговом режиме передайте друг за другом два простых пакета с компьютера PC0 на компьютер PC1:
    16.1. Нажмите на правой панели инструментов кнопку Add Simple PDU, щелкните левой кнопкой мыши по компьютеру PC0, а затем — по компьютеру PC1, чтобы задать направление передачи первого простого пакета.
    16.2. Снова нажмите на правой панели инструментов кнопку Add Simple PDU, щелкните левой кнопкой мыши по компьютеру PC0, а затем — по компьютеру PC1, чтобы задать направление передачи второго простого пакета.
    16.3. Используя кнопку Capture / Forward, передайте пакеты с компьютера PC0 на компьютер PC1 и обратно. По какому маршруту будет передаваться каждый из пакетов?
17. Сохраните модель сети в файле с именем **net_8_2_1**.
18. Завершите работу с программой Cisco Packet Tracer.

8.3. Задание для самостоятельной работы

В целях тренировки попробуйте самостоятельно создать и наладить модель сети, изображенной на рисунке 8.3, используя протокол маршрутизации EIGRP. Компьютеры должны быть подключены к маршрутизаторам перекрестными кабелями, а маршрутизаторы должны быть соединены друг с другом оптоволоконными кабелями и кабелями для создания последовательных каналов.

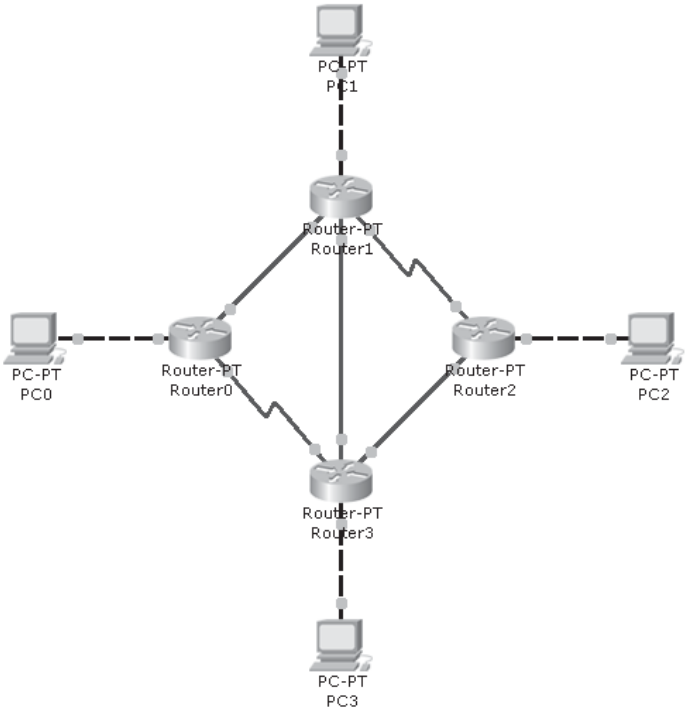

Рис. 8.3. Задание для самостоятельной работы

По какому маршруту пойдет пакет от компьютера PC0 к компьютеру PC2?

9. ПРОТОКОЛ OSPF

Протокол OSPF был разработан в 1988 году группой Internet Engineering Task Force для крупных компьютерных сетей с большим количеством маршрутизаторов. Этот протокол позволяет разделять сети на части — так называемые зоны.

Протокол OSPF основывается на технологии отслеживания состояния канала.

OSPF представляет собой протокол внутреннего шлюза: он распространяет маршрутную информацию между маршрутизаторами, принадлежащими к одной и той же автономной системе.

Протокол OSPF поддерживает маскирование подсетей и использование масок с переменной длиной.

В литературе, описывающей протокол OSPF, используются следующие специфические термины:

- **Автономная система** — группа маршрутизаторов, обменивающаяся маршрутной информацией с помощью одного и того же протокола маршрутизации (в данном случае — OSPF).
- **Зона** (area) — совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор.
- **Магистральная зона** (backbone area) — это зона, которая является транзитной между другими зонами. Магистральная зона имеет номер 0. При наличии нескольких зон магистральная зона занимает центральное положение и все остальные зоны должны быть подключены к магистральной зоне для обмена информацией.
- **Тупиковая зона** (stub area) — зона, не принимающая информацию о маршрутах, являющихся внешними для данной автономной системы. При необходимости она направляет трафик за пределы автономной системы, используя маршрут по умолчанию, который обозначается как 0.0.0.0.
- **Внутренний маршрутизатор** — это маршрутизатор, все интерфейсы которого находятся в одной и той же зоне.
- **Магистральный маршрутизатор** — это маршрутизатор, установленный в магистральной зоне, то есть маршрутизатор, по крайней мере один интерфейс которого подключен к зоне 0.
- **Пограничный маршрутизатор** (Area Border Router, сокращенно — ABR) — это маршрутизатор, интерфейсы которого подключены к нескольким зонам. Пограничные маршрутизатор ведут базы данных состояния каналов со всеми зонами, к которым они подключены, и маршрутизируют входящий и исходящий траффик. Информация, направляемая в другие зоны, может достичь их только через пограничные маршрутизаторы.
- **Пограничный маршрутизатор автономной системы** (Autonomous System Boundary Router, сокращенно — ASBR) — это маршрутизатор, имеющий по крайней мере один интерфейс с внешней сетью (другой автономной системой). Внешняя сеть в этом случае может работать как под управлением OSPF, так и под управлением другого протокола маршрутизации.
- **Ссылка** — соединение маршрутизатора и одной из подключенных к нему сетей.
- **Состояние канала** — состояние соединения между двумя маршрутизаторами.
- **Соседи** — маршрутизаторы, имеющие интерфейсы в общей сети.

- **База данных о соседях** — таблица, содержащая список всех соседей, с которыми установлена связь.
- **Топологическая база данных** — таблица, содержащая информацию о состоянии соединений с соседними маршрутизаторами.
- Протокол OSPF может работать со следующими сетевыми топологиями:
- **Топология точка**—точка имеет место в сети, объединяющей два маршрутизатора друг с другом.
- **Широковещательная топология коллективного доступа** имеет место в сети, в которой присутствует более двух маршрутизаторов и возможна адресация одного сообщения сразу на все маршрутизаторы.
- **Нешироковещательная топология коллективного доступа** имеет место в сети, в которой присутствует более двух маршрутизаторов и отсутствует возможность широковещательной передачи сообщений.

Маршрутизаторы OSPF обмениваются топологической информацией, посылая друг другу объявления о состоянии связей (Link State Advertisement, сокращенно — LSA). Маршрутизаторы также контролируют состояние связей, рассылая друг другу сообщения HELLO каждые десять секунд. Если сообщения перестают поступать от какого-либо из непосредственных соседей, то маршрутизатор делает вывод о том, что связь стала неработоспособной, корректирует свою топологическую базу данных и рассылает соседям сообщение LSA об этом изменении.

9.1. Команды Cisco IOS для настройки OSPF

Для того чтобы на маршрутизаторе заработал протокол OSPF, необходимо настроить интерфейсы, на которых будет использоваться OSPF, включить процесс OSPF и указать подсети, с которыми этот процесс должен взаимодействовать.

Включение процесса OSPF выполняется по команде **router ospf** (сокращенно — **ro ospf**), которая имеет следующий формат:

```
router ospf process-id
```

где *process-id* — идентификатор процесса OSPF (целое число в диапазоне от 1 до 65535)

Так как запускать на одном маршрутизаторе несколько процессов OSPF не рекомендуется, то значение идентификатора процесса можно выбирать произвольным образом.

Для того чтобы указать подсеть, которая является частью сети OSPF, используется команда **network area**, которая имеет следующий формат:

```
network address wildcard-mask area area-id
```

где *address* — адрес подсети или интерфейса, *wildcard-mask* — шаблон маски подсети, *area-id* — номер зоны OSPF, к которой относится подсеть.

Так как в процессе обмена сообщениями маршрутизаторы должны передавать соседям свои идентификаторы, то каждому маршрутизатору должен быть присвоен уникальный идентификатор RID.

Идентификатор **RID** представляет собой 32-битовый номер и записывается в формате IP-адреса.

Идентификатор может быть явным образом присвоен маршрутизатору с помощью команды **router-id**, которая имеет следующий формат:

```
router-id ip-address
```

где *ip-address* — идентификатор маршрутизатора.

Если идентификатор не был присвоен явно, то в качестве RID выбирается наибольший из IP-адресов интерфейсов обратной петли (loopback), а если таковые отсутствуют — выбирается наибольший из IP-адресов рабочих интерфейсов.

Для проверки правильности работы протокол OSPF можно использовать следующие команды:

- команда **show ip ospf** (сокращенно — **sh ip ospf**) отображает общую информацию о процессе маршрутизации протокола OSPF;
- команда **show ip ospf *process-id*** отображает информацию о процессе OSPF с заданным номером *process-id*;
- команда **show ip ospf neighbor** (сокращенно — **sh ip ospf ne**) отображает информацию о соседях;
- команда **show ip ospf database** (сокращенно — **sh ip ospf dat**) отображает записи о состоянии каналов, содержащиеся в базе данных маршрутизатора;
- команда **show ip ospf interface** (сокращенно — **sh ip ospf int**) отображает информацию об интерфейсах;
- команда **show ip ospf adj** отображает информацию о событиях, связанных с построением или разрывом отношений смежности;
- команда **show ip ospf border-routers** отображает таблицы маршрутизации протокола OSPF на граничных маршрутизаторах;
- команда **show ip ospf virtual-links** отображает параметры, описывающие текущее состояние виртуальных каналов протокола OSPF.

9.1.1. Сеть с одной зоной

Рассмотрим процесс настройки маршрутизаторов для работы по протоколу OSPF на примере простой сети с одной зоной, схема которой изображена на рисунке 9.1,

Рис. 9.1. Схема для создания простой сети с одной зоной

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую область Cisco Packet Tracer:
   2.1. В группе Routers выберите модель маршрутизатора 1841 и поместите в рабочую область маршрутизаторы Router0 и Router1.
   2.2. Поместите в рабочую компьютеры PC0 и PC1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:

3.1. Подключите перекрестным кабелем компьютер PC0 к порту FastEthernet0/0 маршрутизатора Router0.
3.2. Подключите перекрестным кабелем компьютер PC1 к порту FastEthernet0/0 маршрутизатора Router1.
3.3. Подключите перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet1/0 маршрутизатора Router1.

4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.2**, маску **255.255.255.0** и адрес шлюза **192.168.2.1**.
6. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#hostname Router0
Router0(config)#line con 0
Router0(config-line)#logging synchronous
Router0(config-line)#int f0/0
Router0(config-if)#ip ad 192.168.1.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#int f0/1
Router0(config-if)#ip ad 192.168.3.1 255.255.255.252
Router0(config-if)#no shut
Router0(config-if)#exit
Router0(config)#router ospf 1
Router0(config-router)#net 192.168.1.0 0.0.0.255 a 0
Router0(config-router)#net 192.168.3.0 0.0.0.3 a 0
Router0(config-router)#router-id 1.1.1.1
Router0(config-router)#end
Router0#clear ip ospf process
Reset ALL OSPF processes? [no]: y
Router0#exit
```

7. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho Router1
Router1(config)#line con 0
Router1(config-line)#logg syn
Router1(config-line)#int f0/0
Router1(config-if)#ip ad 192.168.2.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#int f0/1
Router1(config-if)#ip ad 192.168.3.2 255.255.255.252
Router1(config-if)#no shut
Router1(config-if)#exit
Router1(config)#ro ospf 2
Router1(config-router)#net 192.168.2.0 0.0.0.255 a 0
```

```
Router1(config-router)#net 192.168.3.0 0.0.0.3 a 0
Router1(config-router)#ro 2.2.2.2
Router1(config-router)#end
Router1#cle ip ospf pr
Reset ALL OSPF processes? [no]: y
Router1#exit
```

8. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0. Если в одной из таблиц отсутствует какая-либо сеть — немного подождите.
9. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
10. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
11. Проверьте настройку маршрутизатора Router0 с помощью команд Cisco IOS:
    11.1. Выберите в рабочем пространстве маршрутизатор Router0.
    11.2. В окне Router0 выберите вкладку CLI.
    11.3. Если на экране отсутствует приглашение для ввода команды, то нажмите клавишу Enter.
    11.4. Когда в командной строке появится приглашение Router0>, введите команду **en**.
    11.5. Когда в командной строке появится приглашение Router0#, введите команду **sh ip ro**, для того чтобы вывести на экран таблицу маршрутизации.
    11.6. Введите команду **sh ip ospf**, чтобы вывести на экран общую информацию о работе протокола OSPF.
    11.7. Введите команду **sh ip ospf ne**, чтобы вывести на экран информацию о соседях по протоколу OSPF.
    11.8. Введите команду **sh ip ospf int**, чтобы вывести на экран информацию об интерфейсах, с которыми работает OSPF.
    11.9. Введите команду **exit**, чтобы завершить работу в привилегированном режиме.
    11.10. Закройте окно Router0.
12. Переключите Cisco Packet Tracer в режим Simulation.
13. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC1. После выполнения каждого шага просматривайте передаваемый пакет, чтобы видеть, какие изменения будут происходить в заголовках различных уровней.
14. Переключите Cisco Packet Tracer в режим Realtime.
15. Протестируйте соединение между компьютерами с помощью диагностических утилит из стека протоколов TCP/IP:
    15.1. Выберите в рабочем пространстве компьютер PC0.
    15.2. В окне PC0 выберите вкладку Desktop.
    15.3. На вкладке Desktop нажмите кнопку Command Prompt, чтобы открыть окно, имитирующее работу операционной системы компьютера в режиме командной строки.
    15.4. Введите команду **ping 192.168.2.2** и просмотрите результат ее выполнения.
    15.5. Введите команду **tracert 192.168.2.2** и просмотрите результат ее выполнения.
    15.6. Закройте окно Command Prompt.
    15.7. Закройте окно PC0.
16. Сохраните модель сети в файле с именем **net_9_1_1**.
17. Завершите работу с программой Cisco Packet Tracer.

9.1.2. Сеть с двумя зонами

В качестве следующего примера рассмотрим процесс настройки сети с двумя зонами, схема которой изображена на рисунке 9.2,

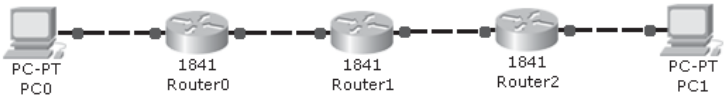

Рис. 9.2. Схема для создания сети с двумя зонами

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую область Cisco Packet Tracer:
   2.1. В группе Routers выберите модель маршрутизатора 1841 и поместите в рабочую область маршрутизаторы Router0, Router1и Router2.
   2.2. Поместите в рабочую компьютеры PC0 и PC1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем компьютер PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем компьютер PC1 к порту FastEthernet0/0 маршрутизатора Router2.
   3.3. Подключите перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet0/0 маршрутизатора Router1.
   3.4. Подключите перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router2 к порту FastEthernet1/0 маршрутизатора Router1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
6. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho Router0
Router0(config)#line con 0
Router0(config-line)#logg syn
Router0(config-line)#int f0/0
Router0(config-if)#ip ad 192.168.1.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#int f0/1
Router0(config-if)#ip ad 192.168.3.1 255.255.255.252
Router0(config-if)#no shut
Router0(config-if)#exit
Router0(config)#ro ospf 1
Router0(config-router)#net 192.168.1.0 0.0.0.255 a 0
```

```
Router0(config-router)#net 192.168.3.0 0.0.0.3 a 0
Router0(config-router)#router-id 1.1.1.1
Router0(config-router)#end
Router0#cle ip ospf pro
Reset ALL OSPF processes? [no]: y
Router0#exit
```

7. Настройте Router1 как граничный маршрутизатор между нулевой и первой зонами, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho Router1
Router1(config)#line con 0
Router1(config-line)#logg syn
Router1(config-line)#int f0/0
Router1(config-if)#ip ad 192.168.3.2 255.255.255.252
Router1(config-if)#no shut
Router1(config-if)#int f0/1
Router1(config-if)#ip ad 192.168.4.1 255.255.255.252
Router1(config-if)#no shut
Router1(config-if)#exit
Router1(config)#ro ospf 2
Router1(config-router)#net 192.168.3.0 0.0.0.3 a 0
Router1(config-router)#net 192.168.4.0 0.0.0.3 a 1
Router1(config-router)#ro 2.2.2.2
Router1(config-router)#end
Router1#cle ip ospf pr
Reset ALL OSPF processes? [no]: y
Router1#exit
```

8. Настройте маршрутизатор Router2, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho Router2
Router2(config)#line con 0
Router2(config-line)#logg syn
Router2(config-line)#int f0/0
Router2(config-if)#ip ad 192.168.2.1 255.255.255.0
Router2(config-if)#no shut
Router2(config-if)#int f0/1
Router2(config-if)#ip ad 192.168.4.2 255.255.255.252
Router2(config-if)#no shut
Router2(config-if)#exit
Router2(config)#ro ospf 3
Router2(config-router)#net 192.168.2.0 0.0.0.255 a 1
Router2(config-router)#net 192.168.4.0 0.0.0.3 a 1
Router2(config-router)#ro 3.3.3.3
Router2(config-router)#end
```

```
Router2#cle ip ospf pro
Reset ALL OSPF processes? [no]: y
Router2#exit
```

9. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0, 192.168.3.0 и 192.168.4.0. Если в одной из таблиц отсутствует какая-либо сеть - немного подождите.
10. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
11. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
12. Проверьте настройку маршрутизатора Router1 с помощью команд Cisco IOS:
13. Переключите Cisco Packet Tracer в режим Simulation.
14. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC1. После выполнения каждого шага просматривайте передаваемый пакет, чтобы видеть, какие изменения будут происходить в заголовках различных уровней.
15. Переключите Cisco Packet Tracer в режим Realtime.
16. Протестируйте соединение между компьютерами с помощью диагностических утилит из стека протоколов TCP/IP:
17. Сохраните модель сети в файле с именем **net_9_1_2**.
18. Завершите работу с программой Cisco Packet Tracer.

9.2. Задание для самостоятельной работы

В целях тренировки попробуйте самостоятельно создать и наладить модель сети, изображенной на рисунке 9.3, используя протокол маршрутизации OSPF.

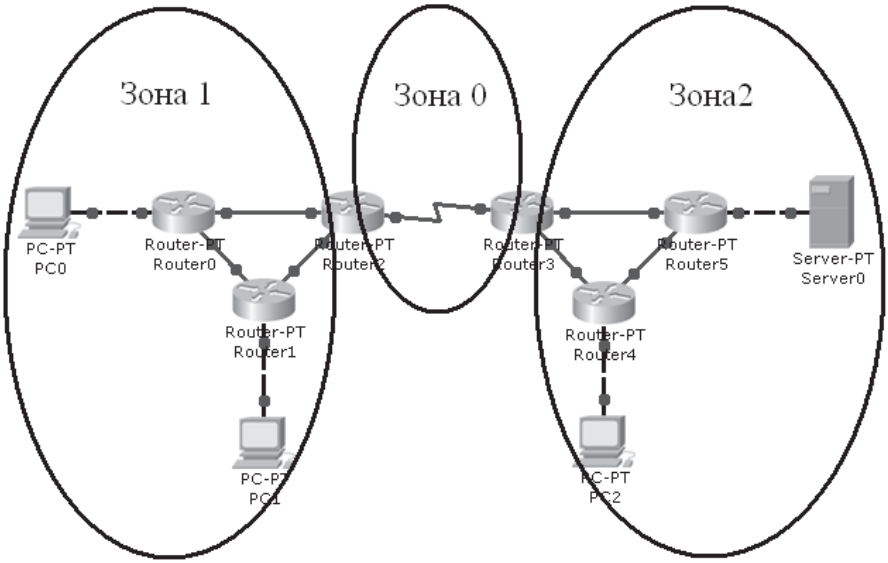

Рис. 9.3. Задание для самостоятельной работы

10. БЕСПРОВОДНЫЕ СЕТИ WI-FI

Логотип **Wi-Fi** — это торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11.

В сетях стандарта IEEE 802.11 используется два разных типа устройств для соединения:

- узловые передатчики (точки доступа);
- сетевые адаптеры (клиенты).

В зависимости от количества компьютеров в сети и расстояния между ними, беспроводные сети могут быть созданы двумя различными способами:

- сеть без базовой станции (**Ad Hoc**);
- сеть с точкой доступа (**Infrastructure Network**).

В сети, использующей способ Ad Hoc, базовая станция отсутствует и передача данных при котором осуществляется в режиме «точка-точка». Компьютеры в такой сети непосредственно взаимодействуют друг с другом. В режиме Ad Hoc требуется минимум оборудования: каждый компьютер должен быть оснащен только беспроводным адаптером. Основными недостатками режима Ad Hoc являются ограниченный диаметр сети и невозможность подключения к внешней сети. Дальность связи в режиме Ad Hoc составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

Реализованные в программе Cisco Packet Tracer модели беспроводных устройств режим Ad Hoc **не поддерживают**.

Для организации долговременных беспроводных сетей используют инфраструктурный режим. В этом режиме компьютеры взаимодействуют друг с другом через базовую станцию — **точку доступа** (Access Point), которая выполняет в беспроводной сети роль концентратора. В компьютерной сети может быть несколько точек доступа, объединенных проводной сетью Ethernet. Через точку доступа возможен выход во внешние проводные сети.

С целью обеспечения безопасности передачи данных разработчики технологии беспроводных сетей предусмотрели на MAC-уровне защитный механизм, включающий аутентификацию станций и шифрование передаваемых данных. Этот механизм должен был обеспечивать такой же уровень защиты, как и в обычных сетях Ethernet, поэтому его назвали **WEP** (Wired Equivalent Privacy). Однако алгоритм WEP использовал ключи длиной 40 бит и имел невысокую криптостойкость, поэтому на смену ему пришел сначала улучшенный алгоритм шифрования **WPA** (Wi-Fi Protected Access), а затем алгоритм **WPA2**.

10.1. Создание сети Wi-Fi с точкой доступа

В процессе создания сети для точки доступа и всех беспроводных адаптеров необходимо настроить следующие параметры:

1) идентификатор беспроводной сети SSID (Service Set IDentifier);
2) используемый канал передачи данных (от 1 до 13);
3) скорость передачи данных (по умолчанию этот параметр имеет значение Auto и скорость выбирается автоматически);
4) режим аутентификации;
5) режим шифрования передаваемых данных;

6) формат ключа шифрования.

Значения перечисленных параметров у всех входящих в сеть беспроводных устройств должны совпадать.

Если в сети отсутствует DHCP-сервер, то для сетевых адаптеров всех рабочих станции необходимо вручную задать маску сети и статические IP-адреса.

К одной сети Ethernet может быть подключено несколько точек доступа. Если все точки доступа имеют одинаковый SSID, то сетевые адаптеры рабочих станций будут подключаться к ближайшей точке доступа (к точке доступа, от которой поступает наиболее мощный радиосигнал).

Если точки доступа имеют различные SSID, то сетевой адаптеры будут подключаться к точке доступа, SSID которой совпадает с SSID адаптера.

10.1.1. Беспроводная сеть с одной точкой доступа

В этом упражнении мы создадим и настроим локальную сеть с одной точкой доступа, изображенную на рисунке 10.1.

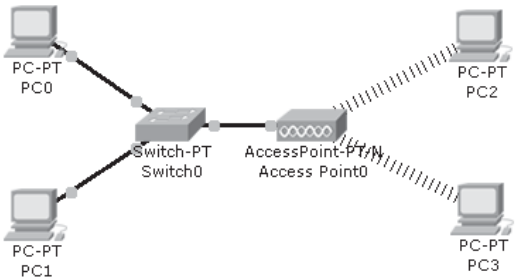

Рис. 10.1. Беспроводная сеть с одной точкой доступа

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. В группе End Devices выберите модель PC-PT.
   2.2. Поместите в рабочее пространство компьютеры PC0 и PC1 типа PC-PT.
   2.3. В группе Custom Made Devices выберите модель Wireless PC.
   2.4. Поместите в рабочее пространство компьютеры PC2 и PC3 типа Wireless PC.
   2.5. В группе Switches выберите модель Switch-PT.
   2.6. Поместите в рабочее пространство коммутатор Switch0 типа Switch-PT.
   2.7. В группе Wireless Devices выберите модель AccessPoint-PT-N.
   2.8. Поместите в рабочее пространство точку доступа Access Point0 типа AccessPoint-PT-N.
3. Соедините прямыми медными кабелями коммутатор с точкой доступа и компьютерами PC0 и PC1 так, как показано на рисунке 10.1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1** и маску **255.255.255.0**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.1.2** и маску **255.255.255.0**.

6. Настройте компьютер PC2:
   6.1. Выберите в рабочем пространстве компьютер PC2.
   6.2. В окне PC2 выберите вкладку Config и нажмите кнопку Wireless0.
   6.3. Задайте в поле SSID значение **Net01**.
   6.4. Отключите аутентификацию: установите переключатель Authentication в положение **Disabled**.
   6.5. Отключите шифрование: установите в выпадающем списке Encryption Type значение **Disabled**.
   6.6. Задайте использование статической конфигурации IP, адрес **192.168.1.3** и маску **255.255.255.0** (рис 10.2).
   6.7. Закройте окно PC2.

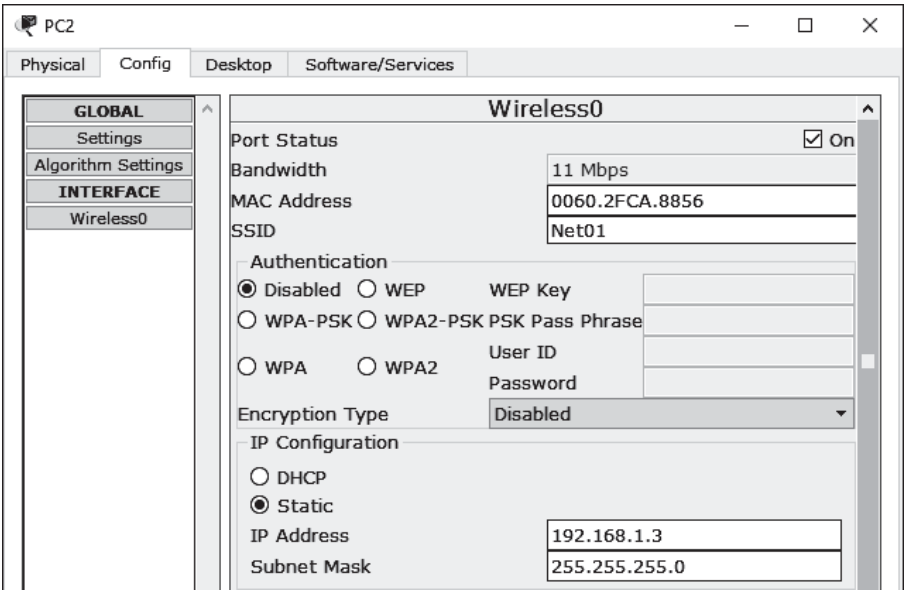

Рис. 10.2. Настройка параметров адаптера беспроводной сети на компьютере PC2

7. Настройте компьютер PC3: задайте SSID **Net01**, отключите аутентификацию и шифрование, задайте IP-адрес **192.168.1.4** и маску **255.255.255.0**.
8. Настройте точку доступа:
   8.1. Выберите в рабочем пространстве точку доступа Access Point0.
   8.2. В окне Access Point0 выберите вкладку Config и нажмите кнопку Port 0.
   8.3. Включите порт: установите галочку **On** в поле Port Status.
   8.4. Задайте автоматический выбор скорости передачи: установите галочку **Auto** в поле Bandwidth.
   8.5. Задайте автоматический выбор режима передачи: установите галочку **Auto** в поле Duplex.
   8.6. На вкладке Config нажмите кнопку Port 1.
   8.7. Включите порт: установите галочку **On** в поле Port Status.
   8.8. Задайте в поле SSID значение **Net01**.

8.9. Выберите в выпадающем списке Channel значение **6** для номера канала.
8.10. Отключите аутентификацию: установите переключатель Authentication в положение **Disabled**.
8.11. Отключите шифрование: установите в выпадающем списке Encryption Type значение **Disabled**. В результате окно Access Point0 должно приобрести вид, показанный на рисунке 10.3.
8.12. Закройте окно Access Point0.

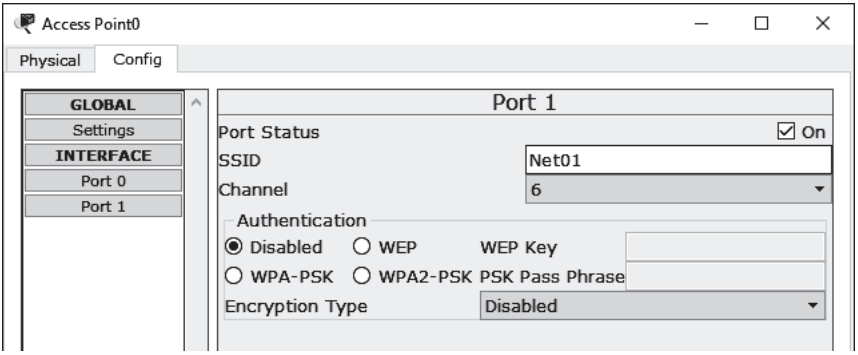

Рис. 10.3. Настройка точки доступа для работы без шифрования

9. Дождитесь появления штриховых соединительных линий, изображающих радиосигналы, между точкой доступа и компьютерами PC2 и PC3.
10. Переключите Cisco Packet Tracer в режим Simulation.
11. Проверьте проводные соединения — в пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1.
12. Проверьте беспроводные соединения — в пошаговом режиме передайте простой пакет с компьютера PC2 на компьютер PC3.
13. Проверьте взаимодействие проводной и беспроводной частей сети — в пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC3.
14. Переключите Cisco Packet Tracer в режим Realtime.
15. Перенастройте точку доступа, чтобы включить шифрование:
    15.1. Выберите в рабочем пространстве точку доступа Access Point0.
    15.2. В окне Access Point0 выберите вкладку Config и нажмите кнопку Port 1.
    15.3. Включите режим аутентификации WEP: установите переключатель Authentication в положение **WEP**.
    15.4. Задайте в поле Key ключ для аутентификации **0123456789**.
    15.5. Выберите в выпадающем списке Encryption Type значение **40/64-Bits(10 Hex digits)**. В результате окно Access Point0 должно приобрести вид, показанный на рисунке 10.4.
    15.6. Закройте окно Access Point0.

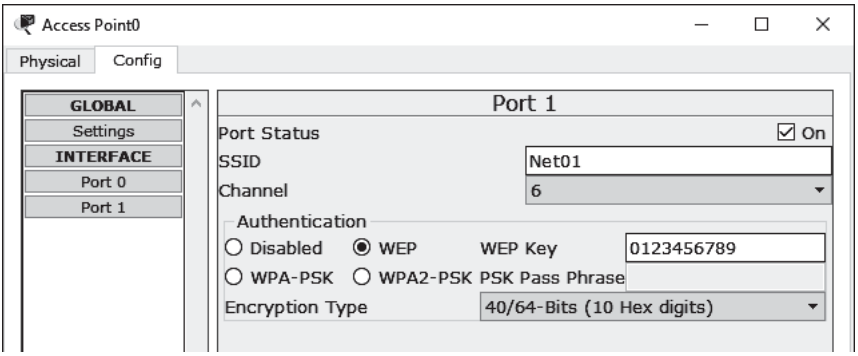

Рис. 10.4. Настройка точки доступа для работы в режиме WPA

16. Перенастройте компьютер PC2:
    16.1. Выберите в рабочем пространстве компьютер PC2.
    16.2. В окне PC2 выберите вкладку Config и нажмите кнопку Wireless.
    16.3. Включите режим аутентификации **WEP**.
    16.4. Задайте в поле Key ключ для аутентификации **0123456789**.
    16.5. Выберите в выпадающем списке Encryption Type значение **40/64-Bits(10 Hex digits)**.
    16.6. Закройте окно PC2.
17. Перенастройте компьютер PC3: включите режим аутентификации **WEP**, задайте ключ для аутентификации **0123456789**, задайте тип шифрования **40/64-Bits(10 Hex digits)**.
18. Переключите Cisco Packet Tracer в режим Simulation.
19. Проверьте беспроводные соединения — в пошаговом режиме передайте простой пакет с компьютера PC2 на компьютер PC3.
20. Проверьте взаимодействие проводной и беспроводной частей сети — в пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC3.
21. Сохраните модель сети в файле с именем **net_10_1_1**.
22. Завершите работу с программой Cisco Packet Tracer.

10.2. Настройка точки доступа, встроенной в маршрутизатор

Точка доступа Wi-Fi может быть встроена в маршрутизатор. Маршрутизатор с встроенной точкой доступа называют беспроводным маршрутизатором.

Маршрутизатор, предназначенный для использования в домашних условиях или в условиях малого офиса, кроме точки доступа обычно содержит четырехпортовый коммутатор Fast Ethernet и встроенный DHCP-сервер. С любой из подключенных к коммутатору рабочих станций можно выполнять настройку параметров маршрутизатора и точки доступа через Web-браузер, используя **графический интерфейс пользователя** (Graphics User Interface, сокращенно — **GUI**). Получить доступ к графическому интерфейсу пользователя можно по IP-адресу, заданному производителем устройства (обычно используется значение 192.168.0.1).

10.2.1. Беспроводная сеть с маршрутизатором и точкой доступа

В этом упражнении мы создадим и настроим беспроводную сеть с маршрутизатором и дополнительной точкой доступа, изображенную на рисунке 10.5.

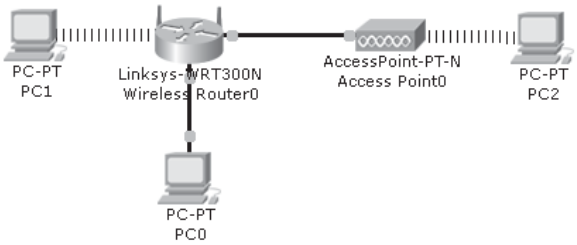

Рис. 10.5. Беспроводная сеть с маршрутизатором и точкой доступа

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. Поместите в рабочее пространство компьютер PC0 типа PC-PT.
   2.2. Поместите в рабочее пространство компьютеры PC1 и PC2 типа Wireless PC.
   2.3. Поместите в рабочее пространство точку доступа Access Point0 типа AccessPoint-PT-N.
   2.4. Поместите в рабочее пространство маршрутизатор Wireless Router0 типа Linksys-WRT300N.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Присоедините прямым кабелем компьютер PC0 к порту Ethernet 1 маршрутизатора Wireless Router0.
   3.2. Присоедините прямым кабелем порт Port 1 точки доступа Access Point0 к порту Ethernet 2 маршрутизатора Wireless Router0.
4. Настройте компьютер PC0: задайте режим конфигурирования IP-адреса через DHCP.
5. Настройте компьютер PC1: задайте SSID **Net01**, режим аутентификации **WEP**, ключ для аутентификации **0123456789**, тип шифрования Encryption Type **40/64-Bits(10 Hex digits)** и режим конфигурирования IP-адреса через DHCP.
6. Настройте компьютер PC2: задайте SSID **Net02**, режим аутентификации **WEP**, ключ для аутентификации **9876543210**, тип шифрования **40/64-Bits(10 Hex digits)** и режим конфигурирования IP-адреса через DHCP.
7. Настройте параметры точки доступа:
   7.1. Выберите в рабочем пространстве точку доступа Access Point0.
   7.2. В окне Access Point0 выберите вкладку Config и нажмите кнопку Port 1.
   7.3. Включите порт: установите галочку **On** в поле Port Status.
   7.4. Задайте в поле SSID значение **Net02**.
   7.5. Выберите в выпадающем списке Channel канал номер **1**.

7.6. Включите режим аутентификации **WEP**.
7.7. Задайте в поле Key ключ для аутентификации **9876543210**.
7.8. Выберите в выпадающем списке Encryption Type значение **40/64-Bits(10 Hex digits)**.
7.9. Закройте окно Access Point0.

8. Проведите настройку маршрутизатора с внешнего терминала:
8.1. Выберите в рабочем пространстве компьютер PC0.
8.2. В окне PC0 выберите вкладку Web Browser.
8.3. Введите в поле URL заданный по умолчанию производителем оборудования IP-адрес порта маршрутизатора **192.168.0.1** и нажмите кнопку Go.
8.4. Когда на экране появится окно авторизации доступа, введите в поле User Name значение **admin**, затем введите в поле Password значение **admin** (рис. 10.6), после чего нажмите кнопку OK. В окне Web Browser после выполнения этой операции должен появиться графический интерфейс пользователя, предназначенный для настройки параметров маршрутизатора.

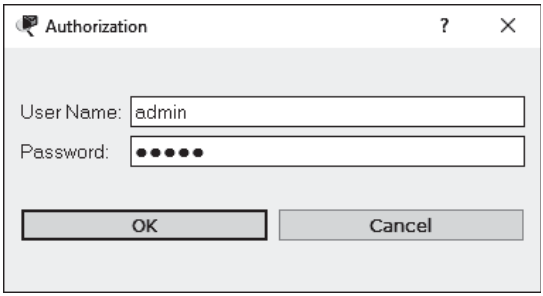

Рис. 10.6. Окно авторизации для доступа к графическому интерфейсу пользователя

8.5. Выберите в главном меню интерфейса пользователя пункт Setup. Просмотрите параметры DHCP (рис. 10.7) и оставьте их без изменения.

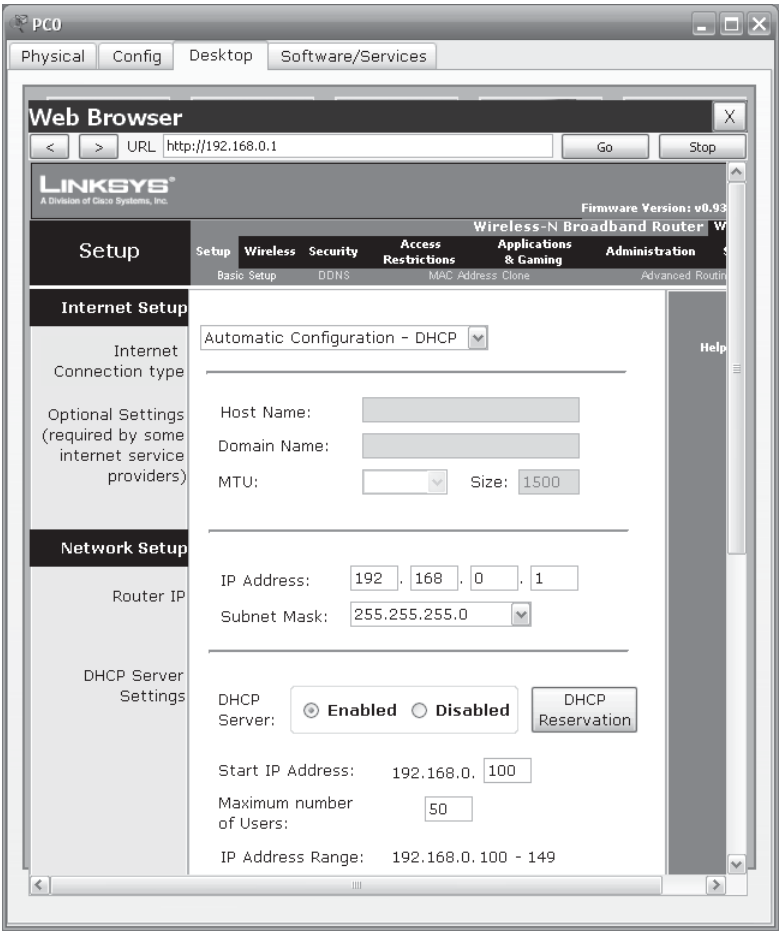

Рис. 10.7. Настройка параметров сетевого подключения и DHCP-сервера

8.6. Выберите в главном меню интерфейса пользователя пункт Wireless.
8.7. В выпадающем списке Network Mode выберите значение **Mixed**.
8.8. В поле Network Name (SSID) введите значение **Net01**.
8.9. В выпадающем списке Radio Band выберите значение **Auto**.
8.10. В выпадающем списке Wide Channel выберите значение **Auto**.
8.11. В выпадающем списке Standard Channel выберите канал номер **6**.
8.12. Переключатель SSID Broadcast установите в положение **Enabled** (рис. 10.8).
8.13. Нажмите кнопку Save Settings, расположенную в нижней части окна пользовательского интерфейса, чтобы сохранить в памяти маршрутизатора новые значения параметров беспроводного соединения.

8.14. Когда в окне Web Browser появится сообщение «Settings are successful», показывающее, что маршрутизатор начал использовать новые значения параметров, установите курсор мыши на слово Continue и щелкните левой кнопкой.
8.15. Закройте окно Web Browser.
8.16. Закройте окно PC0.

9. Дождитесь появления штриховых соединительных линий, изображающих радиосигналы, между маршрутизатором и компьютером PC1, а также между точкой доступа и компьютером PC2.
10. Поочередно наведите курсор мыши на каждый из компьютеров, дождитесь появления всплывающей подсказки и посмотрите, какие адреса присвоил компьютерам DHCP-сервер маршрутизатора.
11. Проверьте сетевые соединения: передайте простой пакет с компьютера PC0 на компьютер PC1, затем передайте пакет с компьютера PC0 на компьютер PC2, затем передайте пакет с компьютера PC1 на компьютер PC2.
12. Сохраните модель сети в файле с именем **net_10_2_1**.
13. Завершите работу с программой Cisco Packet Tracer.

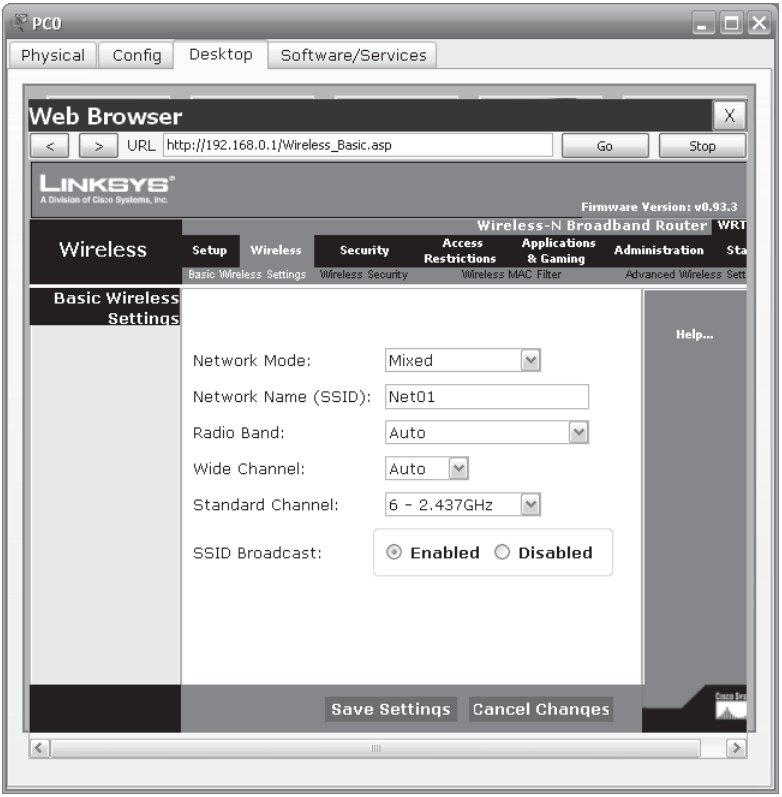

Рис. 10.8. Настройка параметров беспроводного соединения на маршрутизаторе

10.2.2. Настройка маршрутизатора по беспроводному соединению

В этом упражнении мы рассмотрим процесс настройки параметров маршрутизатора по беспроводному соединению, для чего создадим локальную сеть, изображенную на рисунке 10.9.

Рис. 10.9. Беспроводная сеть с маршрутизатором WRT300N

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочую область Cisco Packet Tracer:
   2.1. Поместите в рабочую область компьютеры PC0 и PC1 типа Wireless PC.
   2.2. Поместите в рабочую область маршрутизатор Router0 типа Linksys-WRT300N.
3. Дождитесь появления штриховых соединительных линий, изображающих радиосигналы, между маршрутизатором и компьютерами
4. Проверьте заданные по умолчанию значения параметров беспроводной связи компьютера PC0 (изменять эти значения на данном этапе настройки не нужно):
   4.1. Выберите в рабочем пространстве компьютер PC0.
   4.2. В окне PC0 выберите вкладку Config.
   4.3. Проверьте состояние переключателя Gateway/DNS — он должен находиться в положении **DHCP**.
   4.4. На вкладке Config нажмите кнопку Wireless.
   4.5. Проверьте состояние переключателя Authentication — он должен находиться в положении **Disabled** (аутентификация должна быть выключена).
   4.6. Проверьте состояние выпадающего списка Encryption Type — в списке должно быть выбрано значение **Disabled** (шифрование должно быть отключено).
   4.7. Проверьте состояние переключателя IP Configuration — он должен находиться в положении **DHCP**, чтобы персональный компьютер мог получать параметры сетевого соединения от DHCP-сервера.
   4.8. Проверьте значение полей IP Address и Subnet Mask — этих полях должны находиться IP-адрес и маска подсети, полученные от сервера DHCP.
5. Настройте параметры маршрутизатора Wireless Router0 с компьютера PC0 через браузер:
   5.1. В окне PC0 выберите вкладку Desktop.
   5.2. На вкладке Desktop нажмите кнопку Web Browser.
   5.3. В окне браузера наберите в поле URL адрес шлюза по умолчанию **192.168.0.1** и нажмите кнопку Go. В результате выполнения этой операции поверх окна браузера должно появиться окно Authorization, предназначенное для авторизации доступа к странице параметров маршрутизатора.

5.4. В окне Authorization введите в поле User Name значение **admin** и в поле Password — точно такое же значение **admin**, а затем нажмите кнопку OK. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница, предназначенная для настройки параметров маршрутизатора.
5.5. Измените на вкладке Setup IP-адрес маршрутизатора: введите в поле IP Address значение **192.168.5.1**, прокрутите страницу вниз и нажмите кнопку Save Settings, чтобы сохранить новые значения параметров. После того, как маршрутизатор примет новые параметры, в окне браузера появится сообщение «Request Timeout», указывающее, что время ожидания ответа на запрос истекло (так как адрес маршрутизатора был изменен, маршрутизатор не отвечает на запрос, который компьютер отправил по устаревшему адресу).
5.6. В окне браузера введите в поле URL новый адрес маршрутизатора **192.168.5.1** и нажмите кнопку Go. В результате выполнения этой операции поверх окна браузера должно появиться окно Authorization,.
5.7. В окне Authorization введите в поле User Name значение **admin**, в поле Password — значение **admin**, а затем нажмите кнопку OK.
5.8. Просмотрите страницу параметров маршрутизатора Basic Setup — изменение адреса маршрутизатора приводит к автоматическому изменению настроек DHCP-сервера.
5.9. Перейдите на вкладку Administration, в поле Router Password введите новый пароль **12345**, в поле Re-enter to Confirm введите тот же пароль **12345**, прокрутите страницу вниз и нажмите кнопку Save Settings, чтобы сохранить новые значения параметров.
5.10. Когда в окне Web Browser появится сообщение «Settings are successful», показывающее, что маршрутизатор начал использовать новые значения параметров, установите курсор мыши на слово Continue и щелкните левой кнопкой. В результате выполнения этой операции поверх окна браузера должно появиться окно Authorization.
5.11. В окне Authorization введите в поле User Name значение **admin**, в поле Password — значение **12345**, а затем нажмите кнопку OK.
5.12. В окне параметров маршрутизатора выберите вкладку Wireless.
5.13. В поле Network Name (SSID) введите значение **NET01**, чтобы присвоить идентификатор беспроводной сети.
5.14. Прокрутите вниз страницу параметров беспроводной сети и нажмите кнопку Save Settings, чтобы сохранить новые значения параметров. После того, как маршрутизатор примет новые параметры, в окне браузера появится сообщение Request Timeout, указывающее, что время ожидания ответа на запрос истекло (так как настройки параметров беспроводной сети маршрутизатора и компьютера перестали соответствовать между собой, маршрутизатор не может ответить на запрос компьютера).
5.15. Закройте окно Web Browser.
5.16. На вкладке Desktop нажмите кнопку PC Wireless, после чего на экране появится окно, предназначенное для настройки параметров беспроводного соединения.
5.17. В окне параметров беспроводного соединения проверьте состояние индикаторов Signal Strength и Link Quality на вкладке Link Information — эти индикаторы должны показать отсутствие сигнала.
5.18. В окне параметров беспроводного соединения перейдите на вкладку Connect, выберите в списке беспроводных сетей сеть **NET01** и нажмите кнопку Connect.

5.19. В окне параметров беспроводного соединения перейдите на вкладку Link Information и проверьте состояние индикаторов Signal Strength и Link Quality — эти индикаторы должны показать высокую интенсивность сигнала и высокое качество приема сигнала.
5.20. Закройте окно параметров беспроводного соединения.
5.21. На вкладке Desktop нажмите кнопку Web Browser.
5.22. В окне браузера наберите в поле URL адрес **192.168.5.1** и нажмите кнопку Go. В результате выполнения этой операции поверх окна браузера должно появиться окно Authorization.
5.23. В окне Authorization введите в поле User Name значение **admin**, в поле Password — значение **12345**, а затем нажмите кнопку OK.
5.24. В окне параметров маршрутизатора выберите вкладку Wireless.
5.25. На вкладке Wireless выберите вкладку Wireless Security.
5.26. В выпадающем списке Security Mode выберите значение **WEP**.
5.27. Задайте в поле Key ключ для аутентификации **0123456789**.
5.28. Выберите в выпадающем списке Encryption Type значение **40/64-Bits(10 Hex digits)**.
5.29. Прокрутите вниз страницу параметров беспроводной сети и нажмите кнопку Save Settings, чтобы сохранить новые значения параметров. После того, как маршрутизатор примет новые параметры, в окне браузера появится сообщение «Request Timeout».
5.30. Закройте окно Web Browser.
5.31. На вкладке Desktop нажмите кнопку PC Wireless, после чего на экране появится окно, предназначенное для настройки параметров беспроводного соединения.
5.32. В окне параметров беспроводного соединения перейдите на вкладку Connect, выберите в списке беспроводных сетей сеть **NET01** и нажмите кнопку Connect. После этого на экране появится новое окно WEP Key Needed For Connection, содержащее запрос на ввод ключа WEP.
5.33. В поле WEP Key 1 введите ключ для аутентификации **0123456789** и нажмите кнопку Connect.
5.34. В окне параметров беспроводного соединения перейдите на вкладку Link Information и проверьте состояние индикаторов Signal Strength и Link Quality — эти индикаторы должны показать высокую интенсивность сигнала и высокое качество приема сигнала.
5.35. Закройте окно параметров беспроводного соединения.
5.36. На вкладке Desktop нажмите кнопку Web Browser.
5.37. В окне браузера наберите в поле URL адрес **192.168.5.1** и нажмите кнопку Go. В результате выполнения этой операции поверх окна браузера должно появиться окно Authorization.
5.38. В окне Authorization введите в поле User Name значение **admin**, в поле Password — значение **12345**, а затем нажмите кнопку OK. В результате выполнения этой операции в окне браузера должна отобразиться страница, предназначенная для настройки параметров маршрутизатора.
5.39. Закройте окно Web Browser.
5.40. Закройте окно PC0.

6. Настройте компьютер PC1:
6.1. Выберите в рабочем пространстве компьютер PC1.

6.2. В окне PC1 выберите вкладку Desktop и нажмите кнопку PC Wireless, после чего на экране появится окно, предназначенное для настройки параметров беспроводного соединения.
6.3. В окне параметров беспроводного соединения перейдите на вкладку Connect, выберите в списке беспроводных сетей сеть **NET01** и нажмите кнопку Connect. После этого на экране появится новое окно WEP Key Needed For Connection, содержащее запрос на ввод ключа WEP.
6.4. В поле WEP Key 1 введите ключ для аутентификации **0123456789** и нажмите кнопку Connect.
6.5. В окне параметров беспроводного соединения перейдите на вкладку Link Information и проверьте состояние индикаторов Signal Strength и Link Quality — эти индикаторы должны показать высокую интенсивность сигнала и высокое качество приема сигнала.
6.6. Закройте окно параметров беспроводного соединения.
6.7. Закройте окно PC1.
7. Проверьте беспроводные соединения — в пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1.
8. Сохраните модель сети в файле с именем **net_10_2_2**.
9. Завершите работу с программой Cisco Packet Tracer.
10. Как вы могли убедиться на данном примере, настройка через беспроводное соединение — трудоемкий процесс, поэтому обычно для настройки используют проводное подключение.

10.3. Задание для самостоятельной работы

Создайте и настройте модель, состоящую из четырех компьютеров, беспроводного маршрутизатора и точки доступа (рисунок 10.10).

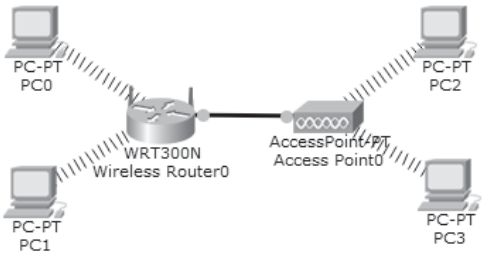

Рис. 10.10. Сеть, состоящая из четырех компьютеров, беспроводного маршрутизатора и точки доступа

11. ТЕХНОЛОГИЯ FRAME RELAY

Технология Frame Relay была разработана в 90-х годах прошлого века для замены технологии X.25.

Сети Frame Relay специально разрабатывались как общественные сети для соединения частных локальных сетей. В настоящее время служба коммутации пакетов Frame Relay широко распространена во всём мире.

11.1. Протокол Frame Relay

Протокол Frame Relay использует метод коммутации пакетов.

Основные преимущества сетей Frame Relay заключаются в их низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежную передачу кадров технология Frame Relay не обеспечивает.

Стандарты Frame Relay определяют два типа виртуальных каналов — постоянные (**PVC**) и коммутируемые (**SVC**). Для соединений, по которым трафик передается постоянно, используют PVC, а для соединений, которые нужны только изредка (на несколько часов в месяц), применяют SVC.

Технология Frame Relay использует адреса, называемые **идентификаторами канала соединения** (data link connection identifiers — **DLCI**). В сети Frame Relay каждый идентификатор DLCI может иметь локальное или глобальное значение, но обычно применяются идентификаторы с локальным значением. Это означает, что маршрутизаторы на разных сторонах виртуального канала в сети Frame Relay могут иметь один и тот же DLCI-номер, поскольку протокол Frame Relay предусматривает отображение локального DLCI-номера на виртуальный канал на каждом из коммутаторов, стоящих в глобальной сети.

Первоначально протокол Frame Relay был разработан для применения в цифровых сетях с интегрированными службами ISDN. В 1990 году компании Cisco, DEC, Northern Telecom и StrataCom образовали консорциум Frame Relay Forum, целью которого было развитие технологии Frame Relay. Эта группа добавила к протоколу Frame Relay расширения, позволяющие устройствам межсетевого взаимодействия обмениваться данными. Эти расширения, называемые **интерфейсом локального управления** (Local Management Interface — **LMI**), позволяют DTE-устройствам сети общаться с DCE-устройствами и производить обмен служебной информацией. Сообщения LMI предоставляют информацию о статусе виртуальных каналов, текущих значениях DLCI и их характере .

Поле номера виртуального соединения DLCI состоит из десяти битов, что позволяет использовать до 1024 виртуальных соединений. Адреса DLCI распределяются между пользователями и сетью следующим образом:

- адрес 0 используется для виртуального канала локального управления LMI;
- адреса в диапазоне от 0 до 15 зарезервированы для дальнейшего использования;
- адреса в диапазоне от 16 до 991 используются абонентами для нумерации PVC и SVC;
- адреса в диапазоне от 992 до 1007 используются сетевой транспортной службой для внутрисетевых соединений;

- адреса в диапазоне от 1008 до 1022 зарезервированы для дальнейшего использования;
- адрес 1023 используется для управления канальным уровнем.

11.2. Настройки интерфейса на работу с каналом Frame Relay

Для того чтобы сконфигурировать интерфейс последовательной передачи данных маршрутизатора Cisco на работу с протоколом Frame Relay, следует ввести команду конфигурирования **encapsulation frame-relay** (сокращенно — **en fr**), которая задает для интерфейса тип инкапсуляции Frame Relay.

После этого нужно присвоить последовательному интерфейсу значение идентификатора DLCI с помощью команды **frame-relay interface-dlci** (сокращенно — **fr in**), которая имеет следующий формат:

```
frame-relay interface-dlci dlci
```

где *dlci* — значение идентификатора dlci.

Устройства Cisco по умолчанию используют на интерфейсах Frame Relay интерфейс Cisco LMI, однако при необходимости с помощью команды конфигурирования интерфейса **framerelay lmi-type** можно явно установить тип интерфейса LMI.

После завершения конфигурирования желательно проверить правильность настройки интерфейса:

- статус интерфейса Frame Relay можно узнать с помощью команды **show interfaces** (сокращенно — **sh in**);
- состояние виртуальных каналов Frame Relay можно проверить, воспользовавшись командой **show frame pvc** (сокращенно — **sh fr pvc**);
- для получения данных о коммутируемых виртуальных каналах можно воспользоваться командой **show frame svc maplist** (опция maplist позволяет получить список соединений между данным устройством и другими устройствами, используемыми при установке коммутируемых виртуальных каналов).

11.3. Облако Cloud-PT

Символ облака обычно используется в литературе для изображения Internet-соединений. В программе Cisco Packet Tracer для создания соединений Frame Relay применяется облако типа Cloud-PT.

Для соединения облака с маршрутизаторами должно использоваться соединение Serial DCE. Так как за синхронизацию передачи данных должно отвечать облако Cloud-PT, то в первую очередь кабель должен быть подключен к облаку (та сторона кабеля, на которой изображены часы), а затем — к маршрутизатору.

Каждому используемому порту облака должно быть присвоено имя и номер DLCI. Необходимо также указать тип интерфейса управления LMI.

После того, как имена присвоены всем используемым портам, требуется создать связи между портами.

11.3.1. Соединение двух сетей каналом Frame Relay

Процесс настройки маршрутизаторов для работы с каналами Frame Relay мы начнем рассматривать с самого простого примера — соединения двух сетей, изображенного на рисунке 11.1.

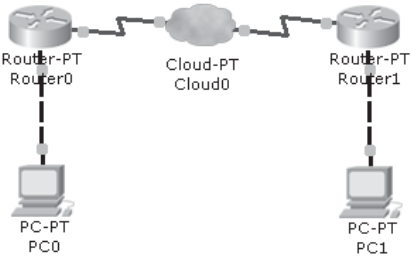

Рис. 11.1. Соединение двух сетей каналом Frame Relay

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. В группе Routers выберите абстрактную модель маршрутизатора Router-PT и поместите в рабочее пространство маршрутизаторы Router0 и Router1.
   2.2. В группе WAN Emulation выберите модель интернет-соединения Cloud-PT и поместите в рабочее пространство облако Cloud0.
   2.3. Поместите в рабочее пространство компьютеры PC0 и PC1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet0/0 маршрутизатора Router1.
   3.3. В группе Connections выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial0 облака Cloud0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router0.
   3.4. Снова выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial1 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1**, маску **255.255.255.0** и адрес шлюза **192.168.1.254**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0** и адрес шлюза **192.168.2.254**.
6. Настройте параметры облака:
   6.1. Выберите в рабочем пространстве облако Cloud0.
   6.2. В окне Cloud0 выберите вкладку Config.
   6.3. На вкладке Config нажмите кнопку Serial0.
   6.4. Включите порт Serial0: установите галочку On в поле Port Status.
   6.5. В выпадающем списке LMI выберите значение **Cisco**.

6.6. В поле DLCI введите значение **101**, в поле Name введите значение **S0toS1** и нажмите кнопку Add, после чего в таблице DLCI должна появиться строка с записью «101 S0toS1», а окно настройки последовательного порта должно приобрести вид, показанный на рисунке 11.2.

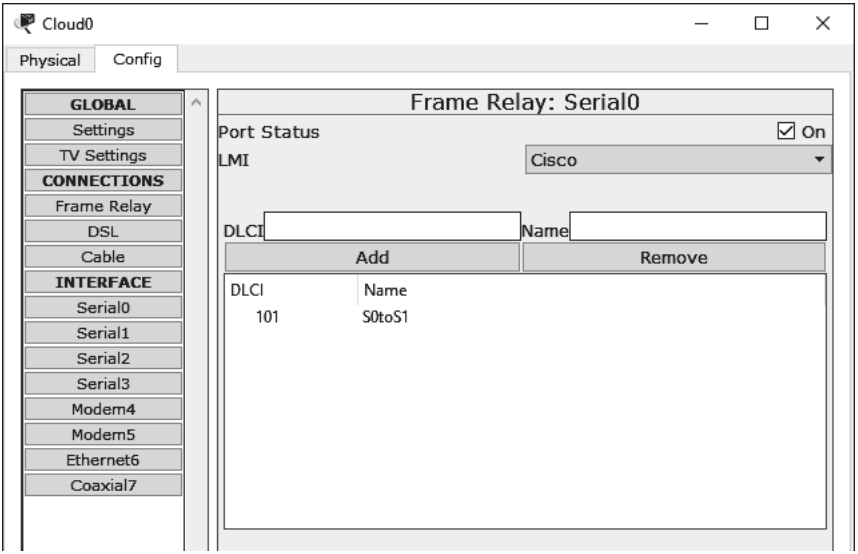

Рис. 11.2. Настройка последовательного порта облака Serial0

6.7. На вкладке Config нажмите кнопку Serial1.
6.8. Включите порт Serial1: установите галочку On в поле Port Status.
6.9. В выпадающем списке LMI выберите значение **Cisco**.
6.10. В поле DLCI введите значение **102**, в поле Name введите значение **S1toS0** и нажмите кнопку Add, после чего в таблице DLCI должна появиться строка с записью «102 S1toS0».
6.11. На вкладке Config нажмите кнопку Frame Relay.
6.12. В расположенном слева выпадающем списке Port выберите значение **Serial0**; в расположенном слева выпадающем списке Sublink выберите значение **S0toS1**; в расположенном справа выпадающем списке Port выберите значение **Serial1**; в расположенном справа выпадающем списке Sublink выберите значение **S1toS0**.
6.13. Нажмите кнопку Add, после чего окно настройки соединения должно приобрести вид, показанный на рисунке 11.3.
6.14. Закройте окно Cloud0.

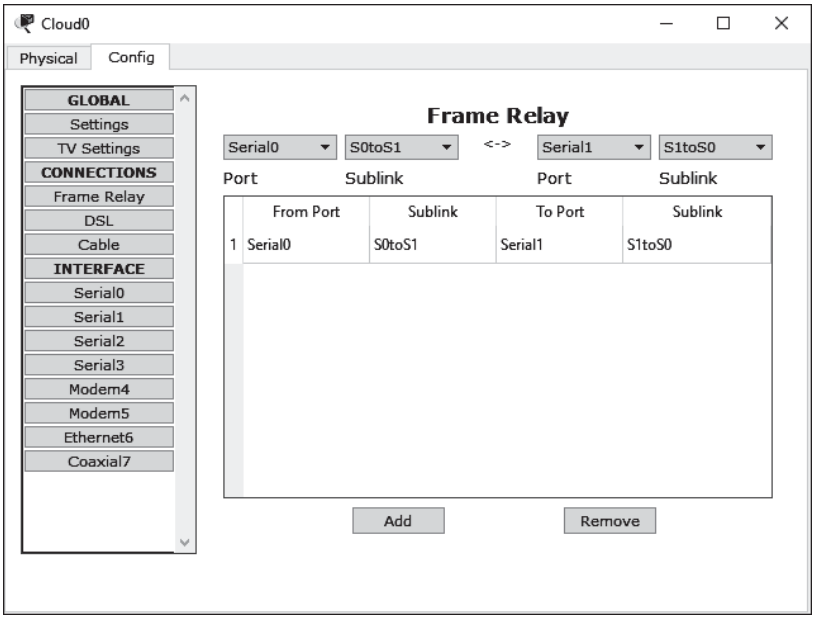

Рис. 11.3. Настройка канала

7. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#ip ad 192.168.3.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.3.0
Router(config-router)#exit
Router(config)#exit
```

8. Проверьте настройку маршрутизатора Router0, для чего введите на вкладке CLI последовательность команд:

```
Router#show interfaces
Router#show frame pvc
Router#exit
```

9. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.3.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.3.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

10. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0. Если в одной из таблиц отсутствует какая-либо сеть — немного подождите.
11. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
12. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
13. Переключите Cisco Packet Tracer в режим Simulation.
14. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC1. После выполнения каждого шага просматривайте передаваемый пакет, чтобы видеть, какие изменения будут происходить в заголовках различных уровней.
15. Переключите Cisco Packet Tracer в режим Realtime.
16. Протестируйте соединение между компьютерами с помощью диагностических утилит из стека протоколов TCP/IP:
    16.1. Выберите в рабочем пространстве компьютер PC0.
    16.2. В окне PC0 выберите вкладку Desktop.
    16.3. На вкладке Desktop нажмите кнопку Command Prompt, чтобы открыть окно, имитирующее работу операционной системы компьютера в режиме командной строки.
    16.4. Введите команду **ping 192.168.2.1** и просмотрите результат ее выполнения.
    16.5. Введите команду **tracert 192.168.2.1** и просмотрите результат ее выполнения.
    16.6. Закройте окно Command Prompt.
    16.7. Закройте окно PC0.
17. Сохраните модель сети в файле с именем **net_11_3_1**.
18. Завершите работу с программой Cisco Packet Tracer.

11.4. Особенности использования общего IP-интерфейса

Простейший способ настройки соединения по протоколу Frame Relay заключается в использовании общего IP-интерфейса, когда все маршрутизаторы связаны в одну общую сеть. В этом случае можно использовать либо полносвязную топологию (рис. 11.4а), когда каждый маршрутизатор имеет соединение с каждым, либо топологию «звезда» (рис. 11.4б), когда имеется один центральный маршрутизатор-хаб, к которому подключены маршрутизаторы-лучи.

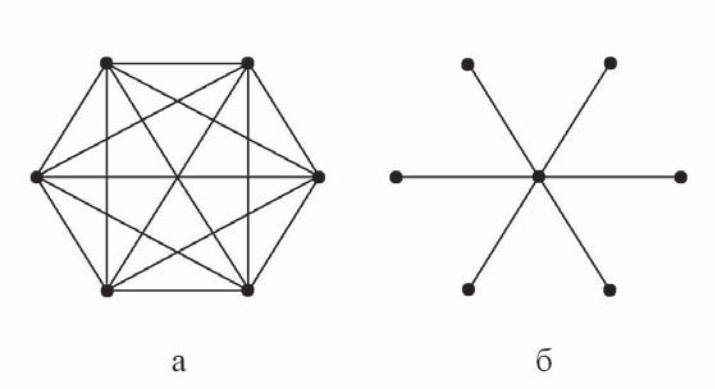

Рис. 11.4. Полносвязная топология (а) и топология «звезда» (б)

За каждое виртуальное соединение пользователи сети должны платить провайдеру. Недостаток полносвязной топологии заключается в том, что для объединения в сеть N маршрутизаторов требуется N(N-1)/2 соединений (имеет место квадратичная зависимость), тогда как при использовании топологии «звезда» требуется только N-1 соединений (линейная зависимость).

Основным недостатком топологии «звезда» при использовании общего IP-интерфейса является отсутствие связи между маршрутизатори-лучами: они видят только центральный маршрутизатор, но не видят друг друга.

11.4.1. Моделирование сети, использующей полносвязную топологию

В этом упражнении мы будем использовать полносвязную топологию для объединения трех сетей друг с другом с помощью технологии Frame Relay. Все маршрутизаторы будут связаны друг с другом виртуальными каналами через «облако», изображающее сеть Frame Relay (рис. 11.5).

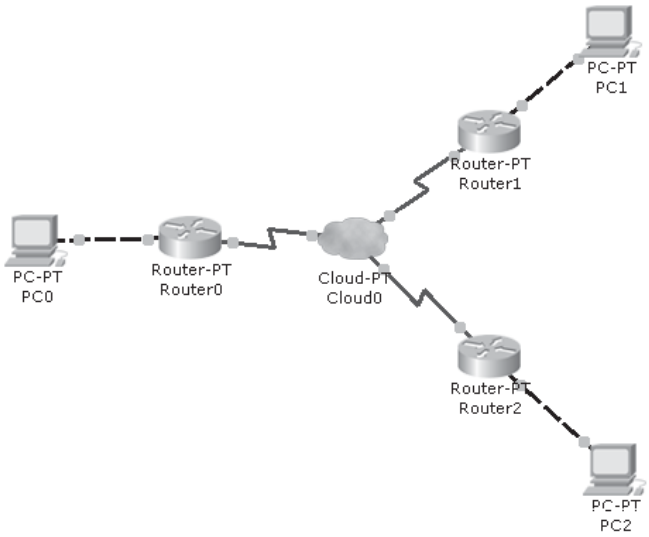

Рис. 11.5. Модель сети, использующей полносвязную топологию

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. В группе WAN Emulation выберите модель интернет-соединения Cloud-PT и поместите в рабочее пространство облако Cloud0.
   2.2. В группе Routers выберите абстрактную модель маршрутизатора Router-PT и поместите в рабочее пространство маршрутизаторы Router0, Router1 и Router2.
   2.3. Поместите в рабочее пространство компьютеры PC0, PC1 и PC2.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet0/0 маршрутизатора Router1.
   3.3. Подключите перекрестным кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/0 маршрутизатора Router2.
   3.4. В группе Connections выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial0 облака Cloud0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router0.
   3.5. Выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial1 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router1.
   3.6. Выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial2 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router2.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.1**, маску **255.255.255.0** и адрес шлюза **192.168.1.254**.

5. Настройте компьютер PC1: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0** и адрес шлюза **192.168.2.254**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.3.1**, маску **255.255.255.0** и адрес шлюза **192.168.3.254**.
7. Настройте параметры облака:
   7.1. Выберите в рабочем пространстве облако Cloud0.
   7.2. В окне Cloud0 выберите вкладку Config.
   7.3. На вкладке Config нажмите кнопку Serial0.
   7.4. Включите порт Serial0: установите галочку On в поле Port Status.
   7.5. В выпадающем списке LMI выберите значение **Cisco**.
   7.6. В поле DLCI введите значение **102**, в поле Name введите значение **S0toS1** и нажмите кнопку Add.
   7.7. В поле DLCI введите значение **103**, в поле Name введите значение **S0toS2** и нажмите кнопку Add.
   7.8. На вкладке Config нажмите кнопку Serial1.
   7.9. Включите порт Serial1.
   7.10. В выпадающем списке LMI выберите значение **Cisco**.
   7.11. В поле DLCI введите значение **201**, в поле Name введите значение **S1toS0** и нажмите кнопку Add.
   7.12. В поле DLCI введите значение **203**, в поле Name введите значение **S1toS2** и нажмите кнопку Add.
   7.13. На вкладке Config нажмите кнопку Serial2.
   7.14. Включите порт Serial2.
   7.15. В выпадающем списке LMI выберите значение Cisco.
   7.16. В поле DLCI введите значение **301**, в поле Name введите значение S2toS0 и нажмите кнопку Add.
   7.17. В поле DLCI введите значение **302**, в поле Name введите значение S2toS1 и нажмите кнопку Add.
   7.18. На вкладке Config нажмите кнопку Frame Relay.
   7.19. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS1**, в расположенном справа выпадающем списке Port выберите значение **Serial1**, в расположенном справа выпадающем списке Sublink выберите значение **S1toS0** и нажмите кнопку Add.
   7.20. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS2**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S2toS0** и нажмите кнопку Add.
   7.21. В расположенном слева выпадающем списке Port выберите значение **Serial1**, в расположенном слева выпадающем списке Sublink выберите значение **S1toS2**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S2toS1** и нажмите кнопку Add.
   7.22. Закройте окно Cloud0.

8. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.4.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.4.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

9. Настройте маршрутизатор Router1, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.4.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.4.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

10. Настройте маршрутизатор Router2, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.3.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.4.3 255.255.255.0
Router(config-if)#no shut
```

```
Router(config-if)#ro rip
Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.4.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

11. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: во всех таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0, 192.168.3.0 и 192.168.4.0. Если в одной из таблиц отсутствует какая-либо сеть, то немного подождите: примерно через минуту после завершения конфигурирования последнего маршрутизатора все таблицы должны быть построены.
12. Проверьте соединения между компьютерами:
    12.1. Передайте простой пакет с компьютера PC0 на компьютер PC1, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
    12.2. Передайте простой пакет с компьютера PC1 на компьютер PC2.
    12.3. Передайте простой пакет с компьютера PC2 на компьютер PC0.
13. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
14. Переключите Cisco Packet Tracer в режим Simulation.
15. В пошаговом режиме передайте простой пакет с компьютера с PC0 на компьютер PC1. После выполнения каждого шага просматривайте передаваемый пакет, чтобы видеть, какие изменения будут происходить в заголовках различных уровней.
16. Переключите Cisco Packet Tracer в режим Realtime.
17. Протестируйте соединение между компьютерами PC0 и PC1 с помощью диагностических утилит из стека протоколов TCP/IP:
    17.1. Выберите в рабочем пространстве компьютер PC0.
    17.2. В окне PC0 выберите вкладку Desktop.
    17.3. На вкладке Desktop нажмите кнопку Command Prompt, чтобы открыть окно, имитирующее работу операционной системы компьютера в режиме командной строки.
    17.4. Введите команду **ping 192.168.2.1** и просмотрите результат ее выполнения.
    17.5. Введите команду **tracert 192.168.2.1** и просмотрите результат ее выполнения.
    17.6. Закройте окно Command Prompt.
    17.7. Закройте окно PC0.
18. Сохраните модель сети в файле с именем **net_11_4_1**.
19. Завершите работу с программой Cisco Packet Tracer.

11.4.2. Моделирование сети, использующей звездообразную топологию

В этом упражнении мы будем использовать звездообразную топологию для объединения четырех сетей друг с другом с помощью технологии Frame Relay (рис. 11.6).

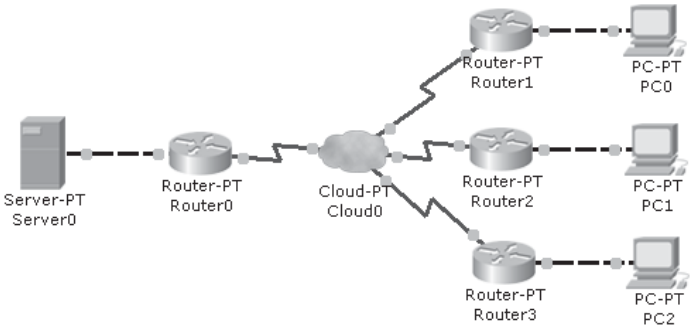

Рис. 11.6. Модель сети, использующей звездообразную топологию

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите устройства, которые необходимо объединить в сеть, в рабочее пространство Cisco Packet Tracer:
   2.1. В группе WAN Emulation выберите модель интернет-соединения Cloud-PT и поместите в рабочее пространство облако Cloud0.
   2.2. В группе Routers выберите абстрактную модель маршрутизатора Router-PT и поместите в рабочее пространство маршрутизаторы Router0, Router1, Router2 и Router3.
   2.3. Поместите в рабочее пространство сервер Server0.
   2.4. Поместите в рабочее пространство компьютеры PC0, PC1 и PC2.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Подключите перекрестным кабелем порт FastEthernet сервера Server0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.2. Подключите перекрестным кабелем порт FastEthernet компьютера PC0 к порту FastEthernet0/0 маршрутизатора Router1.
   3.3. Подключите перекрестным кабелем порт FastEthernet компьютера PC1 к порту FastEthernet0/0 маршрутизатора Router2.
   3.4. Подключите перекрестным кабелем порт FastEthernet компьютера PC2 к порту FastEthernet0/0 маршрутизатора Router3.
   3.5. В группе Connections выберите пиктограмму Serial DCE, соответствующую разъему кабеля на ведущем устройстве последовательного канала, и подключите этот конец кабеля к порту Serial0 облака Cloud0, а затем подключите противоположный конец кабеля к порту Serial2/0 маршрутизатора Router0.
   3.6. Выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial1 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router1.
   3.7. Выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial2 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router2.
   3.8. Выберите пиктограмму Serial DCE и подключите кабель сначала к порту Serial2 облака Cloud0, а затем — к порту Serial2/0 маршрутизатора Router3.
4. Настройте сервер:
   4.1. Выберите в рабочем пространстве сервер Server0.
   4.2. В окне Server0 выберите вкладку Config.

4.3. В области настройки глобальных параметров Global Settings задайте статический режим настройки шлюза и введите адрес шлюза **192.168.1.254**.
4.4. На вкладке Config нажмите кнопку FastEthernet.
4.5. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.1.1** и маску **255.255.255.0**.
4.6. В окне Server0 выберите вкладку Services.
4.7. На вкладке Services нажмите кнопку HTTP.
4.8. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
4.9. На вкладке Conf Services ig нажмите кнопку DNS.
4.10. В области настройки параметров DNS установите переключатель DNS Service в положение **On**, для того чтобы включить поддержку сервиса DNS.
4.11. В поле Name задайте для сервера имя **serv0.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.1.1**, после чего нажмите кнопку Add.
4.12. Закройте окно Server0.
5. Настройте компьютер PC0: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**, адрес шлюза 192.168.2.254 и адрес сервера DNS **192.168.1.1**.
6. Настройте компьютер PC1: задайте IP-адрес **192.168.3.1**, маску **255.255.255.0**, адрес шлюза 192.168.3.254 и адрес сервера DNS **192.168.1.1**.
7. Настройте компьютер PC2: задайте IP-адрес **192.168.4.1**, маску **255.255.255.0**, адрес шлюза 192.168.4.254 и адрес сервера DNS **192.168.1.1**.
8. Настройте облако:
8.1. Выберите в рабочем пространстве облако Cloud0.
8.2. В окне Cloud0 выберите вкладку Config.
8.3. На вкладке Config нажмите кнопку Serial0.
8.4. Включите порт Serial0.
8.5. В выпадающем списке LMI выберите значение **Cisco**.
8.6. В поле DLCI введите значение **102**, в поле Name введите значение **S0toS1** и нажмите кнопку Add.
8.7. В поле DLCI введите значение **103**, в поле Name введите значение **S0toS2** и нажмите кнопку Add.
8.8. В поле DLCI введите значение **104**, в поле Name введите значение **S0toS3** и нажмите кнопку Add.
8.9. На вкладке Config нажмите кнопку Serial1.
8.10. Включите порт Serial1.
8.11. В выпадающем списке LMI выберите значение Cisco.
8.12. В поле DLCI введите значение **201**, в поле Name введите значение **S1toS0** и нажмите кнопку Add.
8.13. На вкладке Config нажмите кнопку Serial2.
8.14. Включите порт Serial2.
8.15. В выпадающем списке LMI выберите значение Cisco.
8.16. В поле DLCI введите значение **301**, в поле Name введите значение **S2toS0** и нажмите кнопку Add.
8.17. На вкладке Config нажмите кнопку Serial3.
8.18. Включите порт Serial3.
8.19. В выпадающем списке LMI выберите значение Cisco.
8.20. В поле DLCI введите значение **401**, в поле Name введите значение **S3toS0** и нажмите кнопку Add.
8.21. На вкладке Config нажмите кнопку Frame Relay.

8.22. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS1**, в расположенном справа выпадающем списке Port выберите значение **Serial1**, в расположенном справа выпадающем списке Sublink выберите значение **S1toS0** и нажмите кнопку Add.

8.23. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS2**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S2toS0** и нажмите кнопку Add.

8.24. В расположенном слева выпадающем списке Port выберите значение **Serial1**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS3**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S3toS0** и нажмите кнопку Add.

9. Настройте маршрутизатор Router0, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.5.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

10. Настройте маршрутизатор Router1, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.5.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
```

```
Router#exit
```

11. Настройте маршрутизатор Router2, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.3.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.5.3 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

12. Настройте маршрутизатор Router3, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.4.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#ip ad 192.168.5.4 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ro rip
Router(config-router)#net 192.168.4.0
Router(config-router)#net 192.168.5.0
Router(config-router)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

13. На правой панели инструментов нажмите кнопку Inspect и проверьте таблицы маршрутизации:
    13.1. В таблице маршрутизатора Router0 должны присутствовать сети 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 и 192.168.5.0. Если в таблице отсутствует какая-либо сеть, то немного подождите.
    13.2. В таблице маршрутизатора Router1 должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.5.0.
    13.3. В таблице маршрутизатора Router2 должны присутствовать сети 192.168.1.0, 192.168.3.0 и 192.168.5.0.
    13.4. В таблице маршрутизатора Router3 должны присутствовать сети 192.168.1.0, 192.168.4.0 и 192.168.5.0.

14. Проверьте наличие связи между компьютерами и сервером:
    14.1. Передайте простой пакет с компьютера PC0 на сервер Server0, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
    14.2. Передайте простой пакет с компьютера PC1 на сервер Server0.
    14.3. Передайте простой пакет с компьютера PC2 на сервер Server0.
15. Попробуйте предать простой пакет с компьютера PC0 на компьютер PC2: пакет передаваться не должен, так каналы Frame Relay настроены таким образом, что маршрутизаторы Router1, Router2 и Router3 видят маршрутизатор Router0, но не видят друг друга.
16. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
17. Переключите Cisco Packet Tracer в режим Simulation.
18. В пошаговом режиме передайте простой пакет с компьютера с PC0 на сервер Server0. После выполнения каждого шага просматривайте передаваемый пакет, чтобы видеть, какие изменения будут происходить в заголовках различных уровней.
19. Переключите Cisco Packet Tracer в режим Realtime.
20. Выберите в рабочем пространстве компьютер PC0.
21. Протестируйте соединение между компьютером PC0 и сервером с помощью диагностических утилит из стека протоколов TCP/IP:
    21.1. В окне PC0 выберите вкладку Desktop.
    21.2. На вкладке Desktop нажмите кнопку Command Prompt.
    21.3. Введите команду **ping 192.168.1.1** и просмотрите результат ее выполнения.
    21.4. Введите команду **tracert 192.168.1.1** и просмотрите результат ее выполнения.
    21.5. Закройте окно Command Prompt.
22. Проверьте наличие доступа к информации, размещенной на сервере:
    22.1. На вкладке Desktop нажмите кнопку Web Browser.
    22.2. В окне браузера наберите в поле URL адрес **serv0.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server0.
    22.3. Закройте окно Web Browser.
    22.4. Закройте окно PC0.
23. Сохраните модель сети в файле с именем **net_11_4_2**.
24. Завершите работу с программой Cisco Packet Tracer.

11.5. Использование подинтерфейсов

Как мы видели из результатов предыдущего упражнения, основным недостатком топологии «звезда» при использовании общего IP-интерфейса является отсутствие связи между маршрутизаторами-лучами: они видят центральный маршрутизатор, но не видят друг друга. Чтобы обеспечить полноценную связь между всеми сегментами сети, вместо общего IP-интерфейса необходимо использовать отдельные подинтерфейсы для каждого луча. Кроме того, в таблицах маршрутизации маршрутизатор необходимо прописать статические маршруты к лучам

Для задания виртуального интерфейса последовательного канала используется команда **interface serial** (сокращенно — **int se**), которая имеет следующий формат:

```
interface serial slot/port.number
```

где *slot* — номер слота, *port* — номер порта, number — номер подинтерфейса.

При создании подинтерфейсов рекомендуется разработать некоторую схему для их нумерации и твердо ее придерживаться: например, можно присваивать подинтерфейсу номер в соответствии с номером DLCI виртуального канала.

11.5.1. Создание подинтерфейсов на интерфейсах, подключенных к каналам Frame Relay

В этом упражнении мы будем использовать ту же звездообразную топологию сети, что и в предыдущем (рис. 11.6), но изменим настройку маршрутизаторов — создадим подинтерфейсы на интерфейсах, подключенных к каналам Frame Relay, а вместо динамической маршрутизации будем использовать статические маршруты.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Схему, показанную на рисунке 11.6, соберите заново точно таким же образом, как в предыдущем упражнении.
3. Настройте сервер:
   - 3.1. Выберите в рабочем пространстве сервер Server0.
   - 3.2. В окне Server0 выберите вкладку Config.
   - 3.3. В области настройки глобальных параметров Global Settings задайте статический режим настройки шлюза и введите адрес шлюза **192.168.1.254**.
   - 3.4. На вкладке Config нажмите кнопку FastEthernet.
   - 3.5. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.1.1** и маску **255.255.255.0**.
   - 3.6. В окне Server0 выберите вкладку Services.
   - 3.7. На вкладке Services нажмите кнопку HTTP.
   - 3.8. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
   - 3.9. На вкладке Services нажмите кнопку DNS.
   - 3.10. В области настройки параметров DNS установите переключатель DNS Service в положение **On**, для того чтобы включить поддержку сервиса DNS.
   - 3.11. В поле Name задайте для сервера имя **serv0.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.1.1**, после чего нажмите кнопку Add.
   - 3.12. Закройте окно Server0.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.2.1**, маску **255.255.255.0**, адрес шлюза **192.168.2.254** и адрес сервера DNS **192.168.1.1**.
5. Настройте компьютер PC1: задайте IP-адрес **192.168.3.1**, маску **255.255.255.0**, адрес шлюза **192.168.3.254** и адрес сервера DNS **192.168.1.1**.
6. Настройте компьютер PC2: задайте IP-адрес **192.168.4.1**, маску **255.255.255.0**, адрес шлюза **192.168.4.254** и адрес сервера DNS **192.168.1.1**.
7. Настройте облако:
   - 7.1. Выберите в рабочем пространстве облако Cloud0.
   - 7.2. В окне Cloud0 выберите вкладку Config.
   - 7.3. На вкладке Config нажмите кнопку Serial0.
   - 7.4. Включите порт Serial0.
   - 7.5. В выпадающем списке LMI выберите значение **Cisco**.
   - 7.6. В поле DLCI введите значение **102**, в поле Name введите значение **S0toS1** и нажмите кнопку Add.

7.7. В поле DLCI введите значение **103**, в поле Name введите значение **S0toS2** и нажмите кнопку Add.
7.8. В поле DLCI введите значение **104**, в поле Name введите значение **S0toS3** и нажмите кнопку Add.
7.9. На вкладке Config нажмите кнопку Serial1.
7.10. Включите порт Serial1.
7.11. В выпадающем списке LMI выберите значение **Cisco**.
7.12. В поле DLCI введите значение **101**, в поле Name введите значение **S1toS0** и нажмите кнопку Add.
7.13. На вкладке Config нажмите кнопку Serial2.
7.14. Включите порт Serial2.
7.15. В выпадающем списке LMI выберите значение **Cisco**.
7.16. В поле DLCI введите значение **101**, в поле Name введите значение **S2toS0** и нажмите кнопку Add.
7.17. На вкладке Config нажмите кнопку Serial3.
7.18. Включите порт Serial3.
7.19. В выпадающем списке LMI выберите значение **Cisco**.
7.20. В поле DLCI введите значение **101**, в поле Name введите значение **S3toS0** и нажмите кнопку Add.
7.21. На вкладке Config нажмите кнопку Frame Relay.
7.22. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS1**, в расположенном справа выпадающем списке Port выберите значение **Serial1**, в расположенном справа выпадающем списке Sublink выберите значение **S1toS0** и нажмите кнопку Add.
7.23. В расположенном слева выпадающем списке Port выберите значение **Serial0**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS2**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S2toS0** и нажмите кнопку Add.
7.24. В расположенном слева выпадающем списке Port выберите значение **Serial1**, в расположенном слева выпадающем списке Sublink выберите значение **S0toS3**, в расположенном справа выпадающем списке Port выберите значение **Serial2**, в расположенном справа выпадающем списке Sublink выберите значение **S3toS0** и нажмите кнопку Add.
7.25. Закройте окно Cloud0.

8. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#no shut
Router(config-if)#interface serial 2/0.102 point-to-point
Router(config-subif)#ip ad 192.168.5.1 255.255.255.0
Router(config-subif)#frame-relay interface-dlci 102
```

```
Router(config-subif)#int se2/0.103 po
Router(config-subif)#ip ad 192.168.6.1 255.255.255.0
Router(config-subif)#fr in 103
Router(config-subif)#int se2/0.104 po
Router(config-subif)#ip ad 192.168.7.1 255.255.255.0
Router(config-subif)#fr in 104
Router(config-subif)#exit
Router(config)#ip ro 192.168.2.0 255.255.255.0 192.168.5.2
Router(config)#ip ro 192.168.3.0 255.255.255.0 192.168.6.2
Router(config)#ip ro 192.168.4.0 255.255.255.0 192.168.7.2
Router(config)#exit
Router#sh fr pvc
Router#exit
```

9. Настройте маршрутизатор Router1, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.2.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#no shut
Router(config-if)#int se2/0.101 po
Router(config-subif)#ip ad 192.168.5.2 255.255.255.0
Router(config-subif)#fr in 101
Router(config-subif)#ip ro 0.0.0.0 0.0.0.0 192.168.5.1
Router(config-if)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

10. Настройте маршрутизатор Router2, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.3.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#no shut
Router(config-if)#int se2/0.101 po
Router(config-subif)#ip ad 192.168.6.2 255.255.255.0
Router(config-subif)#fr in 101
Router(config-subif)#ip ro 0.0.0.0 0.0.0.0 192.168.6.1
Router(config-subif)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

11. Настройте маршрутизатор Router3, для чего введите последовательность команд:

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip ad 192.168.4.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int se2/0
Router(config-if)#en fr
Router(config-if)#no shut
Router(config-if)#int se2/0.101 po
Router(config-subif)#ip ad 192.168.7.2 255.255.255.0
Router(config-subif)#fr in 101
Router(config-subif)#ip ro 0.0.0.0 0.0.0.0 192.168.7.1
Router(config-subif)#exit
Router(config)#exit
Router#sh fr pvc
Router#exit
```

12. На правой панели инструментов нажмите кнопку Inspect и проверьте таблицы маршрутизации:
    12.1. В таблице маршрутизатора Router0 должны присутствовать сети 192.168.1.0–192.168.7.0.
    12.2. В таблице маршрутизатора Router1 должны присутствовать сети 0.0.0.0, 192.168.2.0 и 192.168.5.0.
    12.3. В таблице маршрутизатора Router2 должны присутствовать сети 0.0.0.0, 192.168.3.0 и 192.168.6.0.
    12.4. В таблице маршрутизатора Router3 должны присутствовать сети 0.0.0.0, 192.168.4.0 и 192.168.7.0.
13. Проверьте связь между компьютерами и сервером:
    13.1. Передайте простой пакет с компьютера PC0 на сервер Server0, чтобы проверить соединение. Если первая попытка передачи оказалась неудачной, то попробуйте передать второй пакет.
    13.2. Передайте простой пакет с компьютера PC1 на сервер Server0.
    13.3. Передайте простой пакет с компьютера PC2 на сервер Server0.
14. Очистите сценарий моделирования, нажав в области сценария кнопку Delete.
15. Переключите Cisco Packet Tracer в режим Simulation.
16. Передайте простой пакет с компьютера PC0 на компьютер PC2 в пошаговом режиме. По какому маршруту пойдет этот пакет?
17. Переключите Cisco Packet Tracer в режим Realtime.
18. Протестируйте сетевые соединения с помощью диагностических утилит из стека протоколов TCP/IP:
    18.1. Выберите в рабочем пространстве компьютер PC0.
    18.2. В окне PC0 выберите вкладку Desktop.
    18.3. На вкладке Desktop нажмите кнопку Command Prompt.
    18.4. Введите команду **ping 192.168.1.1** и просмотрите результат ее выполнения.
    18.5. Введите команду **tracert serv0.ru** и просмотрите результат ее выполнения.
    18.6. Введите команду **ping 192.168.4.1** и просмотрите результат ее выполнения.
    18.7. Введите команду **tracert 192.168.4.1** и просмотрите результат ее выполнения.

18.8. Закройте окно Command Prompt.
18.9. Закройте окно PC0.
19. Сохраните модель сети в файле с именем **net_11_5_1**.
20. Завершите работу с программой Cisco Packet Tracer.

11.6. Задание для самостоятельной работы

В целях тренировки попробуйте самостоятельно создать и наладить модель сети, изображенной на рисунке 11.7.

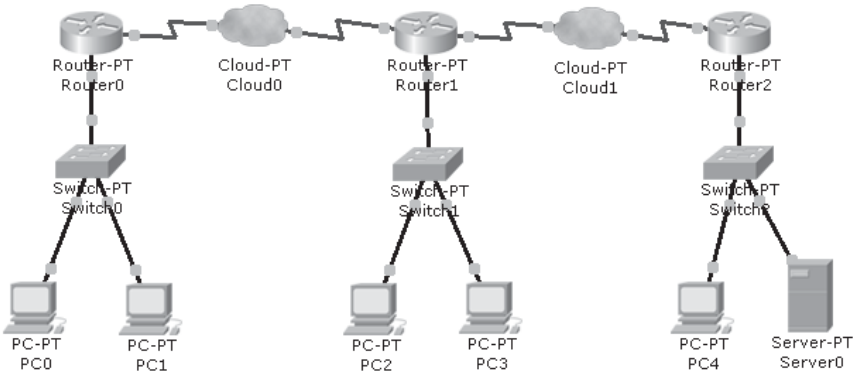

Рис. 11.7. Задание для самостоятельной работы

12. СПИСОК УПРАВЛЕНИЯ ДОСТУПОМ ACL

Список управления доступом (Access Control List, сокращенно — **ACL**) — это последовательный список правил, которые используются для разрешения или запрещения продвижения пакетов внутри сети [1]. Если список доступа не задан, то все пакеты внутри сети передаются без ограничений.

Список управления доступом обычно создают в целях обеспечения безопасности: для защиты от внешних атак, ограничения доступа и распределение загрузки сети.

Отладка списков управления доступом — это пример того, что имитационная модель может быть полезна не только для тренировок. При проведении натурного эксперимента ошибки в списках ACL могут серьезно нарушить работу сети, например, блокируя трафик некоторых приложений.

12.1. Стандартный ACL

При использовании стандартных списков управления доступом единственным критерием для определения того, что пакет разрешен или запрещён, является IP адрес источника этого пакета. Команда **access-list** (сокращенно — **ac**), которая создает один элемент списка доступа, имеет следующий формат:

access-list *access-list-number* {permit|deny} *address* [*source-wildcard*] [log]

где *access-list-number* — номер списка доступа, permit — указание разрешить прохождение пакета, deny — указание запретить прохождение пакета, *address* — IP-адрес источника пакета, *source-wildcard* — шаблон маски, log — указание включить логгирование пакетов, соответствующих данной записи.

В квадратных скобках указаны необязательные параметры.

Число access-list-number определяет принадлежность элемента к списку доступа с указанным номером. Первая команда access-list определяет первый элемент списка доступа, вторая команда определяет второй элемент и т.д. Маршрутизатор обрабатывает список доступа по элементам сверху вниз. То есть, если адрес пакета с учётом маски удовлетворяет условию некоторого элемента списка, то последующие элементы маршрутизатор не обрабатывает. Следовательно, элементы списка ACL, определяющие более общие условия, надлежит помещать в начале списка.

Для одного маршрутизатора может быть задано несколько стандартных списков доступа. Номер стандартного списка должен лежать в диапазоне от 1 до 99.

Если на маршрутизаторе задан список доступа, то маршрутизатор предполагает, что все адреса, не упомянутые в списке, запрещены.

Вместо адреса сети-источника address можно использовать ключевое слово **any**, означающее, что команду нужно применить ко всем источникам пакетов, или ключевое слово **host** со следующим за ним IP-адресом, означающее, что команду нужно применить к конкретному узлу (узлу), а не к сети в целом.

Шаблон маски в простейшем случае (если не используется суммирование маршрутов) представляет собой маску подсети в инверсной форме, то есть в двоичном коде маски все нули должны быть заменены на единицы, а единицы — на нули. Например, маска 255.255.0.0 в инверсной форме выглядит как 0.0.255.255.

Например, для того чтобы разрешить только трафик от узла с адресом 1.2.3.4 и запретить весь остальной трафик, достаточно в список доступа поместить один элемент

```
access-list 5 permit 1.2.3.4 0.0.0.0
```

В данном примере списку доступа присвоен номер 5.

Команды, размещенные в списке доступа, могут применяться к целому диапазону адресов. Например, чтобы разрешить трафик для диапазона адресов 10.2.16.0–10.2.31.255, нужно подать команду

```
access-list 5 permit 10.2.16.0 0.0.15.255
```

Для того, чтобы маршрутизатор начал использовать список доступа, этот список должен быть применен к некоторому интерфейсу с помощью команды **ip access-group** (сокращенно — **ip ac**), которая имеет следующий формат:

```
ip access-group access-list-number {in|out}
```

где *access-list-number* — номер списка управления доступом, in — указание использовать список как входной, out — указание использовать список как выходной.

Когда список управления доступом применяется как входной, маршрутизатор сверяет адрес пакета с элементами списка сразу после его получения. Маршрутизатор пропускает пакет, если его адрес удовлетворяет условиям одного из разрешающих элементов списка, либо отбрасывает пакет, если его адрес соответствует условиям запрещающих элементов или вообще не был упомянут в списке.

Если список управления доступом используется как выходной, то маршрутизатор вначале передает пакет на интерфейс назначения, и только после этого сверяется со списком. Далее маршрутизатор либо разрешает пакету покинуть интерфейс, либо отбрасывает его.

Для того чтобы применить список к интерфейсу, нужно вначале войти в режим конфигурирования интерфейса. После этого, чтобы применить, например, созданный ранее список с номером 5 как входной, нужно подать команду

```
ip access-group 5 in
```

Для того чтобы отменить на интерфейсе список доступа с заданным номером, используется команда **no ip access-group** (сокращенно — **no ip ac**). Например, для отмены входного списка номер 5 нужно применить к интерфейсу следующую команду:

```
no ip access-group 5 in
```

Для того, чтобы проконтролировать настройку маршрутизатора, в привилегированном режиме (после выхода из режима конфигурирования) можно использовать следующие команды:

- **show access-lists** — показать перечень списков доступа;
- **show ip interface** — показать состояние интерфейса (в том числе — номер используемого списка доступа);
- **show running-config** — показать работающую в данный момент конфигурацию.

12.1.1. Настройка стандартного списка ACL

Рассмотрим в качестве примера процесс настройки стандартного списка ACL. Вначале мы создадим и настроим модель компьютерной сети, изображенной на рисунке 12.1, проверим ее работоспособность до начала использования списков доступа. Затем мы создадим стандартный список управления доступом, применим его на выходе интерфейса FastEthernet1/0 маршрутизатора Router0.

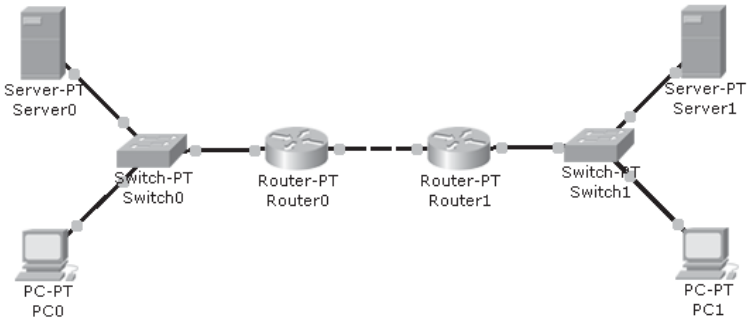

Рис. 12.1. Модель компьютерной сети для упражнений со списками доступа

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве два маршрутизатора Router0 и Router1 типа Router-PT, два коммутатора Switch0 и Switch1 типа Switch-PT, два сервера Server0 и Server1 и два компьютера PC0 и PC1 так, как показано на рисунке 14.1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   - 3.1. Присоедините прямым кабелем порт FastEthernet сервера Server0 к порту FastEthernet0/1 коммутатора Switch0.
   - 3.2. Присоедините прямым кабелем порт FastEthernet компьютера PC0 к порту FastEthernet1/1 коммутатора Switch0.
   - 3.3. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
   - 3.4. Присоедините прямым кабелем порт FastEthernet сервера Server1 к порту FastEthernet0/1 коммутатора Switch1.
   - 3.5. Присоедините прямым кабелем порт FastEthernet компьютера PC1 к порту FastEthernet1/1 коммутатора Switch1.
   - 3.6. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet0/0 маршрутизатора Router1.
   - 3.7. Присоедините перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet1/0 маршрутизатора Router1.
4. Настройте сервер Server0:
   - 4.1. Выберите в рабочем пространстве сервер Server0.
   - 4.2. В окне Server0 выберите вкладку Config.

4.3. В области настройки глобальных параметров Global Settings задайте статический режим настройки шлюза, адрес шлюза **192.168.1.1** и адрес DNS-сервера **192.168.1.2**.
4.4. На вкладке Config в окне Server0 нажмите кнопку FastEthernet.
4.5. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.1.2** и маску **255.255.255.0**.
4.6. В окне Server0 выберите вкладку Services.
4.7. На вкладке Services нажмите кнопку HTTP.
4.8. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
4.9. На вкладке Services в окне Server0 нажмите кнопку DNS.
4.10. В области настройки параметров DNS установите переключатель DNS Service в положение **On**, для того чтобы включить поддержку сервиса DNS.
4.11. В поле Name задайте для сервера имя **serv0.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.1.2**, после чего нажмите кнопку Add.
4.12. В поле Name задайте для сервера имя **serv1.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.2.2**, после чего нажмите кнопку Add. В результате в таблице DNS должно присутствовать две записи (рис. 12.2).
4.13. Закройте окно Server0.

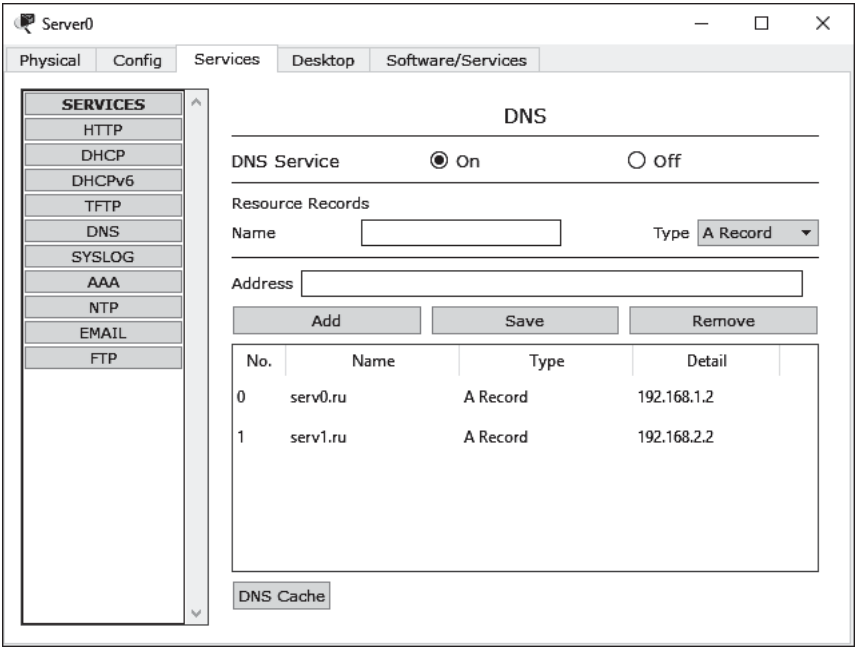

Рис. 12.2. Таблица DNS на сервере Server0

5. Настройте компьютер PC0: задайте IP-адрес **192.168.1.3**, маску **255.255.255.0**, адрес шлюза **192.168.1.1** и адрес сервера DNS **192.168.1.2**.
6. Настройте сервер Server1:
   6.1. Выберите в рабочем пространстве сервер Server1.
   6.2. В окне Server1 выберите вкладку Config.
   6.3. В области настройки глобальных параметров задайте статический режим настройки шлюза, адрес шлюза **192.168.2.1** и адрес DNS-сервера **192.168.2.2**.
   6.4. На вкладке Config нажмите кнопку HTTP.
   6.5. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
   6.6. На вкладке Config нажмите кнопку DNS.
   6.7. В области настройки параметров DNS установите переключатель DNS Service в положение **On**.
   6.8. В поле Name задайте для сервера имя **serv0.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.1.2**, после чего нажмите кнопку Add.
   6.9. В поле Name задайте для сервера имя **serv1.ru**, в списке Type выберите значение **A Record**, в поле Address введите IP-адрес сервера **192.168.2.2**, после чего нажмите кнопку Add.
   6.10. На вкладке Config нажмите кнопку FastEthernet.
   6.11. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **192.168.2.2** и маску **255.255.255.0**.
   6.12. Закройте окно Server1.
7. Настройте компьютер PC1: задайте IP-адрес **192.168.2.3**, маску **255.255.255.0**, адрес шлюза **192.168.2.1** и адрес сервера DNS **192.168.2.2**.
8. Настройте маршрутизатор Router0:
   8.1. Выберите в рабочем пространстве маршрутизатор Router0.
   8.2. В окне Router0 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   8.3. Для интерфейса FastEthernet0/0 задайте статус порта **On**, адрес **192.168.1.1** и маску **255.255.255.0**.
   8.4. На вкладке Config нажмите кнопку FastEthernet1/0.
   8.5. Для интерфейса FastEthernet1/0 задайте статус порта **On**, адрес **192.168.3.1** и маску **255.255.255.0**.
   8.6. На вкладке Config нажмите кнопку RIP.
   8.7. В поле Network введите номер сети **192.168.1.0** и нажмите кнопку Add, затем в поле Network введите номер сети **192.168.3.0** и снова нажмите кнопку Add.
   8.8. Закройте окно Router0.
9. Настройте маршрутизатор Router1:
   9.1. Выберите в рабочем пространстве маршрутизатор Router1.
   9.2. В окне Router1 выберите вкладку Config, а затем нажмите кнопку FastEthernet0/0.
   9.3. Для интерфейса FastEthernet0/0 задайте статус порта **On**, адрес **192.168.2.1** и маску **255.255.255.0**.
   9.4. На вкладке Config нажмите кнопку FastEthernet1/0.
   9.5. Для интерфейса FastEthernet1/0 задайте статус порта **On**, адрес **192.168.3.2** и маску **255.255.255.0**.
   9.6. На вкладке Config нажмите кнопку RIP.
   9.7. В поле Network введите номер сети **192.168.2.0** и нажмите кнопку Add, затем в поле Network введите номер сети **192.168.3.0** и снова нажмите кнопку Add.

9.8. Закройте окно Router1.

10. Подождите до завершения процесса самонастройки коммутаторов (на всех портах должны появиться зеленые сигналы).
11. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу поочередно на каждый из маршрутизаторов и проверьте таблицы маршрутизации: в таблицах должны присутствовать сети 192.168.1.0, 192.168.2.0 и 192.168.3.0.
12. Проверьте связь между конечными узлами сети путем поочередной передачи простых пакетов с компьютера PC0 на сервер Server0, с компьютера PC0 на сервер Server1 и с компьютера PC0 на компьютер PC1. Если процесс передачи какого-либо пакета завершится неудачно, то попробуйте передать пакет повторно.
13. Проверьте наличие доступа к интернет-странице сервера Server1 с компьютера PC0:
    13.1. Выберите в рабочем пространстве персональный компьютер PC0.
    13.2. В окне PC0 выберите вкладку Desktop.
    13.3. На вкладке Desktop нажмите кнопку Web Browser.
    13.4. В окне браузера наберите в поле URL адрес **serv1.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server1.
    13.5. Закройте окно браузера.
    13.6. Закройте окно PC0.
14. Проверьте наличие доступа к интернет-странице сервера Server0 с компьютера PC1:
    14.1. Выберите в рабочем пространстве персональный компьютер PC1.
    14.2. В окне PC1 выберите вкладку Desktop.
    14.3. На вкладке Desktop нажмите кнопку Web Browser.
    14.4. В окне браузера наберите в поле URL адрес **serv0.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server0.
    14.5. Закройте окно браузера.
    14.6. Закройте окно PC1.
15. Сохраните исходную модель сети, в которой на маршрутизаторах не были заданы списки доступа, в файле с именем **net_12_1_1a**.
16. Настройте список доступа на маршрутизаторе Router0 таким образом, чтобы разрешить прохождение пакетов только от узла с адресом 192.168.1.2 (то есть от сервера Server0), для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#access-list 1 permit 192.168.1.2
Router(config)#int fa1/0
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
```

17. Проверьте настройку маршрутизатора Router0:
    17.1. Когда в командной строке появится приглашение Router#, введите команду **sh ac** (сокращенный вариант написания команды show access-lists), чтобы проверить список доступа.
    17.2. Когда в командной строке появится приглашение Router#, введите команду **sh ru** (сокращенный вариант написания команды show running-config), чтобы проверить работающую в данный момент конфигурацию. Если в командной

строке вы видите сообщение «--More--», то нажимайте клавишу пробела до тех пор, пока это сообщение не сменится приглашением Router#.

17.3. Когда в командной строке появится приглашение Router#, введите команду **sh ip int** (сокращенный вариант написания команды show ip interface), чтобы проверить состояние интерфейсов маршрутизатора Router0. Если в командной строке вы видите сообщение «--More--», то нажимайте клавишу пробела до тех пор, пока это сообщение не сменится приглашением Router#. Используя полосу прокрутки, прокрутите изображение на вкладке CLI и убедитесь, что в описании интерфейса FastEthernet1/0 присутствует строка, содержащая текст «Outgoing access list is 1».

17.4. Введите команду **exit**, чтобы завершить работу в привилегированном режиме.

17.5. Закройте окно Router0.

18. Передайте простой пакет с компьютера PC1 на сервер Server0. Если процесс передачи пакета завершится неудачно, то попробуйте передать пакет повторно.
19. Проверьте наличие доступа к интернет-странице сервера Server0 с компьютера PC1:
    19.1. Выберите в рабочем пространстве персональный компьютер PC1.
    19.2. В окне PC1 выберите вкладку Desktop.
    19.3. На вкладке Desktop нажмите кнопку Web Browser.
    19.4. В окне браузера наберите в поле URL адрес **serv0.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server0.
    19.5. Закройте окно браузера.
    19.6. Закройте окно PC1.
20. Переключите Cisco Packet Tracer в режим Simulation.
21. В пошаговом режиме передайте простой пакет с компьютера PC1 на сервер Server0.
22. Попытайтесь в пошаговом режиме передать простой пакет с компьютера PC0 на сервер Server1 и проследите за его продвижением — маршрутизатор Router0 не должен пропускать этот пакет.
23. Попытайтесь в пошаговом режиме передать простой пакет с компьютера PC1 на компьютер PC0 и проследите за его продвижением — пакет с icmp-запросом должен дойти компьютера PC0, но ответный пакет маршрутизатор Router0 пропускать не должен.
24. Сохраните модель сети в файле с именем **net_12_1_1b**.
25. Завершите работу с программой Cisco Packet Tracer.

12.2. Расширенный список ACL

Если в стандартном списке доступа нужно указать только адрес источника пакета, то в расширенном ACL должны быть указаны и адрес приёмника, и адрес источника пакета (вместе с масками). В командах расширенного списка ACL можно также задавать дополнительную информацию о протоколах (например, для протоколов TCP и UDP разрешено указывать номер порта, а для протокола ICMP — тип сообщения).

Команда расширенного списка доступа имеет следующий формат:

```
access-list access-list-number {permit|deny} protocol source
source-wildcard [operator source-port] destination destina-
tion-wildcard [operator destination-port] [established] [log]
```

где access-list-number — номер списка доступа (значение в диапазоне от 100 до 199), permit — указание разрешить прохождение пакета, deny — указание запретить прохождение пакета, *protocol* — тип протокола (eigrp, icmp, ip, tcp, ospf, udp и др.), *source* — IP-адрес источника, *source-wildcard* — шаблон маски источника, *operator* — оператор сравнения, *source-port* — номер порта источника, *destination* — IP-адрес получателя, *destination-wildcard* — шаблон маски получателя, *destination-port* — номер порта получателя, established — указание разрешить прохождение TCP-сегментов, которые являются частью уже установленной TCP-сессии, log — указание включить логгирование пакетов, соответствующих данной записи.

В квадратных скобках указаны необязательные параметры.

Команды расширенного списка доступа позволяют разрешать или запрещать прохождение пакета, основываясь не только на типе протокола, но и на номерах используемых портов. Для общеизвестных приложений применяются порты с номерами меньше 1024:

- 20 — передача данных по FTP;
- 21 — управление протоколом FTP;
- 22 — SSH;
- 23 — Telnet;
- 25 — SMTP;
- 53 — DNS;
- 67, 68 — DHCP;
- 69 — TFTP;
- 80 — HTTP;
- 110 — POP3;
- 161 — SNMP;
- 443 — SSL.

В командах расширенного списка можно использовать не только номера портов, но и их условные обозначения, например, ftp, pop3, smtp, telnet или www.

Для сравнения номеров портов можно использовать операторы eq (равно), neq (не равно), gt (больше чем), lt (меньше чем).

Например, чтобы в списке с номером 115 разрешить передачу пакетов SMTP к узлу 192.168.1.5, нужно подать команду:

```
access-list 115 permit tcp any host 192.168.1.5 eq 25
```

Для того, чтобы задать в команде диапазон портов, нужно указать начальное и конечное значения диапазона.

Так же, как и стандартный список доступа, расширенный список ACL должен быть привязан либо к входящему, либо — к исходящему трафику какого-либо интерфейса.

К одному интерфейсу нельзя привязать более одного списка доступа.

К трафику, сгенерированному самим маршрутизатором, список доступа не применяется.

12.2.1. Настройка расширенного списка ACL

В этом упражнении мы настроим список доступа на маршрутизаторе Router1 таким образом, чтобы запретить только передачу ICMP-пакетов из внешних сетей и во внешние сети.

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Откройте файл **net_12_1_1a** с исходной моделью сети, в которой не использовались списки доступа.
3. Настройте расширенный список доступа на маршрутизаторе Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#access-list 101 deny icmp any any
Router(config)#access-list 101 permit ip any any
Router(config)#int fa1/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
```

4. Когда в командной строке появится приглашение Router#, введите команду **sh ac**, чтобы проверить список доступа. После этого введите команду **exit** и закройте окно Router1.
5. Проверьте наличие доступа к интернет-странице сервера Server1 с компьютера PC0:
   5.1. Выберите в рабочем пространстве персональный компьютер PC0.
   5.2. В окне PC0 выберите вкладку Desktop.
   5.3. На вкладке Desktop нажмите кнопку Web Browser.
   5.4. В окне браузера наберите в поле URL адрес **serv1.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server1.
   5.5. Закройте окно браузера.
   5.6. Закройте окно PC0.
6. Проверьте наличие доступа к интернет-странице сервера Server0 с компьютера PC1:
   6.1. Выберите в рабочем пространстве персональный компьютер PC1.
   6.2. В окне PC1 выберите вкладку Desktop.
   6.3. На вкладке Desktop нажмите кнопку Web Browser.
   6.4. В окне браузера наберите в поле URL адрес **serv0.ru** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server0.
   6.5. Закройте окно браузера.
   6.6. Закройте окно PC1.
7. Переключите Cisco Packet Tracer в режим Simulation.
8. Попытайтесь в пошаговом режиме передать простой пакет с компьютера PC0 на сервер Server1 и проследите за его продвижением — маршрутизатор Router1 не должен пропускать этот пакет.
9. Попытайтесь в пошаговом режиме передать простой пакет с компьютера PC1 на сервер Server0 и проследите за его продвижением — маршрутизатор Router1 должен пропустить icmp-запрос к серверу Server0, но не должен пропускать ответный пакет от сервера к компьютеру PC0.
10. Сохраните модель сети в файле с именем **net_12_2_1**.
11. Завершите работу с программой Cisco Packet Tracer.

12.3. Задание для самостоятельной работы

Используя приведенную на рисунке 12.1 модель, настройте на маршрутизаторах расширенные списки доступа таким образом, чтобы запретить только передачу между сетями пакетов протокола HTTP.

13. ТЕХНОЛОГИИ NAT И PAT

В документации Cisco частные IP-адреса, используемые во внутренней сети предприятия, называются **внутренними локальными адресами**, а адреса, используемые для представления узлов предприятия в Интернете, — **внутренними глобальными адресами** [11].

13.1. Технология преобразования сетевых адресов

Технология преобразования сетевых адресов (Network Address Translation, сокращенно — **NAT**) обеспечивает преобразование IP-адресов транзитных пакетов, позволяя узлам, не имеющим собственных глобально уникальных IP-адресов, осуществлять связь с другими узлами через Интернет.

Для того, чтобы частный узел мог быть представлен в Интернете, маршрутизатор, использующий NAT, заменяет внутренний локальный адрес узла на внутренний глобальный адрес при прохождении пакета из сети предприятия в Интернет, а при получении ответного пакета производит обратную замену.

Существует два способа трансляции адресов: статический и динамический.

Статическая трансляция предусматривает отображение частного IP-адреса на жестко закрепленный за ним глобально уникальный IP-адрес по принципу «один к одному».

Динамическая трансляция отображает частный IP-адрес на IP-адрес из пула (специально созданной группы) глобально уникальных адресов.

Перегруженный NAT (**PAT**) — это форма динамической трансляции адресов, при которой несколько частных адресов отображаются в один глобально уникальный адрес путем использования различных номеров портов.

13.2. Настройка режима преобразования адресов в маршрутизаторе

Рассмотрим порядок действий, выполнение которых необходимо для настройки NAT на маршрутизаторе.

Для того чтобы включить на маршрутизаторе режим статической трансляции адресов, нужно выполнить следующие действия:

- установить режим статической трансляции между внутренним локальным адресом и внутренним глобальным адресом;
- указать внутренний интерфейс и пометить его как принадлежащий внутренней сети;
- указать внешний интерфейс и пометить его как принадлежащий внешней сети.

Задать режим статической трансляции адресов можно с помощью команды **ip nat inside source static** (сокращенно — **ip nat in so st**), которая имеет следующий формат:

```
ip nat inside source static local-ip global-ip
```

где *local-ip* — внутренний IP-адрес, *global-ip* — внешний IP-адрес.

У пакета, пришедшего на внутренний интерфейс, изменяется IP-адрес отправителя, у пакета, пришедшего на внешний интерфейс, изменяется IP-адрес получателя. Пометить интерфейс, как принадлежащий внутренней сети, можно с помощью команды **ip nat inside** (сокращенно — **ip nat in**), а чтобы пометить интерфейс, как принадлежащий внешней сети, нужно использовать команду **ip nat outside** (сокращенно — **ip nat out**).

Например, предположим, что у маршрутизатора M в качестве внутреннего применяется интерфейс FastEthernet0/0 с адресом 192.168.1.1, в качестве внешнего — интерфейс FastEthernet1/0 с адресом 201.1.1.1, и нужно включить преобразование внутреннего адреса 192.168.1.3 во внешний IP-адрес 201.1.1.3. В этом случае последовательность команд будет выглядеть следующим образом:

```
M(config)#ip nat inside source static 192.168.1.3 200.1.1.3
M(config)#interface f0/0
M(config-if)#ip address 192.168.1.1 255.255.255.0
M(config-if)#ip nat inside
M(config-if)#no shut
M(config-if)#interface f1/0
M(config-if)#ip address 201.1.1.1 255.255.255.248
M(config-if)#ip nat outside
M(config-if)#no shut
```

Для включения режима динамической трансляции адресов нужно выполнить следующие действия:

- создать пул глобальных адресов;
- создать стандартный список доступа и указать в нем диапазон внутренних адресов, подлежащих трансляции;
- установить режим динамической трансляции адресов;
- указать внутренний интерфейс и пометить его как принадлежащий внутренней сети;
- указать внешний интерфейс и пометить его как принадлежащий внешней сети.

Создать пул глобальных адресов можно при помощи команды **ip nat pool**, которая имеет следующий формат:

ip nat pool *name start-ip end-ip* netmask *netmask*

где *name* — имя пула, *start-ip* — начальный адрес диапазона входящих в пул адресов, *end-ip* — конечный адрес диапазона адресов, *netmask* — маска сети.

Адреса, входящие в пул, должны находиться в той же подсети, что и адрес внешнего интерфейса.

Установить режим динамической трансляции адресов можно с помощью команды **ip nat inside source list**, которая имеет следующий формат:

ip nat inside source list *number* pool *name* [overload]

где *number* — номер списка доступа, *name* — имя пула адресов.

Если в этой команде присутствует необязательный параметр overload, то будет выполняться перегруженная трансляция адресов (PAT).

Трансляции будут подвергаться только адреса, разрешенные в списке доступа. Пакеты с другими (запрещенными) адресами не отбрасываются и их адреса не изменяются.

Предположим, что у маршрутизатора M в качестве внутреннего применяется интерфейс FastEthernet0/0 с адресом 192.168.1.1, а в качестве внешнего — интерфейс FastEthernet1/0 с адресом 201.1.1.1. Нужно включить преобразование адресов частной сети 192.168.1.0 в IP-адреса, лежащие в диапазоне от 201.1.1.3 до 201.1.1.6, используя метод PAT. В этом случае последовательность команд будет такой:

```
M(config)#access-list 25 permit 192.168.1.0 0.0.0.255
M(config)#ip nat pool p 201.1.1.3 201.1.1.6 netmask
255.255.255.248
M(config)#ip nat inside source list 25 pool p overload
M(config)#int f0/0
M(config-if)#ip ad 192.168.1.1 255.255.255.0
M(config-if)#ip nat inside
M(config-if)#no shut
M(config-if)#int f1/0
M(config-if)#ip ad 201.1.1.1 255.255.255.248
M(config-if)#ip nat outside
M(config-if)#no shut
```

13.2.1. Моделирование перегруженной трансляции адресов

В этом упражнении мы настроим перегруженную трансляцию адресов на маршрутизаторе Router0 таким образом, чтобы обеспечить доступ в Интернет с компьютеров, входящих в частную сеть.

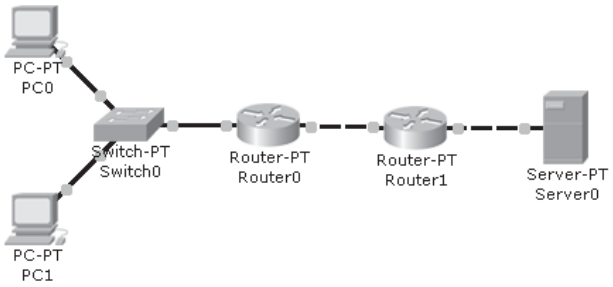

Рис. 13.1. Модель компьютерной сети, в которой используется трансляция адресов

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве маршрутизаторы Router0 и Router1 типа Router-PT, коммутатор Switch0 типа Switch-PT, сервер Server0 и компьютеры PC0 и PC1 так, как показано на рисунке 13.1.
3. Соедините между собой устройства, размещенные в рабочем пространстве:

3.1. Присоедините перекрестным кабелем сервер Server0 к порту FastEthernet0/0 маршрутизатора Router1.
3.2. Присоедините прямым кабелем компьютер PC0 к порту FastEthernet1/1 коммутатора Switch0.
3.3. Присоедините прямым кабелем компьютер PC1 к порту FastEthernet2/1 коммутатора Switch0.
3.4. Присоедините прямым кабелем порт FastEthernet0/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
3.5. Присоедините перекрестным кабелем порт FastEthernet1/0 маршрутизатора Router0 к порту FastEthernet1/0 маршрутизатора Router1.
4. Настройте компьютер PC0: задайте IP-адрес **192.168.1.2**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
5. Настройте компьютер PC0: задайте IP-адрес **192.168.1.3**, маску **255.255.255.0** и адрес шлюза **192.168.1.1**.
6. Настройте сервер Server0:
6.1. Выберите в рабочем пространстве сервер Server0.
6.2. В окне Server0 выберите вкладку Config.
6.3. В области настройки глобальных параметров Global Settings задайте статический режим настройки и введите адрес шлюза **200.1.1.1**.
6.4. На вкладке Config в окне Server0 нажмите кнопку FastEthernet.
6.5. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IP, адрес **200.1.1.2** и маску **255.255.255.0**.
6.6. В окне Server0 выберите вкладку Services.
6.7. На вкладке Services нажмите кнопку HTTP.
6.8. В области настройки параметров протокола HTTP установите переключатель HTTP в положение **On**.
6.9. Закройте окно Server0.
7. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho R0
R0(config)#access-list 5 permit 192.168.1.0 0.0.0.255
R0(config)#ip nat pool p1 201.1.1.3 201.1.1.6 netmask
255.255.255.248
R0(config)#ip nat ins source list 5 pool p1 overload
R0(config)#int f0/0
R0(config-if)#ip ad 192.168.1.1 255.255.255.0
R0(config-if)#ip nat inside
R0(config-if)#no shut
R0(config-if)#int f1/0
R0(config-if)#ip ad 201.1.1.1 255.255.255.248
R0(config-if)#ip nat outside
R0(config-if)#no shut
R0(config-if)#exit
R0(config)#ip route 0.0.0.0 0.0.0.0 201.1.1.2
R0(config)#exit
R0#exit
```

8. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ho R1
R1(config)#int f0/0
R1(config-if)#ip ad 200.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int f1/0
R1(config-if)#ip ad 201.1.1.2 255.255.255.0
R1(config-if)#no shut
R1(config-if)#end
R1#exit
```

9. Нажмите кнопку Fast Forward Time, чтобы временно ускорить процесс моделирования
10. Просмотрите таблицу маршрутизации на маршрутизаторе Router0: в таблице должны присутствовать сети 192.168.1.0 и 201.1.1.0, а также предназначенный для использования по умолчанию статический маршрут 0.0.0.0.
11. Просмотрите таблицу маршрутизации на маршрутизаторе Router1: в таблице должны присутствовать сети 200.1.1.0 и 201.1.1.0.
12. Передайте простой пакет с компьютера PC0 на сервер Server0. Если процесс передачи пакета завершится неудачно, то несколько раз повторите передачу.
13. Проверьте наличие доступа к интернет-странице сервера Server0 с компьютера PC1:
    13.1. Выберите в рабочем пространстве персональный компьютер PC1.
    13.2. В окне PC1 выберите вкладку Desktop.
    13.3. На вкладке Desktop нажмите кнопку Web Browser.
    13.4. В окне браузера наберите в поле URL адрес **200.1.1.2** и нажмите кнопку Go. В результате выполнения этой операции в окне браузера должна отобразиться интернет-страница сервера Server0.
    13.5. Закройте окно браузера.
    13.6. Закройте окно PC1.
14. Попробуйте передать простой пакет с сервера Server0 на компьютер PC0. Пакет передаваться не должен, так как частная сеть невидима из Интернет.
15. Переключите Cisco Packet Tracer в режим Simulation.
16. В пошаговом режиме передайте простой пакет с PC0 на Server0. После выполнения каждого шага проверяйте заголовок IP-пакета. Как будут меняться адреса отправителя и получателя при прохождении пакета через маршрутизатор Router0?
17. Сохраните модель сети в файле с именем **net_13_2_1**.
18. Завершите работу с программой Cisco Packet Tracer.

13.3. Задание для самостоятельной работы

Настройте изображенную на рисунке 13.2 модель таким образом, чтобы обеспечить доступ к серверу с персональных компьютеров, используя перегруженную трансляцию адресов.

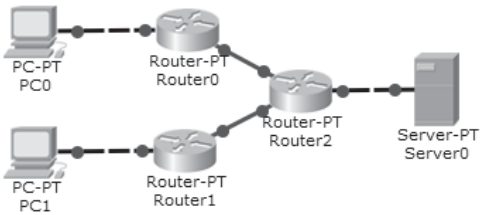

Рис. 13.2. Задание для самостоятельной работы

Примечание: маршрутизаторы нужно соединить друг с другом при помощи оптоволоконных кабелей.

14. ПРОТОКОЛ IPv6

Стремление решить проблему нехватки IP-адресов в компьютерных сетях, использующих протокол IPv4, привело к разработке новой, шестой версии протокола IP (IPv6).

14.1. Адресация по протоколу IPv6

Рассмотрим систему адресации, которую использует протокол IPv6.

Адрес IPv6 состоит из префикса подсети и идентификатора интерфейса. Адрес имеет длину 128 бит, разделяется на части по 16 бит, которые преобразуются в 4-значные шестнадцатеричные числа и разделяются двоеточиями (такая форма записи называется двухточечно-шестнадцатеричной).

Пространство адресов IPv6 делится согласно значениям старших битов адреса, которые образуют **префикс**. Длина префикса ***переменная***. Префикс записывается в нотации «адрес/длина префикса». Если префикс имеет длину n бит, то длина идентификатора интерфейса составляет (128-n) бит.

Представление адресов IPv6 может быть упрощено путём удаления начальных нулей в каждом 16-битном блоке, однако каждый из блоков должен содержать не менее одной цифры шестнадцатеричного кода.

Некоторые типы адресов содержат длинные последовательности нулей. Для дальнейшего упрощения адресов непрерывная последовательность блоков, состоящих из нулей, может быть сокращена до двойного двоеточия (например, адрес FF01:0:0:0:0:0:0:1 можно сократить до FF01::1). Подобное сокращение можно использовать только для одного сплошного ряда блоков и только один раз.

Адреса IPv6 ассоциируются с интерфейсами, а не с узлами, причем **одному интерфейсу могут соответствовать несколько адресов**.

Интерфейс принадлежит только одному узлу, а узел может иметь несколько интерфейсов.

В стандарте IPv6 определено три типа идентификаторов интерфейсов:

- **Unicast** (уникаст) — идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.
- **Anycast** (эникаст) — идентификатор набора интерфейсов, принадлежащих разным узлам. Пакет, посланный по эникастному адресу, доставляется ближайшему из интерфейсов, указанных в адресе.
- **Multicast** (мультикаст) — идентификатор набора интерфейсов, принадлежащих разным узлам. Пакет, посланный по мультикастному адресу, доставляется всем интерфейсам, заданным этим адресом.

Существует несколько форм адресов одиночного интерфейса:

- глобальный адрес уникастного интерфейса провайдера;
- адрес локальной связи;
- адрес локальной подсети;
- адрес, совместимый с IPv4;
- адрес точки доступа к услугам.

Глобальный адрес уникастного интерфейса провайдера эквивалентен общедоступному адресу IPv4 и применяется для глобальной маршрутизации.

Адрес локальной связи используется при обмене данными с соседними узлами сети. Адреса локальной связи начинаются с префикса FE80::/64.

Адрес локальной подсети начинается с префикса FEC0::/48 и недоступен из других подсетей.

Адреса совместимости определены для облегчения перехода от адресов IPv4 к адресам IPv6:

- **IPv4-совместимый адрес** используется узлами, работающими как с протоколом IPv4, так и с протоколом IPv6. Адрес имеет вид 0:0:0:0:0:0:w.x.y.z или ::w.x.y.z, где w.x.y.z — точечно-десятичное представление адреса IPv4.
- **IPv4-сопоставленный адрес** применяется для представления узлу IPv6 другого узла, работающего только по протоколу IPv4. Адрес имеет вид 0:0:0:0:0:FFFF:w.x.y.z или ::FFFF:w.x.y.z.
- **Адрес 6to4** используется узлами, работающими как с IPv4, так и с IPv6. Адрес формируется путём объединения префикса 2002::/16 с 32-битным адресом IPv4, в результате чего получается 48-битный префикс.

Адрес точки доступа к услугам (Network Service Access Point, **NSAP**) имеет префикс 0000001, а последние 121 бит адреса сопоставляются адресу NSAP.

Адрес любого интерфейса группы интерфейсов идентифицирует некоторую группу интерфейсов. Пакеты, отправляемые на такой адрес, доставляются на один (ближайший) интерфейс.

Адрес группы интерфейсов (мультикаст-адрес) используется для групповой доставки пакетов. Отправляемые на такой адрес пакеты доставляются на все указанные этим адресом интерфейсы. В стандарте IPv6 не существует широковещательных адресов, а их функции переданы мультикастным адресам.

Узлу назначаются следующие уникастные адреса:

- адрес локальной связи для каждого интерфейса;
- адреса для каждого интерфейса;
- петлевой адрес.

Кроме того, каждый узел прослушивает трафик на следующих адресах многоадресной рассылки:

- адрес всех узлов в области локального узла (FF01::1);
- адрес всех узлов в области локальной связи (FF02::1);
- адрес запроса узла для каждого уникастного адреса на каждом интерфейсе;
- адреса многоадресной рассылки для групп, присоединённых к каждому интерфейсу.

Маршрутизатору назначаются следующие уникастные адреса:

- адрес локальной связи для каждого интерфейса;
- уникастные адреса для каждого интерфейса;
- петлевой адрес.

Маршрутизатору также назначаются эникастные адреса для каждой подсети.

Кроме того, каждый маршрутизатор прослушивает трафик на следующих адресах многоадресной рассылки:

- адрес всех узлов в области локального узла (FF01::1);
- адрес всех маршрутизаторов в области локального узла (FF01::2);
- адрес всех узлов в области локальной связи (FF02::);
- адрес всех маршрутизаторов в области локальной связи (FF02::2);
- адрес всех маршрутизаторов в области локальной подсети (FF05::2);
- адрес запроса узла для каждого уникастного адреса на каждом интерфейсе;
- адреса групп, присоединённых к каждому интерфейсу.

Идентификатор интерфейса может быть сформирован следующими способами:

- сгенерирован на основе адреса EUI-64 согласно документу RFC-3513;
- сгенерирован случайным образом согласно документу RFC-3041;
- назначен при автоматической настройке адреса, например, по протоколу DHCPv6;
- настроен вручную.

Согласно RFC-3513, все уникастные адреса, имеющие префиксы с 001 по 111, должны использовать 64-битный идентификатор интерфейса, образованный из адреса EUI-64 (Extended Unique Identifier);

IEEE EUI-64 — это новый стандарт адресации сетевых интерфейсов: длина идентификатора компании в нем составляет 24 бита, а идентификатор расширения имеет длину 40 бит.

Адрес EUI-64 образуется из адреса IEEE 802 путём вставки в адрес IEEE 802 между идентификатором компании и идентификатором расширения следующих 16 бит: 11111111 11111110 (0xFF 0xFE). Для получения идентификатора интерфейса IPv6 из адреса IEEE 802 необходимо сначала преобразовать адрес IEEE 802 в адрес EUI-64, а затем инвертировать седьмой бит в первом байте адреса (бит U/L).

14.1.1. Настройка адресации в случае прямого соединения компьютеров

Для начала рассмотрим самый простой пример — настройку адресации по протоколу IPv6 в случае прямого соединения компьютеров друг с другом (рис. 14.1).

Рис. 14.1. Модель сети с прямым соединением компьютеров

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Поместите в рабочее пространство компьютеры PC0 и PC1 и соедините их перекрестным кабелем, как показано на рисунке 14.1.
3. Настройте компьютер PC0:
   3.1. Выберите в рабочем пространстве компьютер PC0.
   3.2. В окне PC0 выберите вкладку Config, а затем нажмите кнопку FastEthernet.
   3.3. Для адаптера сети Fast Ethernet задайте использование статической конфигурации IPv6 и адрес **2000::1**.
   3.4. Переместите курсор мыши в поле префикса и установите в качестве длины префикса значение **64**.
   3.5. Закройте окно PC0.
   3.6. Снова выберите в рабочем пространстве компьютер PC0.
   3.7. В окне PC0 перейдите на вкладку Config и нажмите кнопку FastEthernet. Программой Cisco Packet Tracer на основе глобального адреса IPv6 и MAC-адреса адаптера должен быть автоматически сформирован адрес локальной связи (рис. 14.2). Сравните друг с другом адрес локальной связи и MAC-адрес.
   3.8. Закройте окно PC0.

4. Аналогичным образом задайте для компьютера PC1 статическую конфигурацию IPv6 и адрес **2000::2**.
5. Наведите курсор мыши поочередно на каждую из станций PC0 и PC1, подождите до появления всплывающей подсказки и проверьте настройку IP-адресов.
6. Переключите Cisco Packet Tracer в режим Simulation.
7. Для того, чтобы проверить соединение, в пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1.
8. Сохраните модель сети в файле с именем **net_14_1_1**.
9. Завершите работу с программой Cisco Packet Tracer.

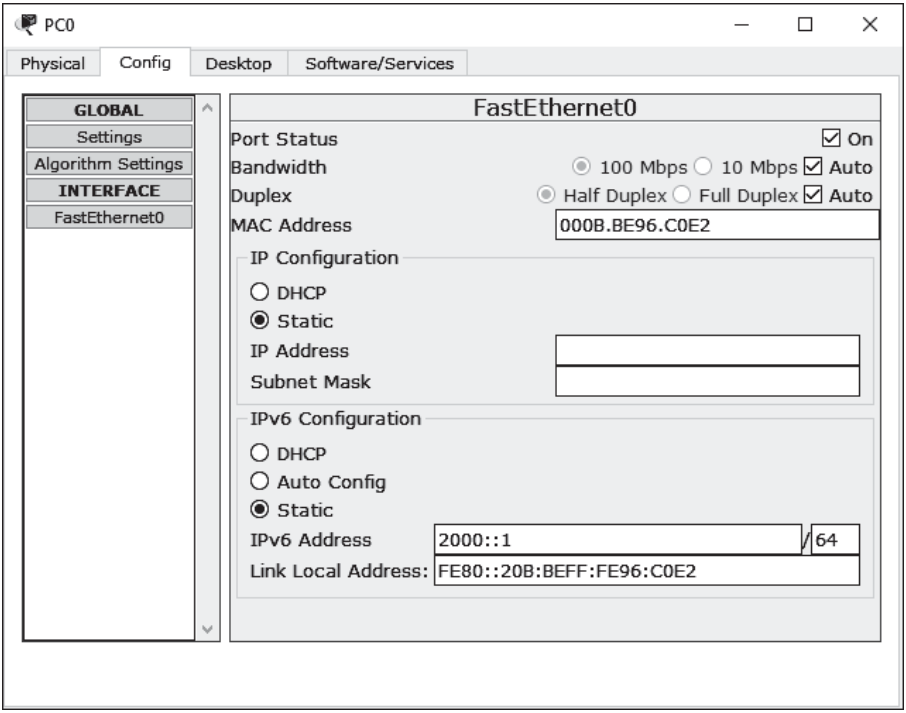

Рис. 14.2. Настройка адреса IPv6 на вкладке Config в окне модели компьютера

14.2. Команды для настройки интерфейсов

Задать IPv6-адрес для интерфейса можно с помощью команды ipv6 address (сокращенно — ipv6 ad), которая имеет следующий формат:

`ipv6 address` *`ipv6-address/prefix-length`*

где *ipv6-address* — адрес IPv6, *prefix-length* — длина префикса.

Например, чтобы присвоить интерфейсу FastEthernet 1/1 адрес 2000::100 с длиной префикса 64, нужно подать такую последовательность команд:

```
interface fastethernet 1/1
ipv6 address 2000::100/64
```

Задать адрес EUI-64 можно с помощью команды, которая имеет следующий формат:

```
ipv6 address ipv6-prefix/prefix-length eui-64
```

где *ipv6-prefix* — префикс IPv6, *prefix-length* — длина префикса.

Например, чтобы присвоить интерфейсу GigabitEthernet 1/0 адрес EUI-64, нужно подать следующие команды:

```
interface gigabitethernet 1/0
ipv6 address 2001:0DB8:0:A::/64 eui-64
```

Для того чтобы задать адрес локальной связи, нужно использовать команду следующего формата

```
ipv6 address ipv6-address link-local
```

где *ipv6-address* — адрес локальной связи.

Например, чтобы присвоить интерфейсу GigabitEthernet 0/0 адрес локальной связи FE80::1, нужно подать следующую последовательность команд:

```
interface gigabitethernet 0/0
ipv6 address FE80::1 link-local
```

После завершения процесса конфигурирования можно проверить правильность настройки устройства с помощью команды show ipv6 interfaces (сокращенно — **sh ipv6 int**), которая позволяет просмотреть статистику по всем сконфигурированным интерфейсам или только по интерфейсам определенного типа. Эта команда имеет следующий формат:

```
show ipv6 interfaces [type]
```

где *type* — символьное обозначение типа интерфейса.

Параметр type в команде show ipv6 interfaces является необязательным. Если этот параметр задан, то выводится информация по всем интерфейсам указанного типа или по конкретному интерфейсу с заданным номером, а если опущен — по всем сконфигурированным интерфейсам.

14.3. Команды для настройки маршрутизации

Для того чтобы маршрутизатор мог начать работать с адресами, соответствующими стандарту IPv6, необходимо подать команду **ipv6 unicast-routing** (сокращенно — **ipv6 uni**).

Разрешить на интерфейсе использование протокола маршрутизации RIP с поддержкой IPv6 можно с помощью команды **ipv6 rip enable** (сокращенно — **ipv6 rip en**), которая имеет следующий формат:

```
ipv6 rip word enable
```

где *word* — символический идентификатор процесса.

Например, чтобы разрешить использование RIP на интерфейсе FastEthernet 0/0 и присвоить процессу RIP идентификатор «cisco», нужно подать следующие команды:

```
interface fastethernet 0/0
ipv6 rip cisco enable
```

Если на маршрутизаторе требуется запустить протокол EIGRP, то настройку нужно начинать с присвоения маршрутизатору номера автономной системы. Указать номер автономной системы можно при помощи команды **ipv6 router eigrp** (сокращенно — **ipv6 ro ei**), которая имеет следующий формат:

```
ipv6 router eigrp autonomous-system-number
```

где *autonomous-system-number* — номер, идентифицирующий автономную систему (целое число в диапазоне от 1 до 65535).

Для корректной работы с протоколом IPv6 протоколу EIGRP требуются идентификаторы маршрутизаторов, аналогичные тем, которые используются протоколом OSPF. Идентификатор маршрутизатора RID представляет собой 32-битовый номер, записывается в формате IP-адреса и может быть присвоен маршрутизатору с помощью команды **router-id**, которая имеет следующий формат:

```
router-id ip-address
```

где *ip-address* — идентификатор маршрутизатора в формате адреса IPv4.

По умолчанию маршрутизация пакетов IPv6 на маршрутизаторе отключена, и ее нужно включить при помощи команды **no shutdown**.

Для того чтобы разрешить использование EIGRP на конкретном интерфейсе, нужно использовать команду **ipv6 eigrp** (сокращенно — **ipv6 ei**), которая имеет следующий формат:

```
ipv6 eigrp autonomous-system-number
```

где *autonomous-system-number* — номер автономной системы.

Включить на интерфейсе процесс OSPF можно с помощью командой **router ospf** (сокращенно - **ro ospf**), которая имеет следующий формат:

```
ipv6 ospf process-id area area-id
```

где *process-id* — идентификатор процесса OSPF (целое число в диапазоне от 1 до 65535), *area-id* — номер зоны OSPF, к которой относится интерфейс.

Прежде чем включать процесс OSPF, нужно вначале разрешить на интерфейсе использование протокола IPv6 с помощью команды **ipv6 enable**. Например, чтобы включить на интерфейсе FastEthernet 1/0 процесс OSPF с идентификатором 123 и прикрепить его к зоне 0, нужно подать последовательность команд:

```
ipv6 unicast-routing
interface fastethernet 1/0
ipv6 enable
ipv6 ospf 123 area 0
```

14.4. Команды для проверки правильности настройки

Сокращенную справку о состоянии интерфейсов можно получить с помощью команды **show ipv6 interfaces brief** (сокращенно — **sh ipv6 int br**).

Получить информацию об используемых протоколах маршрутизации можно при помощи команды **show ipv6 protocols**.

Просмотреть содержимое таблицы маршрутизации для IPv6 можно при помощи команды **show ipv6 route**.

Получить информацию о процессах протокола RIP можно при помощи команды **show ipv6 rip**.

Для протокола EIGRP имеются следующие специфические команды:

- **show ipv6 eigrp neighbors** — получить информацию о соседях;
- **show ipv6 eigrp route** — получить информацию о маршрутах;
- **show ipv6 eigrp topology** — получить информацию о топологии связей.
- Для протокола OSPF имеются следующие специфические команды:
- **show ipv6 ospf** — получить информацию о процессах протокола OSPF;
- **show ipv6 ospf interface** — получить информацию об интерфейсах, на которых запущен OSPF;
- **show ipv6 ospf neighbor** — получить информацию о соседях.

14.5.1. Настройка сети с двумя маршрутизаторами

В этом упражнении мы настроим компьютерную сеть с двумя маршрутизаторами, показанную на рисунке 14.3, используя протокол EIGRP.

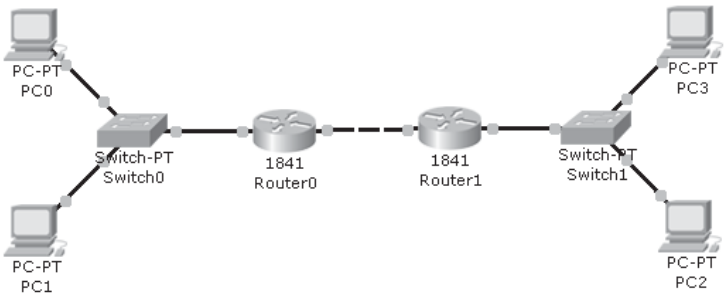

Рис. 14.3. Компьютерная сеть двумя маршрутизаторами

Выполните в следующие действия:

1. Запустите программу Cisco Packet Tracer.
2. Разместите в рабочем пространстве маршрутизаторы Router0 и Router1 типа 1841, коммутаторы Switch0 и Switch1 типа Switch-PT и компьютеры PC0–PC3 так, как показано на рисунке 14.3.
3. Соедините между собой устройства, размещенные в рабочем пространстве:
   3.1. Присоедините прямым кабелем компьютер PC0 к порту FastEthernet0/1 коммутатора Switch0.
   3.2. Присоедините прямым кабелем компьютер PC1 к порту FastEthernet1/1 коммутатора Switch0.
   3.3. Присоедините прямым кабелем компьютер PC2 к порту FastEthernet0/1 коммутатора Switch1.
   3.4. Присоедините прямым кабелем компьютер PC3 к порту FastEthernet1/1 коммутатора Switch1.
   3.5. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch0 к порту FastEthernet0/0 маршрутизатора Router0.
   3.6. Присоедините прямым кабелем порт FastEthernet2/1 коммутатора Switch1 к порту FastEthernet0/0 маршрутизатора Router1.
   3.7. Присоедините перекрестным кабелем порт FastEthernet0/1 маршрутизатора Router0 к порту FastEthernet0/1 маршрутизатора Router1.
4. Настройте компьютер PC0:
   4.1. Выберите в рабочем пространстве компьютер PC0.
   4.2. В окне PC0 выберите вкладку Config.
   4.3. В области настройки глобальных параметров Global Settings выберите статический режим настройки параметров IPv6 и задайте адрес шлюза IPv6 **FE80::1**.
   4.4. На вкладке Config нажмите кнопку FastEthernet.
   4.5. Для адаптера сети Fast Ethernet выберите использование статической конфигурации IPv6 и задайте адрес **2001:DB8:ABCD:A::3**.
   4.6. Закройте окно PC0.
5. Настройте компьютер PC1: задайте IPv6-адрес **2001:DB8:ABCD:A::4** и адрес шлюза **FE80::1**.
6. Настройте компьютер PC2: задайте IPv6-адрес **2001:DB8:ABCD:B::3** и адрес шлюза **FE80::2**.
7. Настройте компьютер PC3: задайте IPv6-адрес **2001:DB8:ABCD:B::4** и адрес шлюза **FE80::2**.

8. Настройте маршрутизатор Router0, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router eigrp 1
Router(config-rtr)#router-id 1.1.1.1
Router(config-rtr)#no shutdown
Router(config-rtr)#exit
Router(config)#int f0/0
Router(config-if)#ipv6 address 2001:DB8:ABCD:A::1/64
Router(config-if)#ipv6 address FE80::1 link-local
Router(config-if)#ipv6 eigrp 1
Router(config-if)#no shut
Router(config-if)#int f0/1
Router(config-if)#ipv6 ad 2001:DB8:ABCD:C::1/64
Router(config-if)#ipv6 ad FE80::1 link-local
Router(config-if)#ipv6 eigrp 1
Router(config-if)#no shut
Router(config-if)#end
Router#exit
```

9. Настройте маршрутизатор Router1, для чего введите на вкладке CLI последовательность команд:

```
Router>en
Router#conf t
Router(config)#ipv6 uni
Router(config)#ipv6 router eigrp 1
Router(config-rtr)#ro 2.2.2.2
Router(config-rtr)#no shut
Router(config-rtr)#exit
Router(config)#int f0/0
Router(config-if)#ipv6 ad 2001:DB8:ABCD:B::1/64
Router(config-if)#ipv6 ad FE80::2 link-local
Router(config-if)#ipv6 eigrp 1
Router(config-if)#no shut
Router(config-if)#int f0/1
Router(config-if)#ipv6 ad 2001:DB8:ABCD:C::2/64
Router(config-if)#ipv6 ad FE80::2 link-local
Router(config-if)#ipv6 eigrp 1
Router(config-if)#no shut
Router(config-if)#end
Router#exit
```

10. Нажмите кнопку Fast Forward Time, размещенную под рабочим пространством, чтобы временно ускорить процесс моделирования.
11. На правой панели инструментов нажмите кнопку Inspect, а затем наведите лупу на маршрутизатор Router0, щелкните левой кнопкой мыши, чтобы вызвать меню, и

выберете в меню пункт IPv6 Routing Table, для того чтобы просмотреть таблицу маршрутизации. Таблица должна выглядеть так, как показано на рисунке 14.4.

12. Аналогичным образом проверьте таблицу маршрутизации IPv6 на маршрутизаторе Router1.
13. Проверьте настройку маршрутизаторов, используя команды **show ipv6 interfaces brief**, **show ipv6 protocols**, **show ipv6 route**, **show ipv6 eigrp neighbors**, **show ipv6 eigrp route** и **show ipv6 eigrp topology**.
14. Переключите Cisco Packet Tracer в режим Simulation.
15. В пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC1. Если операция завершилась неудачно, то попробуйте повторить передачу пакета.
16. В пошаговом режиме передайте простой пакет с компьютера PC2 на компьютер PC3.
17. В пошаговом режиме передайте простой пакет с компьютера PC0 на компьютер PC3.
18. Сохраните модель сети в файле с именем **net_14_5_1**.
19. Завершите работу с программой Cisco Packet Tracer.

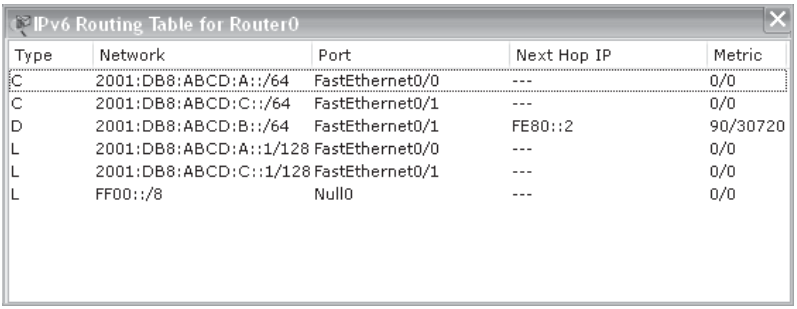

Рис. 14.4. Таблица маршрутизации для протокола IPv6

14.6. Задание для самостоятельной работы

Настройте показанную на рисунке 14.5 компьютерную сеть, используя протокол EIGRP.

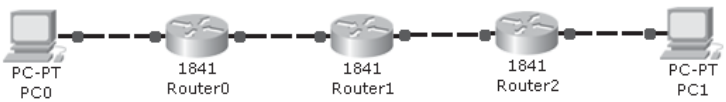

Рис. 14.5. Задание для самостоятельной работы

ЗАКЛЮЧЕНИЕ

Изучив материал данного пособия, вы самостоятельно можете строить модели простых компьютерных сетей.

Не прекращайте тренироваться после прохождения курсов Сетевой Академии Cisco и получения сертификата, так как без периодических тренировок знания и навыки, приобретенные в процессе обучения, постепенно утрачиваются.

Попробуйте воспроизвести в среде Cisco Packet Tracer лабораторные работы по компьютерным сетям, которые вы выполняли на реальной аппаратуре Cisco. Придумывайте собственные модели сетей. Постарайтесь воспринимать тренировки на симуляторе Cisco Packet Tracer не как скучную работу, а как игру.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Бони Дж. Руководство по Cisco IOS. – СПб. : Питер, 2008. – 784 с. : ил.
2. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. – Пер. с англ. – СПб. : Символ Плюс, 2003. – 512 с. : ил.
3. Кулябов Д. С., Королькова А. В. Архитектура и принципы построения современных сетей и систем телекоммуникаций: Учеб. пособие. – М. : РУДН, 2008. – 281 с. : ил.
4. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco, 2-е изд. : Пер. с англ. – М. : Издательский дом «Вильямс», 2001. – 368 с. : ил.
5. Локальные вычислительные сети: методические указания к практическим занятиям / В. Г. Кулаков. – М. : РГУИТП, 2012. – 62 с.
6. Локальные вычислительные сети. Часть 2: занятия 10–13: методические указания к практическим занятиям / В. Г. Кулаков. – М. : РГУИТП, 2013. – 46 с.
7. Локальные сети: методические указания к лабораторным работам по курсу «Локальные вычислительные сети» / В. Г. Кулаков. – М. : РГУИТП, 2012. – 92 с.
8. Макарова Н. В., Волков В. Б. Информатика: Учебник для вузов. – СПб.: Питер, 2011. – 576 с. : ил.
9. Моделирование информационных сетей: методические указания к лабораторным работам по курсу «Глобальные сети передачи данных» / В. Г. Кулаков. – М.: РГУИТП, 2012. – 49 с.
10. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640–822, 3-е изд. : Пер. с англ. – М. : ООО «И. Д. Вильямс», 2013. – 720 с. : ил.
11. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640–816, 3-е изд. : Пер. с англ. – М. : ООО «И. Д. Вильямс», 2013. – 752 с. : ил.
12. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб. : Питер, 2010. – 944 с. : ил.
13. Основы организации сетей Cisco, том 1. : Пер. с англ. – М. : Издательский дом «Вильямс», 2002. – 512 с. : ил.
14. Пакет К., Тир Д. Создание масштабируемых сетей Cisco. : Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 792 с. : ил.
15. Хилл Б. Полный справочник по Cisco. – М. : Издательский дом «Вильямс», 2004. – 1079 с. : ил.
16. Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию маршрутизаторов Catalist. : Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 560 с. : ил.
17. Чеппел Л., Титтел Э. TCP/IP. Учебный курс : Пер. с англ. – СПб. : БХВ-Петербург, 2003. – 976 с. : ил.
18. Шеннон Р. Имитационное моделирование систем: искусство и наука. – М. : Мир, 1978. – 418 с. : ил.
19. TCP/IP. Для профессионалов. 3-е изд. / Т. Паркер, К. Сиян. – СПб. : Питер, 2004. – 859 с. : ил.
20. Cisco IOS Configuration Fundamentals Command Reference. – Cisco Systems, Inc., 2010.
21. Cisco IOS Interface Command Reference. Release 12.2. – Cisco Systems, Inc., 2005.
22. Cisco IOS LAN Switching Command Reference. Release 12.4. – Cisco Systems, Inc., 2006.

23. Cisco IOS IP Addressing Services Command Reference. – Cisco Systems, Inc., 2008.
24. Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols. Release 12.2. – Cisco Systems, Inc., 2005.
25. Cisco IOS IP Routing: EIGRP Command Reference. – Cisco Systems, Inc., 2010.
26. Cisco IOS IP Routing Protocols Command Reference. Release 12.4. – Cisco Systems, Inc., 2006.
27. Cisco IOS Wide-Area Networking Command Reference. – Cisco Systems, Inc., 2011.

Учебное издание

Кулаков Владимир Геннадьевич

Леохин Юрий Львович

Моделирование компьютерных сетей в симуляторе Cisco Packet Tracer 6

Учебное пособие

Негосударственное образовательное учреждение
высшего образования
Московский технологический институт

Подписано в печать 31.08.2016. Формат 60×84 1/16.
Усл. печ. л 10,35. Тираж 500 экз.
Отпечатано в типографии «Вишневый пирог»
115114, Москва, 2-й Кожевнический пер, д.12.
Заказ .