**Курс:\_\_\_3\_\_\_\_\_\_\_, группа(ы)\_\_\_\_ПКС\_179\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Дисциплина (МДК) МДК 02.01.«Инфокоммуникационные системы и сети»\_\_\_\_\_\_\_\_**

**ФИО преподавателя\_\_\_Булиль К.В.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Программу для работы можно получить по ссылке <https://yadi.sk/d/jcqhS38RV2ar4g>  
Программа запуска Cisco Packet Tracer 5.3.2\bin\PacketTracer5.exe

Результаты с **save.pkt** высылать на почту [miron.sulejman@yandex.ru](mailto:miron.sulejman@yandex.ru) к 26.03.2020

**Тема: Принцип передачи данных . Маршрутизация и Коммутация.**

**Динамическая маршрутизация на протоколах RIP и EIGRP**

***Маршрутизация*** - процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. *Динамическая маршрутизация* может быть осуществлена с использованием одного и более протоколов (*RIP* v2, *OSPF* и др.).

**Новый термин**

***Динамическая маршрутизация***— вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP).

Каждый *протокол маршрутизации* использует свою систему оценки маршрутов (*метрику*). *Маршрут* к сетям назначения строится на основе таких критериев как

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

Маршрутизаторы обмениваются друг с другом информацией о маршрутах с помощью служебных пакетов по протоколу *UDP*. Такой обмен информации увеличивает наличие дополнительного трафика в сети и нагрузку на эту *сеть*. Возможна также ситуация, при которой таблицы маршрутизации на роутерах не успевают согласоваться между собой, что может повлечь появление ошибочных маршрутов и потерю данных.

Протоколы маршрутизации делятся на три типа:

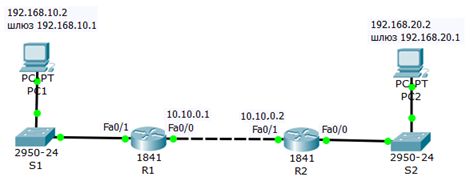
* Дистанционно векторные протоколы (RIP)
* Протоколы с отслеживанием состояния каналов (OSPF)
* Смешанные протоколы (EIGRP)
* И др.

**Протокол RIP**

*RIP* — протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути *алгоритм* Беллмана-Форда. *Алгоритм* маршрутизации *RIP*- один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в *сеть* свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст *адрес*. Максимальное количество "хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (*метрика* 15). Ограничение в 15 хопов не дает применять *RIP* в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышена *безопасность* за счет введения дополнительной маршрутной информации. Принцип дистанционно-векторного протокола: каждый *маршрутизатор*, использующий протокол *RIP* периодически широковещательно рассылает своим соседям специальный пакет-*вектор*, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. *Маршрутизатор* получивший такой *вектор*, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет *вектор* информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный *вектор* *маршрутизатор* рассылает всем своим соседям. *Маршрутизатор* выбирает из нескольких альтернативных маршрутов *маршрут* с наименьшим значением метрики, а *маршрутизатор*, передавший информацию о таком маршруте помечается как следующий (*next* *hop*). Протокол непригоден для работы в больших сетях, так как засоряет *сеть* интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами *EIGRP* и *OSPF*.

**Практическая работа 8-1. Настройка протокола RIP версии 2 для сети из шести устройств**

Наша задача – настроить маршрутизацию на схеме, представленной на [рис. 8.1](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.1).



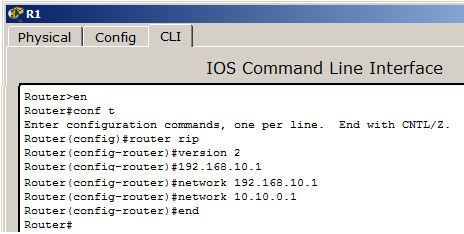
**Рис. 8.1.**Схема сети

**Примечание**

При настройке сети не забывайте включать порты.

**Настройка протокола RIP на маршрутизаторе R1**

Войдите в конфигурации в консоль роутера и выполните следующие настройки ([рис. 8.2](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.2)).



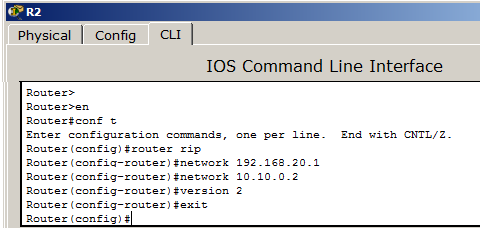
**Рис. 8.2.**Настройка протокола RIPv2 на маршрутизаторе Router1

**Примечание**

**Router(config)#router rip** (Вход в режим конфигурирования протокола RIP). **Router(config-router)#network 192.168.10.1** (Подключение клиентской сети к роутеру со стороны коммутатора S1). **Router(config-router)#network 192.168.20.1** (Подключение второй сети, то есть сети между роутерами). **Router(config-router)#version 2** (Задание использования второй версии протокол RIP).

**Настройка протокола RIP на маршрутизаторе R2**

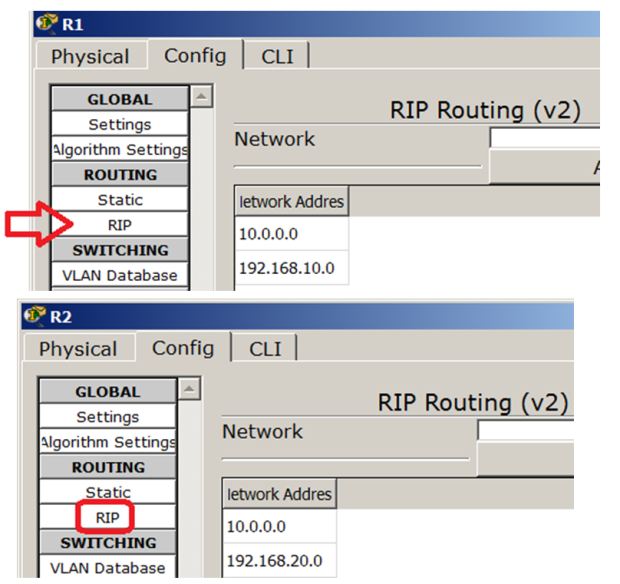
Войдите в конфигурации роутера 2 и выполните следующие настройки ([рис. 8.3](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.3)).



**Рис. 8.3.**Настройка протокола RIPv2 на маршрутизаторе R2

**Проверяем настройки коммутаторов и протокола RIP**

Давайте посмотрим настройки протокола RIPv2 на маршрутизаторах R1 и R2 ([рис. 8.4](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.4)).



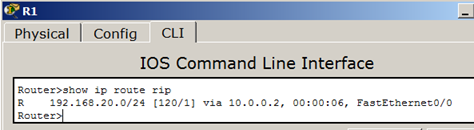
**Рис. 8.4.**Настройки маршрутизаторов R1 и R2

Чтобы убедиться в том, что маршрутизаторы действительно правильно сконфигурированы и работают корректно, просмотрите таблицу RIP роутеров, используя команду: **Router#show ip route rip** ([рис. 8.5](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.5) и [рис. 8.6](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.6)).

Таблица маршрутизации R1

**Рис. 8.5.**Таблица маршрутизации R1

Данная таблица показывает, что к сети 192.168.10.0 есть только один маршрут: через R1(сеть 10.10.0.1).

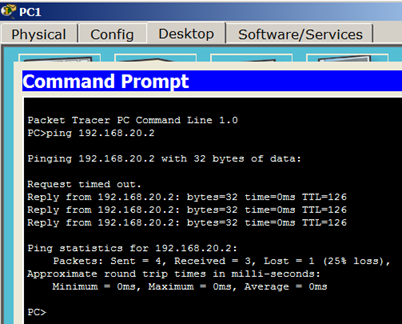


**Рис. 8.6.**Таблицы маршрутизации R2

Данная таблица показывает, что к сети 192.168.20.0 есть только один маршрут: через R2 (сеть 10.10.0.2).

**Проверка связи между PC1 и PC2**

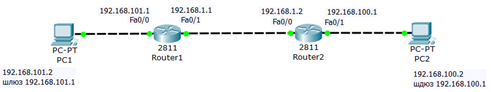
Проверим, что маршрутизация производится верно ([рис. 8.7](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=1#image.8.7)).



**Рис. 8.7.**Пинг с PC1 на PC2

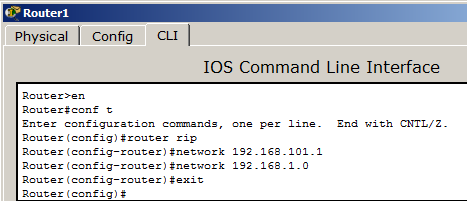
**Практическая работа 8-2. Конфигурирование протокола RIP версии 2 для сети из четырех устройств**

На [рис. 8.8](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.8) представлена *сеть*, на примере которой мы сконфигурируем *протокол маршрутизации* *RIP* v2.



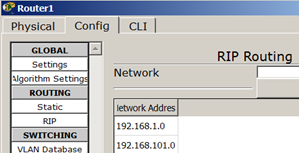
**Рис. 8.8.**Сеть для конфигурации протоколов маршрутизации

Сначала сконфигурируем R1 ([рис. 8.9](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.9)).



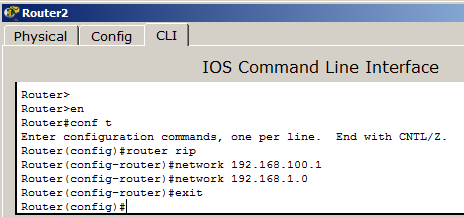
**Рис. 8.9.**Настройка RIP на R1

Смотрим результат на вкладке **Config** ([рис. 8.10](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.10)).



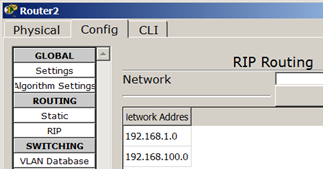
**Рис. 8.10.**Окно R1,вкладка Config

Конфигурируем R2 ([рис. 8.11](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.11)).



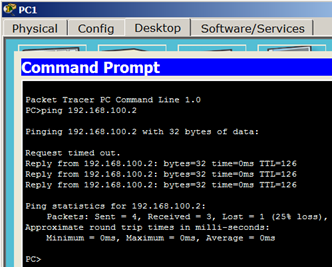
**Рис. 8.11.**Настройка RIP на R2

Наблюдаем результат ([рис. 8.12](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.12)).



**Рис. 8.12.**Окно R2, вкладка Config

Проверяем доступность ПК из разных сетей ([рис. 8.13](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.13)).



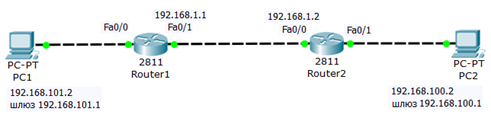
**Рис. 8.13.**Результат маршрутизации по протоколу RIP

**Протокол маршрутизации EIGRP**

Протокол *EIGRP* более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол *OSPF*. Также *EIGRP* имеет более продвинутый *алгоритм* вычисления метрики. В формуле вычисления метрики есть возможность учитывать загруженность и *надежность* интерфейсов на пути пакета. Недостатком протокола *EIGRP* является его ограниченность в его использовании только на оборудовании компании Cisco.

**Практическая работа 8-3. Конфигурирование протокола EIGRP**

Схема сети изображена на [рис. 8.14](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.14).

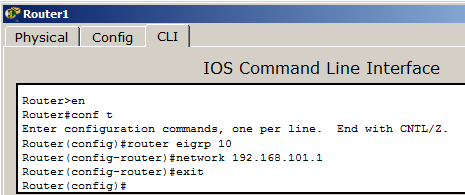


**Рис. 8.14.**Схема для конфигурации протокола EIGRP

Настройка протокола *EIGRP* очень похожа на настройку протокола *RIP*.

**Программирование R1**

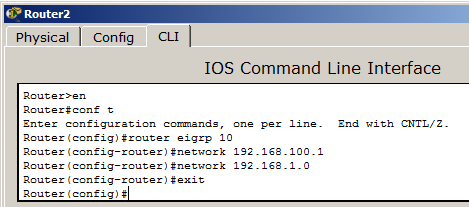
Конфигурируем R1 ([рис. 8.15](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.15)).



**Рис. 8.15.**Конфигурирование R1

**Программирование R2**

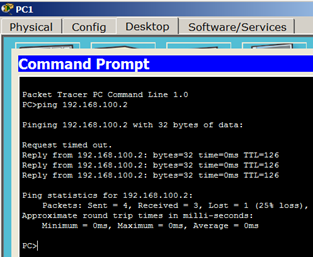
Конфигурируем R2 ([рис. 8.16](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.16)).



**Рис. 8.16.**Конфигурирование R2

**Проверка работы сети**

Проверяем работу маршрутизаторов ([рис. 8.17](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=2#image.8.17)).



**Рис. 8.17.**Результат проверки работоспособности сети

**Протокол OSPF**

*Алгоритм* работы протокола динамической маршрутизации *OSPF* основан на использовании всеми маршрутизаторами единой *базы данных*, описывающей, с какими сетями связан каждый *маршрутизатор*. Описывая каждую *связь*, маршрутизаторы связывают с ней метрику – *значение*, характеризующее "качество" канала связи. Это позволяет маршрутизаторам *OSPF* (в отличие от *RIP*, где все каналы равнозначны) учитывать реальную пропускную способность канала и выявлять наилучшие маршруты. Важной особенностью протокола *OSPF* является то, что используется групповая, а не широковещательная рассылка (как в *RIP*), то есть, нагрузка каналов меньше.

*OSPF* (*Open* Shortest *Path* *First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала link-state (*LSA*). Основан на алгоритме для поиска кратчайшего пути. Отслеживание состояния канала требует отправки объявлений о состоянии канала (*LSA*) на активные интерфейсы всех доступных маршрутизаторов зоны. В этих объявлениях содержится описание всех каналов маршрутизатора и *стоимость* каждого канала. *LSA* сообщения отправляются, только если произошли какие-либо изменения в сети, но раз в 30 минут *LSA* сообщения отправляются в принудительном порядке. Протокол реализует *деление* автономной системы на зоны (areas). Использование зон позволяет снизить нагрузку на *сеть* и процессоры маршрутизаторов и уменьшить размер таблиц маршрутизации.

**Описание работы протокола:**

Все маршрутизаторы обмениваются специальными Hello-пакетами через все интерфейсы, на которых активирован протокол *OSPF*. Таким образом, определяются маршрутизаторы-соседи, разделяющие общий *канал передачи данных*. В дальнейшем hello-пакеты посылаются с интервалом раз в 30 секунд. Маршрутизаторы пытаются перейти в состояние соседства со своими соседями. Переход в данное состояние определяется типом маршрутизаторов и типом сети, по которой происходит обмен hello-пакетами, по зонному признаку. Пара маршрутизаторов в состоянии соседства синхронизирует между собой базу данных состояния каналов. Каждый *маршрутизатор* посылает объявление о состоянии канала своим соседям, а каждый получивший такое объявление записывает информацию в базу данных состояния каналов и рассылает копию объявления другим своим соседям. При рассылке объявлений по зоне, все маршрутизаторы строят идентичную базу данных состояния каналов. Каждый *маршрутизатор* использует *алгоритм* *SPF* для вычисления графа (дерева кратчайшего пути) без петель. Каждый *маршрутизатор* строит собственную маршрутизацию, основываясь на построенном дереве кратчайшего пути.

**Прямая и обратная маска**

В оборудовании **Cisco** иногда приходится использовать обратную маску, то есть не привычную нам **255.255.255.0** (Subnet mask — прямая *маска*), а **0.0.0.255** (Wildcard mask — обратная *маска*). Обратная *маска* используется в листах допуска (*access list*) и при описании сетей в протоколе **OSPF**. Прямая *маска* используется во всех остальных случаях. Отличие масок заключается также в том, что прямая *маска* оперирует сетями, а обратная — хостами. С помощью обратной маски вы можете, например, выделить во всех подсетях хосты с конкретным адресом и разрешить им *доступ* в *Интернет*. Так, как чаше всего в локальных сетях используют адреса типа 192.168.1.0 с маской 255.255.255.0, то самая распространенная Wildcard mask (шаблонная *маска* или обратная *маска*, или инверсная *маска*) - *маска* 0.0.0.255.

**Новый термин**

Шаблонная маска (wildcard mask) — маска, указывающая на количество хостов сети. Является дополнением для маски подсети. Вычисляется по формуле для каждого из октетов маски подсети как 255-маска\_подсети. Например, для сети 192.168.1.0 и маской подсети 255.255.255.242 шаблонная маска будет выглядеть как 0.0.0.13. Шаблонная маска используется в настройке некоторых протоколов маршрутизации, а также является удобным параметром ограничений в списках доступа.

**Расчёт Wildcard mask**

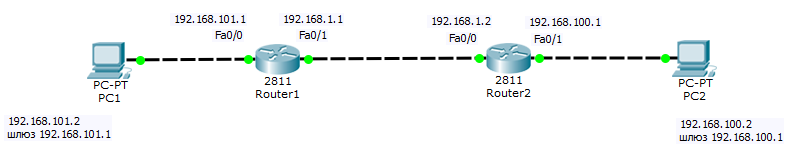
Существует *связь*, между обратной и *прямой* маской: в сумме эти маски по каждому разряду должны составлять 255. Пусть наша *сеть* 192.168.32.0 /28. Рассчитает wildcard mask: *префикс* /28 это 255.255.255.240 или 11111111.11111111.11111111.11110000. Для wildcard mask нам нужны только нули, то есть, 11110000 переводим в десятичное число и считаем: 128/64/32/16/8/4/2/1 это будет 8+4+2+1=15, т.е. наша wildcard mask будет равна 0.0.0.15.

**Самостоятельно**

Дана прямая *маска* **255.255.255.248**. Выполните расчет и докажите, что обратная равна **0.0.0.7**.

**Практическая работа 8-2-1. Пример конфигурирования протокола OSPF для 4-х устройств**

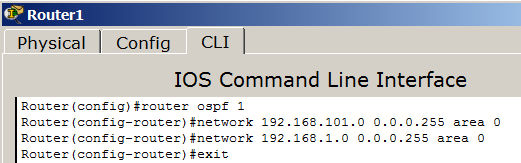
Соберите схему, изображенную на [рис. 8.18](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.18).



**Рис. 8.18.**Схема для конфигурации протокола OSPF

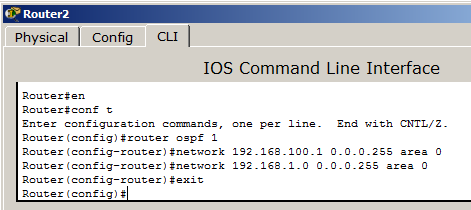
**Настройка роутеров**

Выполним конфигурирование R1 ([рис. 8.19](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.19)).



**Рис. 8.19.**Настройка R1

Теперь выполним настройки R2 ([рис. 8.20](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.20)).



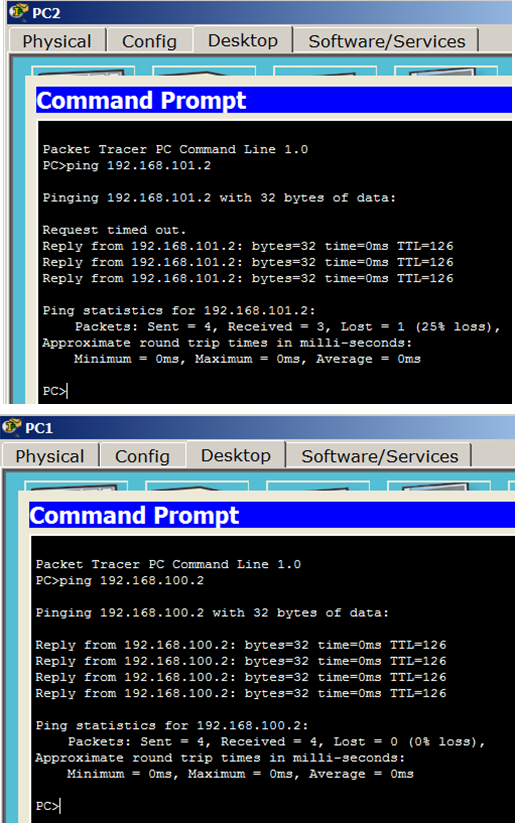
**Рис. 8.20.**Настройка R2

**Совет**

Если вам потребуется в CPT сбросить настройки роутера, то следует выключить его тумблер питания, а затем снова включить.

**Проверка результата**

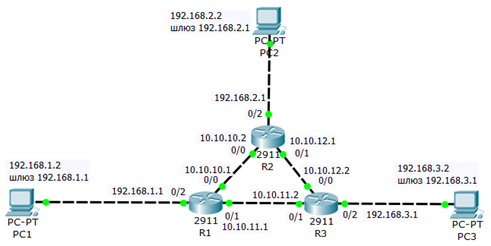
Для проверки маршрутизации пропингуем ПК из разных сетей ([рис. 8.21](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.21)).



**Рис. 8.21.**Результат проверки работоспособности OSPF

**Практическая работа 8-2-2. Настройка маршрутизации по протоколу OSPF для 6 устройств**

Постройте следующую схему ([рис. 8.22](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.22)).



**Рис. 8.22.**Начальная схема сети для нашей работы

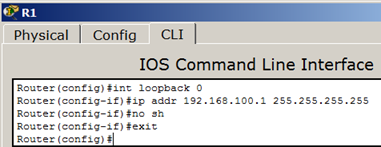
Цель работы – настроить маршрутизацию в данной сети по протоколу *OSPF*.

**Настроим loopback интерфейс на R1**

На R1 настроим программный **loopback интерфейс** — алгоритм, который направляет полученный сигнал (или данные) обратно отправителю ([рис. 8.23](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.23)).

**Примечание**

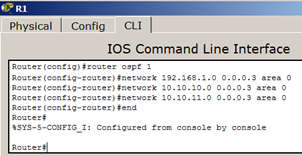
IPv4-адрес, назначенный loopback-интерфейсу, может быть необходим для процессов маршрутизатора, в которых используется IPv4-адрес интерфейса в целях идентификации. Один из таких процессов — алгоритм кратчайшего пути (OSPF). При включении интерфейса loopback для идентификации маршрутизатор будет использовать всегда доступный адрес интерфейса loopback, а не IP-адрес, назначенный физическому порту, работа которого может быть нарушена. На маршрутизаторе можно активировать несколько интерфейсов loopback. IPv4-адрес для каждого интерфейса loopback должен быть уникальным и не должен быть задействован другим интерфейсом.



**Рис. 8.23.**Настраиваем интерфейс loopback на R1

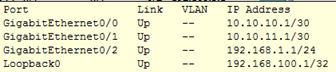
**Настраиваем протокол OSPF на R1**

Включаем OSPF на R1, все маршрутизаторы должны быть в одной зоне **area 0** ([рис. 8.24](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.24)).



**Рис. 8.24.**Включаем протокол OSPF на R1

Подводим курсор мыши к R1 и наблюдаем результат наших настроек ([рис. 8.25](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.25)).



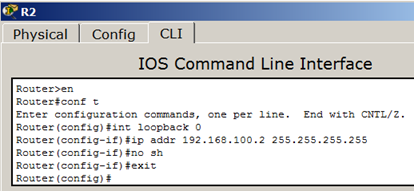
**Рис. 8.25.**Маршрутизатор R1 настроен

**Примечание**

Обратите внимание, что физически порта 192.168.100.1 нет, он существует только логически (программно).

**Настроим loopback интерфейс на R2**

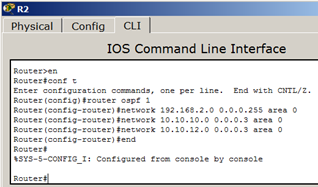
На R2 настроим программный loopback интерфейс по аналогии с R1 ([рис. 8.26](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.26)).



**Рис. 8.26.**Настраиваем логический интерфейс loopback на R2

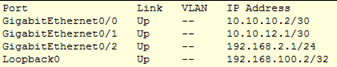
**Настраиваем OSPF на R2**

Включаем протокол OSPF на R2, все маршрутизаторы должны быть в одной зоне area 0 ([рис. 8.27](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.27)).



**Рис. 8.27.**Включаем протокол OSPF на R2

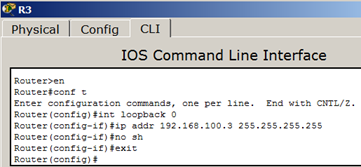
Подводим курсор мыши к R2 и наблюдаем результат наших настроек ([рис. 8.28](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.28)).



**Рис. 8.28.**Маршрутизатор R2 настроен

**Настраиваем loopback интерфейс на R3**

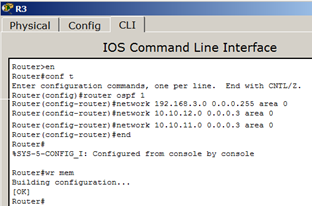
Делаем все аналогично ([рис. 8.29](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.29)).



**Рис. 8.29.**Настраиваем логический интерфейс loopback на R3

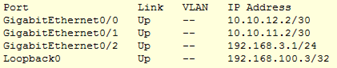
**Настраиваем протокол OSPF на R3**

Здесь делаем все, как раньше ([рис. 8.30](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.30)).



**Рис. 8.30.**Включаем протокол OSPF на R2

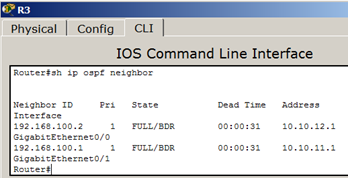
Проверяем результат ([рис. 8.31](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.31)).



**Рис. 8.31.**Маршрутизатор R3 настроен

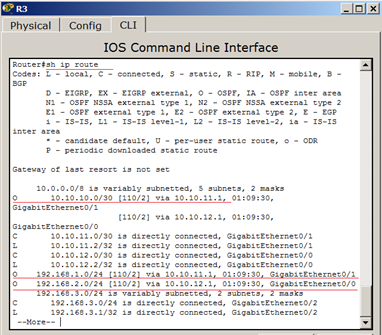
**Проверяем работу сети**

Убеждаемся, что роутер R3 видит R2 и R1 ([рис. 8.32](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.32)).



**Рис. 8.32.**Роутер R3 видит своих соседей

Теперь посмотрим таблицу маршрутизации для R3 ([рис. 8.33](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.33)).

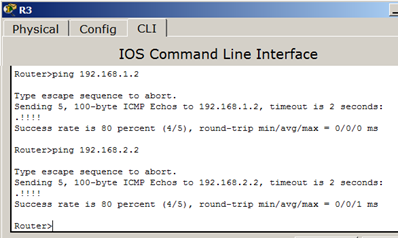


**Рис. 8.33.**Таблица маршрутизации для R3

**Примечание**

В этой таблице запись с буквой "О" говорит о том, что данный маршрут прописан протоколом OSPF. Мы видим, что сеть 192.168.1.0 доступна для R3 через адрес 10.10.11.1 (это порт gig0/1 маршрутизатора R1). Аналогично, сеть 192.168.2.0 доступна для R3 через адрес 10.10.12.1 (это порт gig0/1 маршрутизатора R2).

Теперь проверяем доступность разных сетей ([рис. 8.34](https://www.intuit.ru/studies/courses/3549/791/lecture/29224?page=3#image.8.34)).



**Рис. 8.34.**Сети 192.168.1.0 и 192.168.2.0 доступны

***Примечание****:*

*Решения сдать в электронном формате* **save.pkt** *до* ***26.03.2020*** *на электронную почту* [miron.sulejman@yandex.ru](mailto:miron.sulejman@yandex.ru)

Программу для работы можно получить по ссылке <https://yadi.sk/d/jcqhS38RV2ar4g>

Программа запуска Cisco Packet Tracer 5.3.2\bin\PacketTracer5.exe