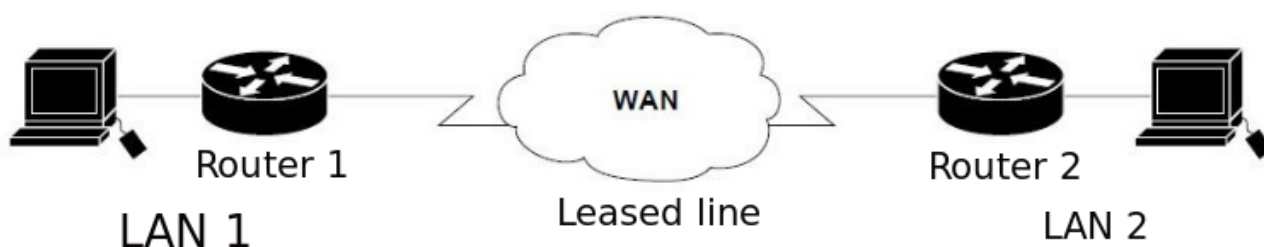


### Лабораторная работа №3. Проектирование WAN сетей на CISCO PACKET TRACER. Статическая и динамическая маршрутизация

Глобальные сети - **World Area Networks (WAN)**. Объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах. Охватывает большие территории и включает в себя большое число компьютеров.

#### Принципы построения WAN

Многие глобальные сети построены для конкретной организации и являются закрытыми. Другие, построенные интернет провайдерами, предоставляют соединение из локальной сети организации в интернет. WAN довольно часто построены с использованием выделенных линий (закрытых двусторонних линий между двумя или более локациями, предоставляемых за определенную месячную плату). На каждом конце выделенной линии, роутер соединяет локальную сеть на его стороне со вторым роутером, имеющим собственную локальную сеть. Однако, выделенные линии могут быть очень дорогими. Поэтому вместо них WAN также могут быть построены с использованием менее дорогой схемы передачи пакетов.



Основными используемыми протоколами в глобальных сетях являются TCP/IP, SONET/SDH, MPLS, ATM и Frame relay. Ранее был также широко распространён протокол X.25, который может по праву считаться прародителем Frame relay.

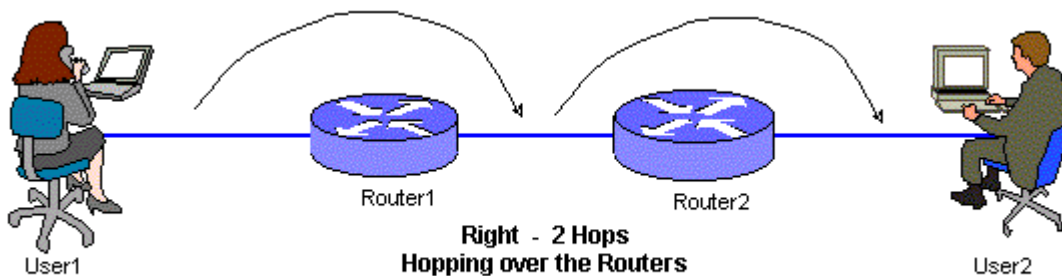
#### Принцип работы глобальных сетей[[править](#)]

Существуют так называемые «операторы связи», которые содержат собственные каналы и арендуют провайдерам доступ к ним. Собственность каждого оператора, включая все локальные сети провайдеров, подключенные к нему, принято называть «автономной системой».

Автономная система – это ряд связанных между собой машин с единой внутренней политикой маршрутизации (**IGP – Internal Gateway Protocol**). Сами автономные системы посредством мощных каналов соединяются между собой, образуя единую сеть Internet. Но невозможно передать данные каждому маршрутизатору обо всех остальных роутерах. Поэтому принято выделять так называемые «пограничные шлюзы» автономной системы. Все шлюзы соединяются по единой магистрали и обмениваются данными посредством внешних протоколов маршрутизации (**EGP – External Gateway Protocol**).

К внутренним протоколам относятся *RIP* и *OSPF*.

Прежде чем описать эти протоколы, введем понятие «хоп», использующееся во многих метриках протоколов. **Хоп** или **транзитный участок** — участок сети между двумя узлами сети, по которому передаются сетевые пакеты. Обычно используется для определения «расстояния» между узлами. Чем больше хопов — тем сложнее путь маршрутизации и тем «дальше» находятся узлы друг от друга. Например, на иллюстрации ниже количество хопов будет равно 2.



## 1. RIP

Протокол RIP (Routing Information Protocol) очень прост и универсален, поэтому поддерживается всеми операционными системами и железными маршрутизаторами. Он относится к классу «дистанционно-векторных» протоколов.

Идея RIP очень проста. Каждый маршрутизатор через определенный интервал времени (30 секунд) отправляет информацию о связях своим соседям. Сосед соотносит их со своей базой и добавляет данные, если они актуальны. Таким образом, все роутеры должны знать обо всех своих сетях. Метрика в RIP совпадает с числом хопов до нужной сети. В случае, если метрика равна 16, сеть считается недоступной. Следовательно, протокол может работать с сетью, в которой максимально число шлюзов менее 16.

Бывают случаи, когда происходят внештатные ситуации, получившие названия «зацикливание» и «счет до бесконечности». Зацикливание происходит после отключения одной из сети, когда сторонний роутер оповестит соседа, что сеть доступна через него (в случае, если сосед не успеет оповестить маршрутизатор о недоступности сети). Таким образом, между шлюзами образуется петля.

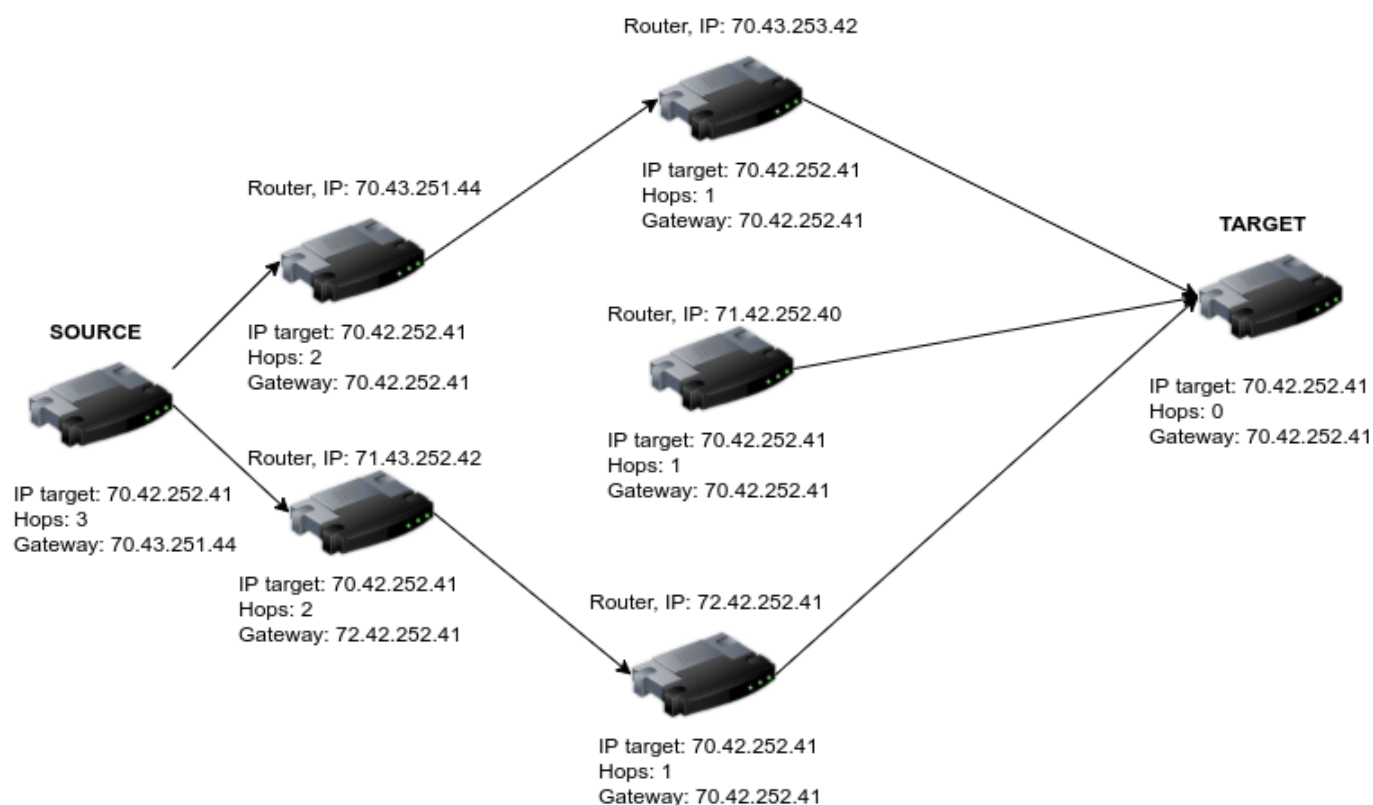
Чтобы избежать петель, вводят два ограничения в протокол RIP. Первое называется «правилом разделения горизонта». Оно гласит, что маршрутизатор А не должен отправлять данные о сети В, маршрутизатору С, если последний ему сообщил о сети В. Иными словами, роутер не шлет информацию о сети соседу, если изначально получил сведения об этой сети от него. Второе ограничение обязывает шлюз изменить метрику маршрута, если ее разослал тот же самый роутер. Отчасти, эти добавления спасают от петель, но не всегда. Бывает, что маршрутизатор получает ложные данные от стороннего шлюза по цепочке.

Счет до бесконечности происходит в результате несвоевременного оповещения станций. При этом ложный маршрут может существовать, пока метрика сети не станет равной 16.

Более формально, алгоритм работает следующим образом: таблица маршрутизации RIP содержит по записи на каждую обслуживаемую машину. Запись должна включать в себя

- IP-адрес места назначения;
- Метрика маршрута (от 1 до 15; число хопов до места назначения);
- IP-адрес ближайшего маршрутизатора (gateway) по пути к месту назначения;
- Таймеры маршрута.

Периодически (через таймаут) маршрутизатор посылает копию своей маршрутной таблицы всем своим соседям-маршрутизаторам, а те обновляют свои таблицы, если находят более короткий маршрут. На иллюстрации показано финальное состояние после выполнения алгоритма поиска пути от **Source** до **Target**:



В процессе алгоритма происходило следующее:

- У **Target** число хопов равно 0, потому что это расстояние до него самого;
- Затем, когда пройдет таймаут, Target пошлет свою таблицу маршрутизации всем соседям — 70.43.253.42, 71.42.252.40 и 72.42.252.41 (пошлют свои таблицы все роутеры, но только для этого нам интересно что будет);
- У этих его соседей изменится оптимальное расстояние — раньше оно было неизвестно, теперь 1;
- Затем каждый из них пошлет свои таблицы своим соседям, у них число хопов станет равно 2;
- На третьем шаге, дело дойдет до **Source**, и мы нашли число хопов для него — это 3.

Также обратите внимание на поле *Gateway* в каждой таблице — благодаря нему можно восстановить весь маршрут.

## 2. OSPF

На смену RIP пришел протокол OSPF, который снимает ограничение в 15 узлов и сводит к минимуму служебный трафик. Он относится к классу протоколов «состояния связей», а его работа складывается в два этапа:

1. Каждый маршрутизатор после включения рассылает информацию по всем своим интерфейсам обо всех своих соседях.
2. После составления полной сетевой картины роутер начинает искать оптимальный маршрут до каждой сети с помощью алгоритма Дейкстры.

Метрика представляет собой уже не число хопов, а пропускную способность канала (время передачи одного бита в 10-наносекундных интервалах). Так, для Ethernet метрика равна десяти, для Fast Ethernet — единице, а для канала 56 Кб/с — 1785. Полная метрика для определенного маршрута является суммой всех промежуточных каналов. При этом OSPF никогда не пропустит пакет через канал в один хоп, если имеется связь, построенная на Fast Ethernet, пусть даже состоящая из 3-4 хопов.

Следует отметить, что OSPF умеет посылать данные сразу по нескольким каналам, тем самым, уменьшая нагрузку на сеть. Однако в этом случае действует ограничение по метрике. Подробно это здесь описывать не будем.

## 3. BGP

На текущий момент BGP зарегистрирован под четвертой версией и не имеет конкурентов. Общая схема работы BGP такова. BGP-маршрутизаторы соседних АС, решившие обмениваться

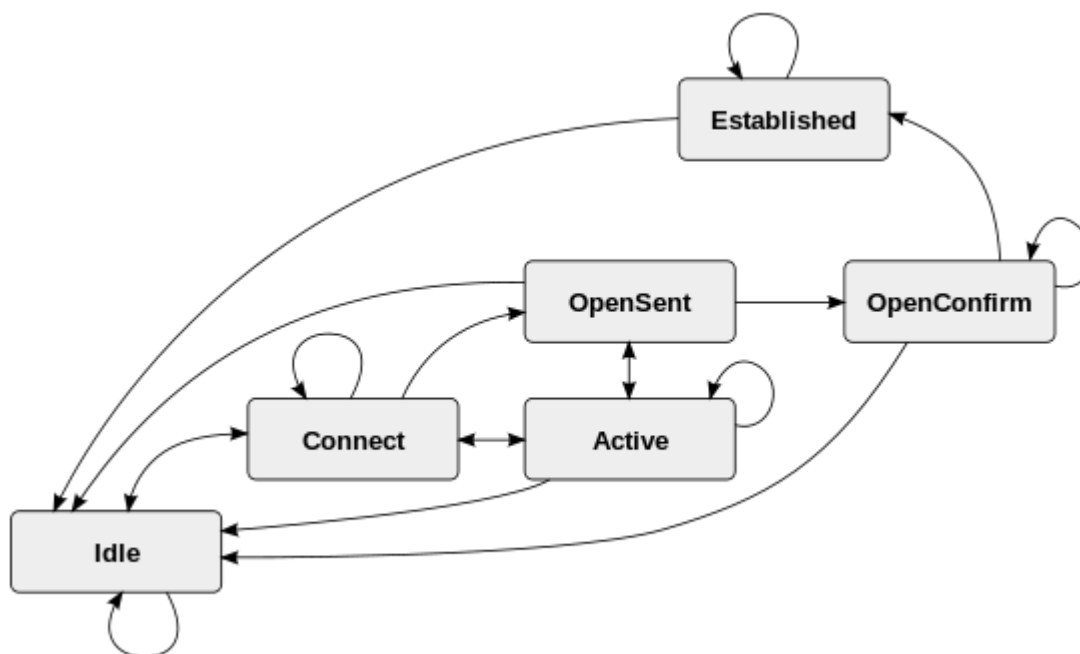
маршрутной информацией, устанавливают между собой соединения по протоколу BGP и становятся BGP-соседями

Далее BGP использует подход под названием *path vector*, являющийся развитием дистанционно-векторного подхода. BGP-соседи рассылают друг другу векторы путей (path vectors). Вектор путей, в отличие от вектора расстояний, содержит не просто адрес сети и расстояние до нее, а адрес сети и список атрибутов (path attributes), описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть.

#### Типы BGP-сообщений

- *OPEN* - посылается после установления TCP-соединения. Ответом на OPEN является сообщение *KEEPALIVE*, если вторая сторона согласна стать BGP-соседом; иначе посылается сообщение *NOTIFICATION* с кодом, поясняющим причину отказа, и соединение разрывается.
- *KEEPALIVE* - сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности открытого соединения: для этого BGP-соседи обмениваются *KEEPALIVE*-сообщениями через определенные интервалы времени.
- *UPDATE* - сообщение предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений *UPDATE* пересылаются все маршруты, которые маршрутизатор хочет объявить соседу (full update), после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления (partial update).
- *NOTIFICATION* - сообщение этого типа используется для информирования соседа о причине закрытия соединения. После отправления этого сообщения BGP-соединение закрывается.

Примерная схема работы сообщений в BGP выглядит так:



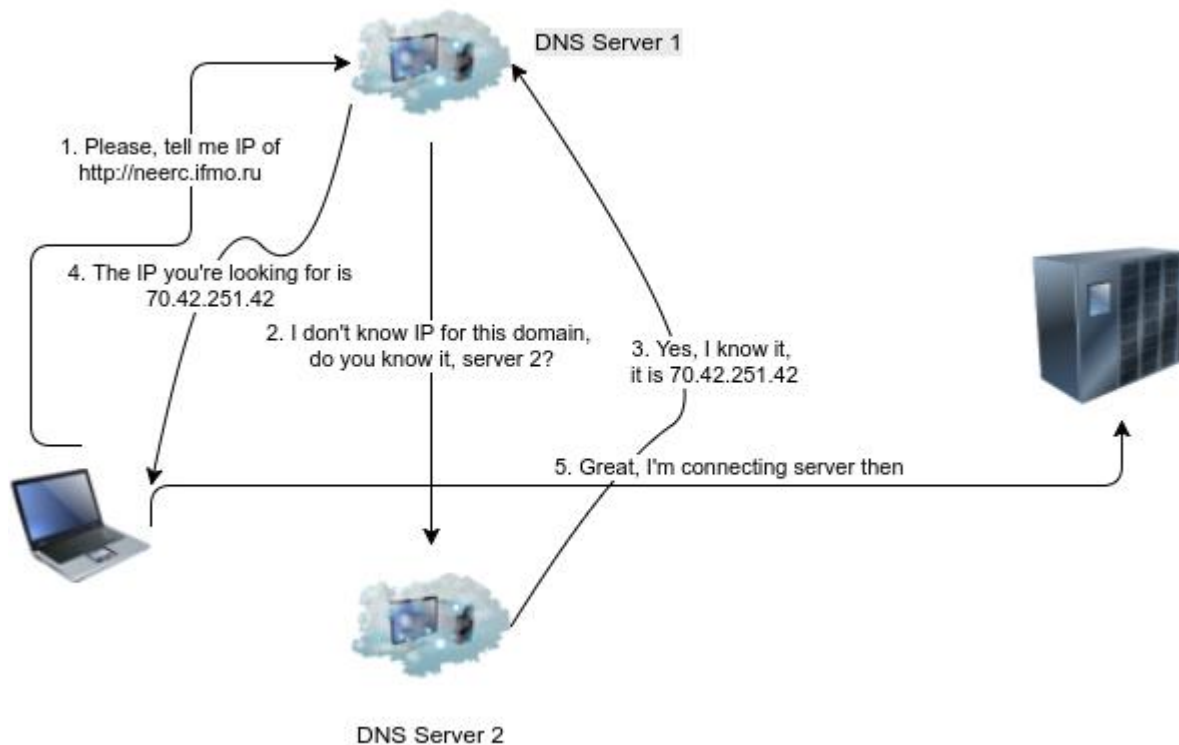
При выборе протокола маршрутизации необходимо взвесить все «за» и «против». С одной стороны, громоздкий OSPF. С другой — никто не мешает использовать RIP второй версии, который научился понимать маски подсети и аутентификацию, чего не умел его предшественник.

#### Принцип работы глобальных сетей: пример

Представим, что мы сидим в Ташкенте и хотим подключиться к серверу, который находится в Санкт-Петербурге по адресу <http://neerc.ifmo.ru>. Что примерно будет происходить, когда мы наберем адрес и нажмем Enter?

В первую очередь в ход идет DNS-сервер: он транслирует сначала поддомены (neerc), обращаясь к локальному провайдеру, затем транслирует основной домен (ifmo.ru), обращаясь в глобальную сеть. Получив IP-адрес сервера, мы знаем, куда надо подключаться. Наш IP тоже известен, поэтому мы спокойно подключаемся, создаем соединение и передаем/получаем нужную информацию.

Возможное примерное развитие событий представлено на картинке. DNS-серверов обычно несколько, в данном случае рассмотрен вариант двух:



Маршрутизация заключается в пересылке данных между сетями. В отличие от коммутаторов, маршрутизатор принимает и пересылает пакеты данных, ориентируясь на IP адреса. Маршрутизатор считывает адрес назначения прибывшего пакета и переправляет его в соответствии с информацией, хранящейся в таблице маршрутизации.

Отдельные записи таблицы маршрутизации называются маршрутами. Существуют следующие типы маршрутов:

- маршрут к сети – определяет маршрут к определенной сети;
- маршрут по умолчанию – один маршрут, по которому отправляются все пакеты, чей адрес не совпадает ни с одним из маршрутов таблицы.

Маршрутизация бывает статическая и динамическая. Для *статической маршрутизации* необходимы таблицы маршрутизации, которые создает сетевой администратор; в них указываются фиксированные (статические) маршруты между любыми двумя маршрутизаторами. Эту информацию администратор вводит в таблицы вручную. Администратор сети также отвечает за ручное обновление таблиц в случае отказа каких-либо сетевых устройств. Маршрутизатор, работающий со статическими таблицами, может определить факт неработоспособности какого-либо сетевого канала, однако он не может автоматически изменить пути передачи пакетов без вмешательства со стороны администратора.

*Динамическая маршрутизация* выполняется независимо от сетевого администратора. Протоколы динамической маршрутизации позволяют маршрутизаторам автоматически выполнять следующие операции:

- находить другие доступные маршрутизаторы в остальных сетевых сегментах;
- определять с помощью метрик кратчайшие маршруты к другим сетям;
- определять моменты, когда сетевой путь к некоторому маршрутизатору недоступен или не может использоваться;
- применять метрики для перестройки наилучших маршрутов, когда некоторый сетевой путь становится недоступным;
- повторно находить маршрутизатор и сетевой путь после устранения сетевой проблемы в этом пути.

## 5. Пример выполнения задания.

Задание: Построить локальную сеть, состоящую из сегмента на основе коммутатора из 5 компьютеров и сервера. Коммутатор соединен с маршрутизатором, к которому также подключен сервер. Необходимо задать статические IP адреса сетевым интерфейсам маршрутизаторов, локальных компьютеров и серверов. Установить на маршрутизаторах пароли для доступа к привилегированному режиму. Настроить маршрутизацию по протоколу RIP. Добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети.

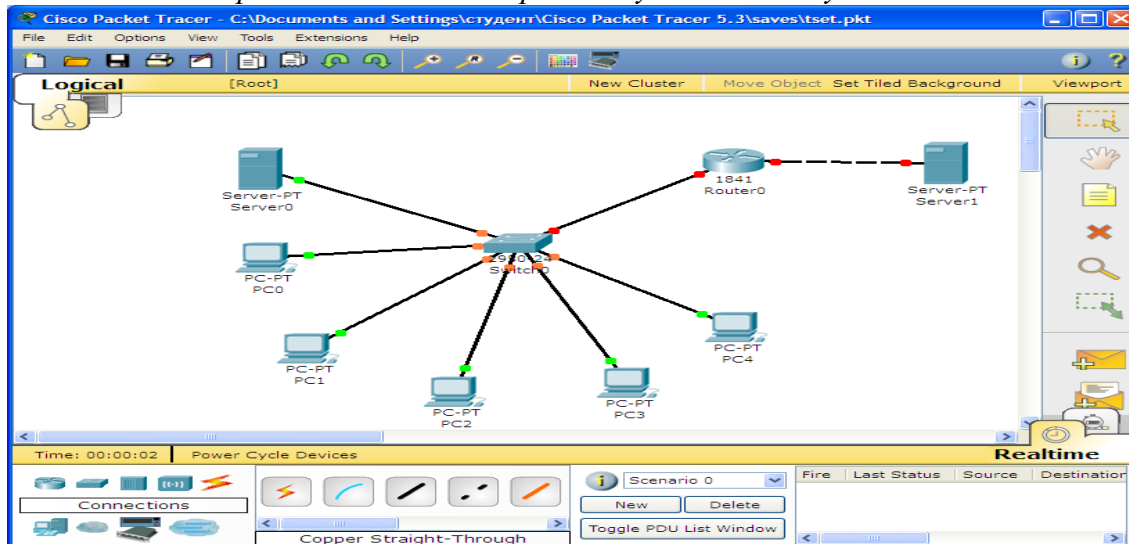


Рис. 8. Рабочее поле

Зададим ip-адреса узлам сегмента в диапазоне 192.168.0.x, а серверу, подключенному к маршрутизатору – 192.168.1.1. Маска подсети – 255.255.255.0. (Рис. 9).

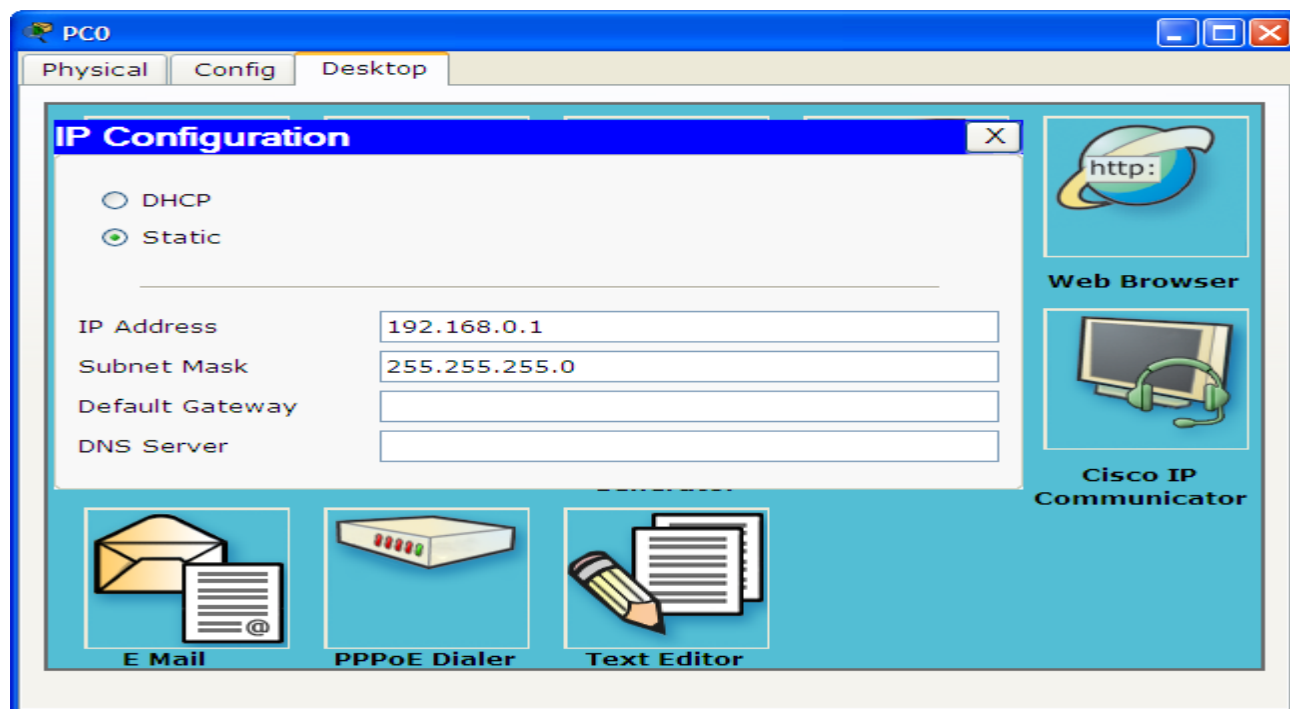


Рис. 9. IP конфигурация рабочей станции.

Зададим соответствующие ip адреса на интерфейсах маршрутизатора и включим эти порты. (Рис. 10).



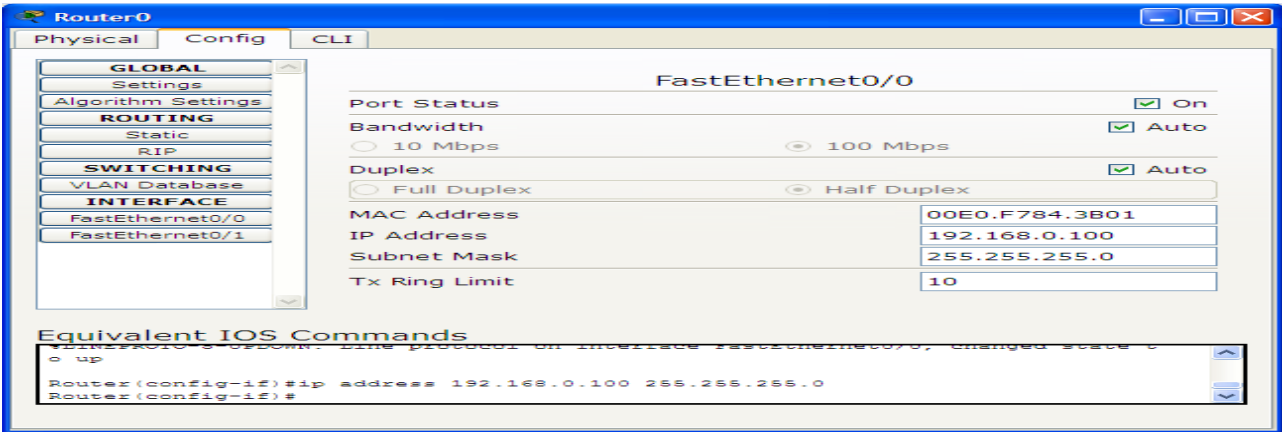


Рис. 10. IP конфигурация маршрутизатора.  
Зайдем в Command Line Interface маршрутизатора и с помощью команды enable secret зададим пароль для доступа в привилегированный режим и сохраним конфигурацию. (Рис. 11).

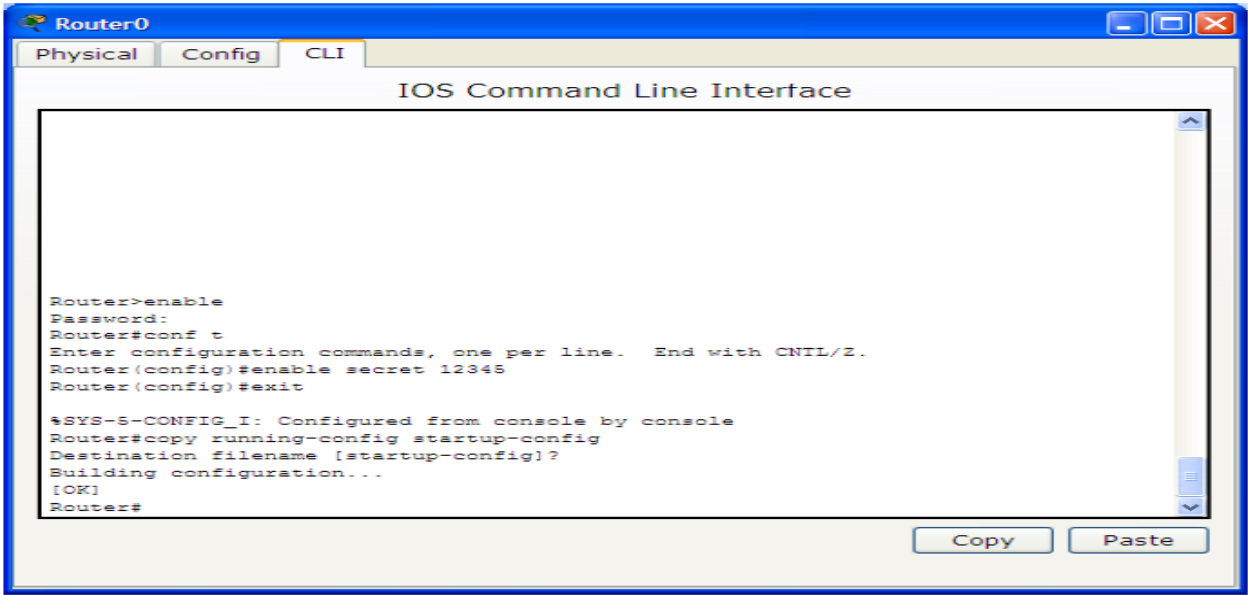


Рис. 11. Работа в Command Line Interface.

Для настройки маршрутизации по протоколу RIP откроем вкладку Config в окне свойств маршрутизатора и выберем пункт RIP. Зададим там адреса всех подсетей, которым разрешено общение. (Рис. 12).

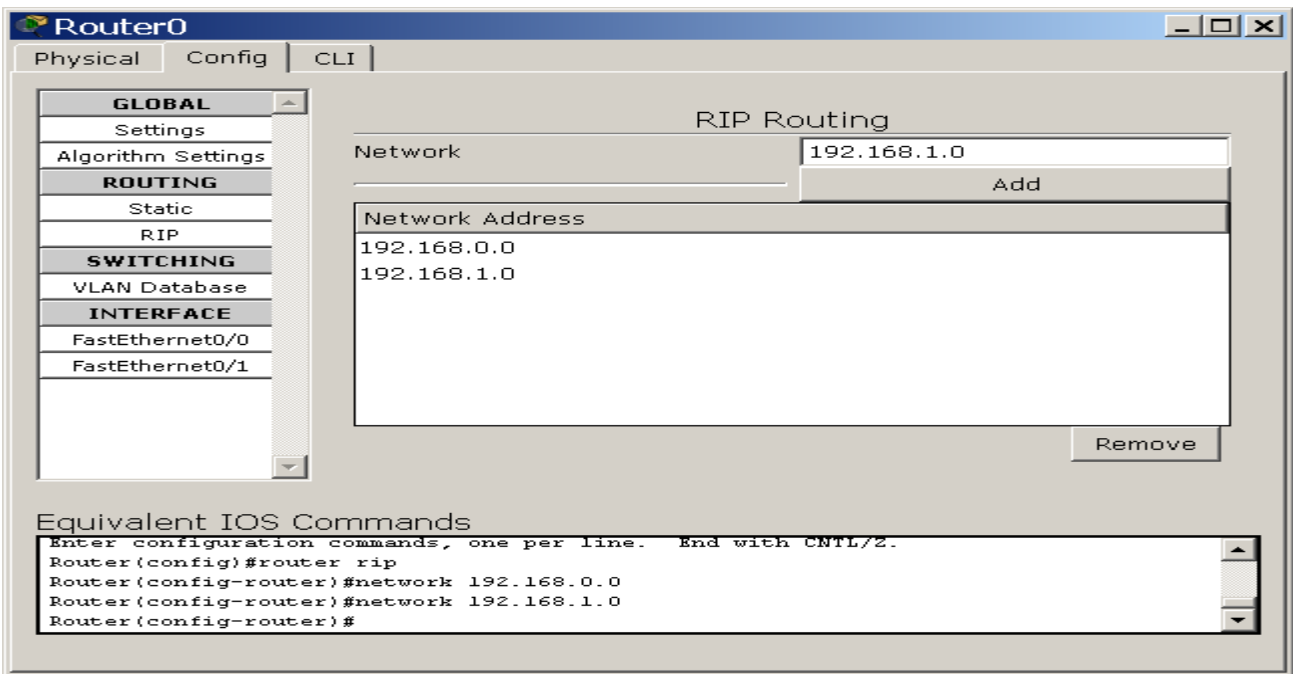


Рис. 12. Настройка маршрутизации по протоколу RIP.

Проверяем доступность рабочих станций друг для друга. Для этого в правом столбце выбираем инструмент Add simple PDU и выбираем станцию-отправитель и станцию-получатель. Убеждаемся, что передача завершена успешно. (Рис. 13).

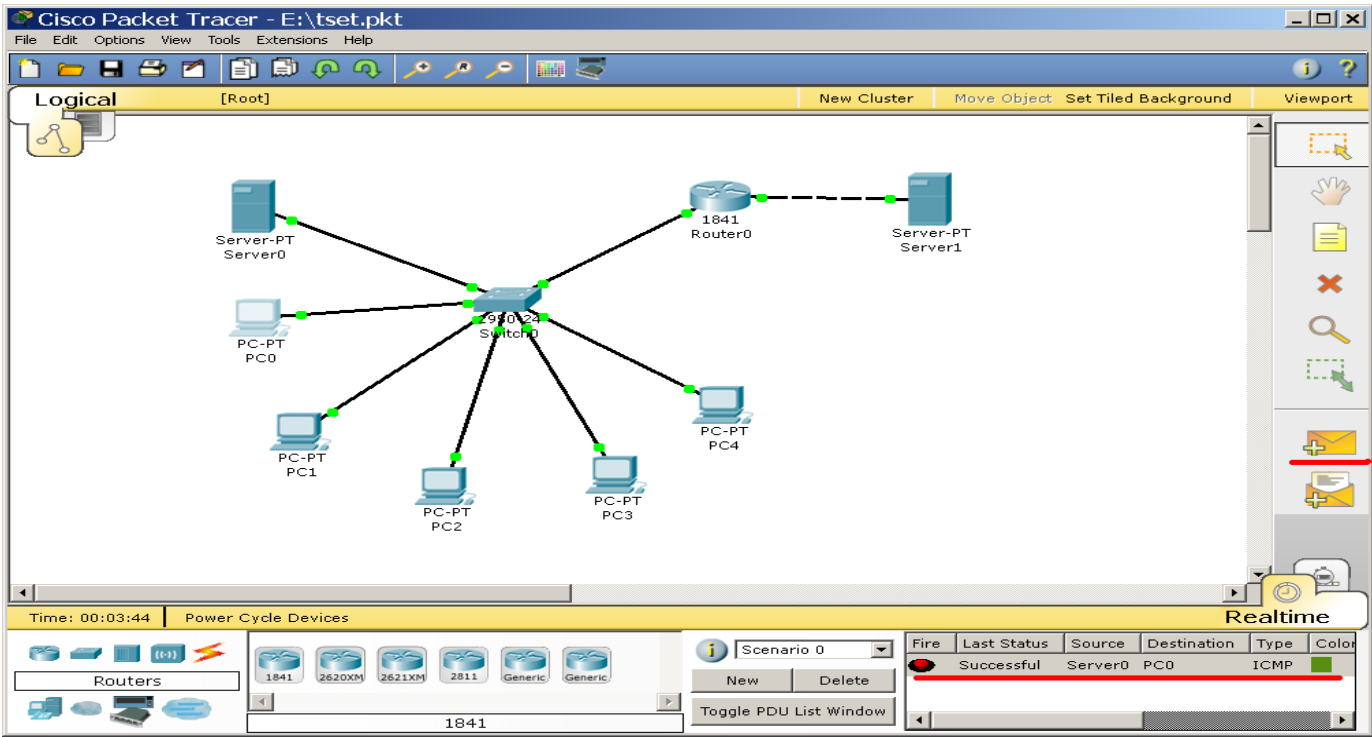


Рис. 13. Проверка доступности узлов в сети.

**Задание 1. Статическая маршрутизация.**

Построить сеть из трех сегментов, каждый из которых состоит из С, D и Е рабочих станций соответственно. Каждый сегмент построен на базе коммутатора, и каждый коммутатор подключен к отдельному маршрутизатору. Шлюзом для каждого сегмента служит соответствующий маршрутизатор. Маршрутизаторы соединены между собой с помощью интерфейса DTE. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов и локальных компьютеров. Задать параметр Clock Rate на маршрутизаторах. Установить на маршрутизаторах пароли для доступа к привилегированному режиму. Настроить статическую маршрутизацию и добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети.

**Задание 2. Динамическое распределение IP-адресов и DNS.**

Построить сеть, состоящую из двух сегментов на основе коммутаторов. Сегмент №1 содержит В рабочих станций, сегмент №2 – С рабочих станций и сервер. Маршрутизатор является шлюзом. Сегменты соединены маршрутизатором. В первом сегменте IP адреса раздаются маршрутизатором динамически в диапазоне 192.168.F.x, где F выбирается согласно варианту, а x — произвольное число, во втором IP адреса заданы статически.

Расставляем на рабочем поле необходимые узлы, используя браузер в нижней части окна (рис. 8). Соединяем узлы в соответствии с заданием с помощью витой пары. Сервер с маршрутизатором соединяется кросс-овером. Соединения, обозначенные зеленым цветом указывают, что они активны, оранжевым – что они на стадии подключения, красным – не рабочие.

Настроить маршрутизацию по протоколу RIP. Сервер является DNS и веб-сервером. Настроить на сервере веб-страницу произвольного формата. Добиться возможности пересылки данных по протоколу ICMP между всеми объектами сети. Добиться просмотра веб-страницы с сервера во встроенных браузерах рабочих станций.



**Задавать** ip-адреса узлам сегмента в диапазоне 192.168.(номер своего варианта по лмс).х, а серверу, подключенному к маршрутизатору – 192.168.1.1. Маска подсети – 255.255.255.0. (Рис. 9).

## **6. Контрольные вопросы.**

- Сетевое оборудование и его функции.
- стек протоколов TCP/IP.
- Отличие между различными стандартами сетей Ethernet.
- Формат кадров в сети Ethernet.
- Сети wi-fi – основные стандарты и принципы работы.
- Назначение шлюза.
- Маршрутизация.
- Эталонная модель OSI/ISO.