Лабораторная работа № 4
Адаптивная маршрутизация

4.1. Цель работы

Лабораторная работа № 4 предназначена для изучения технологий и протоколов адаптивной маршрутизации и представляет собой сценарий для Cisco Packet Tracer. Для успешного выполнения лабораторной работы студентам необходимо выполнить задание сценария и подготовить отчет (по своему варианту), а также защитить его в форме собеседования.

4.2. Теоретическая часть

4.2.1. Адаптивная маршрутизации

Адаптивная (динамическая) маршрутизация — вид маршрутизации, при котором формирование таблиц маршрутизации автоматизировано на основе протоколов маршрутизации.

Все протоколы маршрутизации разработаны для получения данных об удалённых сетях и быстрой адаптации к любым изменениям в топологии. Метод, используемый протоколом маршрутизации для выполнения этих задачи, зависит от выбранного протокола и его эксплуатационных характеристик.

В целом, работу протокола динамической маршрутизации можно описать следующим образом:

1. Маршрутизатор отправляет и принимает сообщения маршрутизации с помощью своих интерфейсов.
2. Маршрутизатор предоставляет общий доступ к сообщениям маршрутизации и данным о маршрутах для других маршрутизаторов, использующих тот же протокол маршрутизации.
3. Маршрутизаторы осуществляют обмен данными маршрутизации для получения информации об удалённых сетях.
4. При обнаружении изменений в топологии, маршрутизатор использует протокол маршрутизации для извещения других маршрутизаторов об этом изменении.

Протоколы маршрутизации можно классифицировать по различным группам в соответствии с их назначением и характеристиками (Рис 4.1).

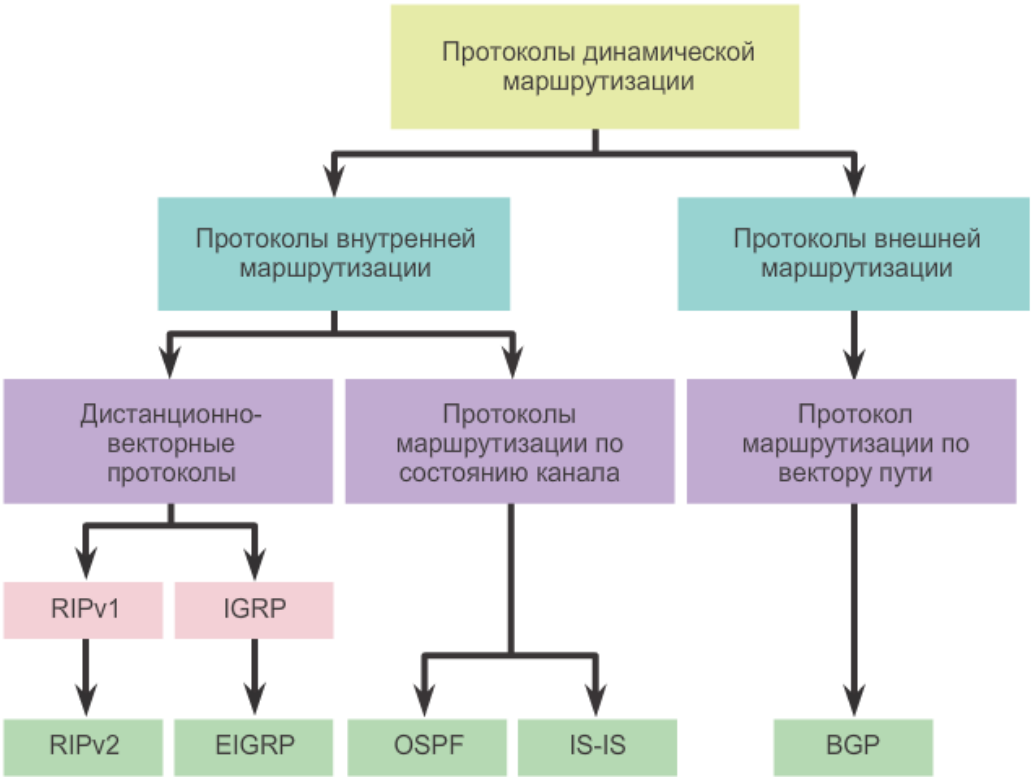

Рис. 4.1. Классификация протоколов маршрутизации

Бывают ситуации, когда протокол маршрутизации получает более одного маршрута до одной сети назначения. Для выбора оптимального маршрута протокол маршрутизации должен уметь оценивать и различать возможные пути. Эта задача выполняется посредством использования метрик маршрутизации.

Метрика (metric) – аддитивная характеристика протяженности маршрута (напр., количество хопов, битовая скорость, задержки) – критерий выбора маршрута.

Если на маршрутизаторе одновременно работает несколько протоколов динамической маршрутизации, то для выбора лучшего маршрута, маршрутизатор использует другую характеристику – административную дистанцию (AD). AD – первый критерий, который используется маршрутизатором для выбора из протоколов, предоставляющих информацию о маршруте до одной и той же сети. AD – это мера надежности источника информации о маршруте. AD имеет локальное значение (в пределах данного маршрутизатора), информация о ней не включается в рассылку маршрутной информации.

Значения AD по умолчанию для различных источников маршрутной информации приведены в таблице 4.1.

Таблица 4.1

Значения AD для различных источников маршрутов

Источник маршрута	Административная дистанция
Прямой (Connected, C)	0
Статический (Static, S)	1
Суммарный маршрут EIGRP	5
Внешний BGP	20
Внутренний EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Внешний EIGRP	170
Внешний BGP	200

4.2.2 Routing Information Protocol (RIP)

Routing information protocol — динамический протокол маршрутизации дистанционно-векторного типа. Протокол RIP использует алгоритм Беллмана-Форда в качестве алгоритма маршрутизации. Он основан на двух алгоритмах, разработанных в 1958 и 1956 гг. Ричардом Беллманом (Richard Bellman) и Лестером Фордом-мл. (Lester Ford, Jr). Есть три версии протокола:

- RIPv1 — динамический протокол классовой маршрутизации;
- RIPv2 — динамический протокол бесклассовой маршрутизации;
- RIPng — динамический протокол бесклассовой маршрутизации с поддержкой IPv6.

«Дистанционно-векторный» означает, что маршруты объявляются путём указания двух характеристик:

- Расстояние — определяет удалённость сети назначения;
- Вектор — определяет направление маршрутизатора следующего перехода или выходного интерфейса маршрута для доступа к адресу назначения.

Протокол RIP использует простейшую метрику – количество хопов, т.е количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP. В лабораторной работе № 3 было показано, что непосредственно подключенные сети появляются в таблице маршрутов сразу

после инициализации интерфейсов маршрутизатора IP-адресами в этих сетях. Начнем рассмотрение процесса с момента, когда минимальные таблицы заполнены. Тогда работа протокола RIP может быть описана как бесконечный цикл повторения двух действий:

1. Маршрутизатор выполняет рассылку всем своим соседям специального служебного сообщения протокола RIP, в котором содержатся сведения обо всех известных ему сетях и лучших маршрутах к ним.

2. Маршрутизатор получает аналогичные сообщения от соседних маршрутизаторов, также использующих протокол RIP. Получив такое сообщение, маршрутизатор для всех маршрутов, содержащихся в указанном сообщении, увеличивает метрику на единицу и запоминает через какой порт и от какого маршрутизатора получена новая информация (адрес этого маршрутизатора станет адресом следующего маршрутизатора, если эта запись будет внесена в таблицу маршрутизации). После маршрутизатор сравнивает новую информацию с той, которая хранится в его таблице. Протокол RIP замещает запись о какой-либо сети только в том случае, если новая информация имеет лучшую метрику (с меньшим расстоянием в хопах), чем имеющаяся. В результате в таблице маршрутизации о каждой сети остается только одна запись (за исключением случаев, когда несколько маршрутов имеют одинаковые метрики). Для этого правила существует исключение — если худшая информация о какой-либо сети пришла от того же маршрутизатора, на основании сообщения, которого была создана данная запись, то худшая информация замещает лучшую.

4.2.3. RIP: Обработка изменений в топологии

В протоколе RIP период рассылки обновлений выбран равным 30 секундам, а в качестве тайм-аута выбрано шестикратное значение периода рассылки, то есть 180 секунд. Шестикратный запас времени нужен для уверенности в том, что сеть действительно стала недоступной, а не просто произошли потери RIP-сообщений (а это возможно, так как протокол RIP использует транспортный протокол UDP, который не обеспечивает надежной доставки сообщений). Если какой-либо маршрутизатор отказывает, переставая слать своим соседям сообщения о сетях, которые можно достичь через него, то через 180 секунд все записи, отправленные этим маршрутизатором, у его ближайших соседей станут недействительными. После этого процесс повторится уже для ближайших соседей — они вычеркнут подобные записи уже через 360 секунд.

4.2.4. RIP: Маршрутные петли

В силу недостатков, изначально заложенных в дистанционно-векторных протоколах, протокол RIP подвержен возникновению маршрутных петель – ситуаций, когда два маршрутизатора добавляют в таблицу маршруты до одной сети, направленные друг на друга. Это приводит к зацикливанию пакетов на данном участке сети и имеет крайне негативные последствия для работы сети в целом. Рассмотрим последовательность возникновения петли и зацикливания пакетов на примере (Рис 4.2).

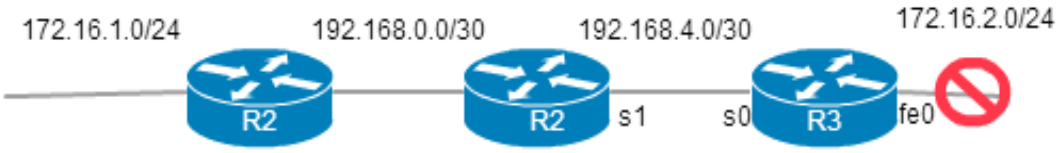

Рисунок 4.2. Маршрутная петля

1. Сеть 172.16.2.0/24 стала недоступной (например, вследствие обрыва кабеля). Интрерфейс fe0 маршрутизатора R3 переходит в состояние down, и маршрутизатор R3 в таблице маршрутизации устанавливает для этой непосредственно подключенной сети метрику 16.
2. Маршрутизатор R3 не успевает отослать соседям обновление о том, что у сети 172.16.2.0/24 теперь метрика 16 и она не доступна. В этот момент R2 посылает обновление свой таблицы маршрутизатору R3 в которой есть путь до сети 172.16.2.0/24 с метрикой 1;
3. Маршрутизатор R3, получив обновление видит, что в таблице маршрутизации R2 есть путь до сети 172.16.2.0/24 с метрикой = 1. R3 записывает новый маршрут до сети 172.16.2.0/24 через R2, увеличивая метрику до 2. Теперь любой пакет, идущий в сеть 172.16.2.0/24 будет зациклен между R3 и R2.

Однако описанный пример носит условный характер, т.к. в протоколе RIP предусмотрен ряд алгоритмов, предотвращающих возникновение петель. Среди них:

- **Triggered updates** – триггерные обновления. Маршрутизатор получив данные об изменение метрики до какой-либо сети, не ждет истечения 30-секундного периода передачи таблицы маршрутизации, а передаёт обновление немедленно.
- **Holddown timer** – таймер заморозки. Маршрутизатор блокирует все изменения маршрутов, связанные с потенциально недоступной сетью, причем величина (240 секунд) таймера превышает стандартные 180 секунд таймаута обновления маршрутной записи.

– **Split horizon** – разделенный горизонт. Маршрутизатор не передает информации о сети на тот интерфейс, через который эта информация была получена. Есть также усовершенствованный алгоритм Split horizon with Poison reverse. При его использовании маршрутизатор передаёт обратно на интерфейс, через который получена информация о сети, маршрут с бесконечной метрикой (16).

4.2.5. Open Shortest Path First (OSPF)

Протокол маршрутизации OSPF (англ. Open Shortest Path First – «открыть кратчайший путь первым») основан на алгоритме поиска кратчайшего пути (алгоритм SPF, алгоритм Дейкстры) и относится к внутренним протоколам маршрутизации по состоянию каналов (англ. link-state). В отличие от дистанционно-векторных протоколов, протоколы маршрутизации по состоянию каналов могут сохранять в памяти полную топологию сети путём сбора данных от остальных маршрутизаторов. На основе этой топологии вычисляются кратчайшие пути.

Процесс маршрутизации по состоянию каналов может быть декомпозирован на несколько этапов. Как и в случае с RIP, будем считать, что к началу процесса минимальная таблица маршрутизации заполнена – в нее добавлены сведения о непосредственно подключенных сетях.

1. Каждый маршрутизатор рассылает служебные сообщения hello со всех интерфейсов, где включен OSPF. Сообщения hello включают в себя номер зоны, способ расчета метрики и т.д. При получении сообщений hello от соседей и в случае совпадения настроек в этих сообщениях они устанавливают отношения соседства (англ. adjacency). Рассылка сообщений повторяется каждые 15 секунд для поддержания сведений о состоянии каналов в актуальном состоянии.

2. Каждый маршрутизатор создаёт пакет состояния канала (LSP), в котором содержатся подробные сведения о состоянии каждого из напрямую подключённых каналов:

– IP-адрес сети и маска;
– IP-адрес интерфейса маршрутизатора в этой сети;
– тип сети;
– метрика;
– информация о соседних (adjacent) маршрутизаторах на этом канале.

3. Каждый маршрутизатор выполняет лавинную рассылку пакетов состояния канала всем соседним устройствам, которые затем сохраняют полученные пакеты в свою базу данных и отправляют дальше без изменений.

Таким образом обеспечивается получение каждым маршрутизатором каждого LSP.

4. Каждый маршрутизатор на основе полученных LSP формирует базу данных для создания полной карты топологии – базу данных состояния каналов (англ. link-state database, LSDB) и вычисляет по алгоритму Дейкстры оптимальный путь к каждой сети назначения.

Алгоритм SPF (Shortest Path First), также называемый алгоритмом Дейкстры (Рис 4.3) – алгоритм на графах, позволяющий найти кратчайшее расстояние от одной из вершин графа до всех остальных (работает только для графов без рёбер отрицательного веса).

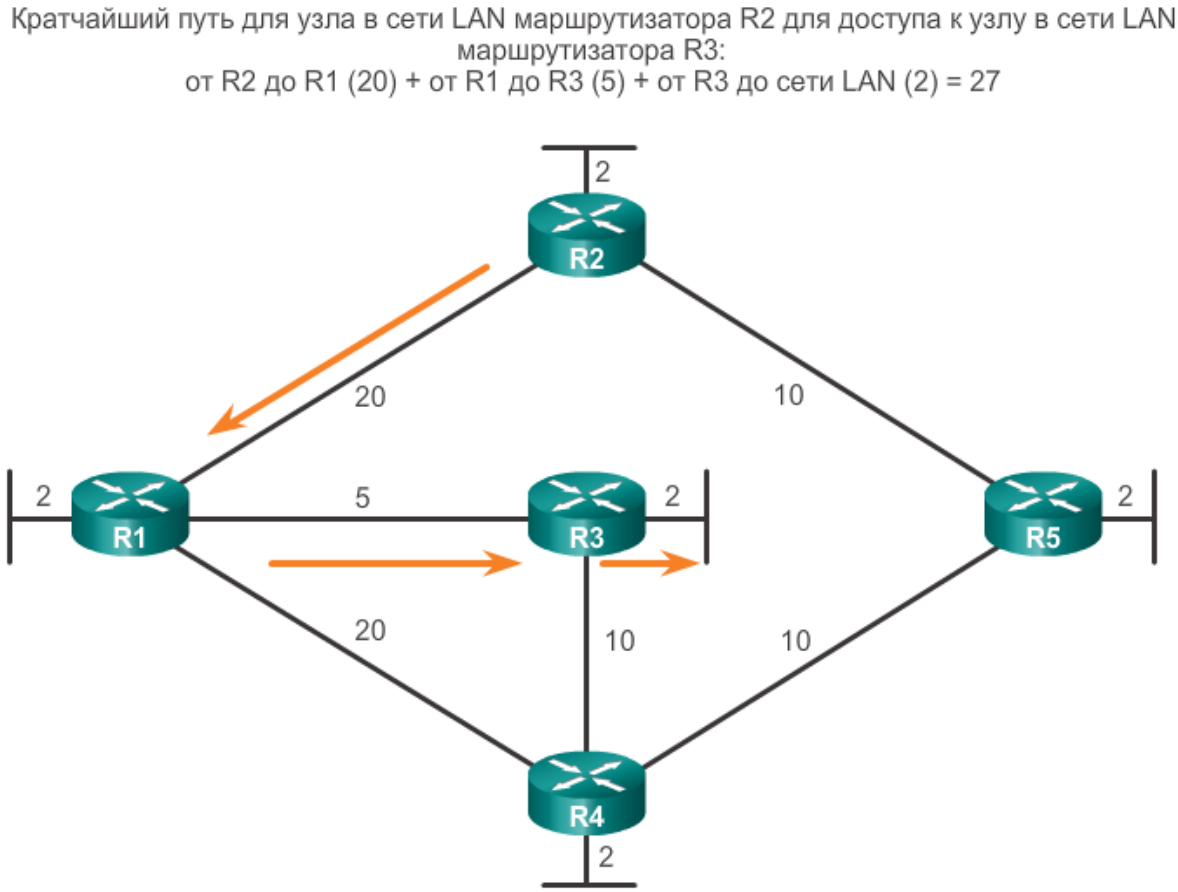

Рисунок 4.3. Алгоритм Дейкстры

Алгоритм основан на последовательном переборе вершин графа и вычислении расстояния от текущей вершины до каждой следующей. Математически доказано, что, если рассматривать вершины в порядке увеличения расстояния до корня, итоговые вычисленные значения расстояний (то есть, метрик) будут минимальными.

Более подробно алгоритм SPF рассмотрен в лекционном курсе.

4.2.6. OSPF: Аутентификация

Маршрутизаторы, выполняющие определённые роли в сети, настолько важны, что часто они подвергаются сетевым атакам. Системы маршрутизации могут быть атакованы посредством нарушения смежности маршрутизаторов или фальсификации данных, передаваемых протоколом маршрутизации. Аутентификация необходима для противодействия атакам на протокол маршрутизации.

Когда на маршрутизаторе настроена аутентификация соседних устройств, маршрутизатор проверяет источник каждого получаемого пакета обновлений маршрутов. Эта аутентификация реализуется путем обмена ключа аутентификации (который также называют паролем), известного маршрутизатору – отправителю и маршрутизатору – получателю.

OSPF поддерживает аутентификацию трех типов:

– нулевая (null) — это способ по умолчанию, который означает, что аутентификация для OSPF не используется;

– простая (plain) аутентификация по паролю (также ее называют аутентификацией на базе открытого ключа, поскольку пароль в обновлении отправляется по сети в виде обычного текста) — этот способ аутентификации OSPF считается устаревшим;

– аутентификация MD5 — наиболее безопасный и рекомендуемый способ аутентификации. Аутентификация MD5 гарантирует более высокий уровень безопасности, равноправные узлы не обмениваются паролями. Вместо этого он вычисляется по алгоритму MD5. Отправителя аутентифицируют совпадающие результаты.

Работа алгоритма аутентификации MD5 по шагам:

1. Маршрутизатор – отправитель обновления вычисляет значение подписи с помощью алгоритма MD5, используя передаваемое сообщение маршрутизации и предварительно согласованный секретный ключ. Подпись также называют значением хэш-функции. Подпись добавляется к сообщению маршрутизации и отправляется на соседний маршрутизатор.

2. Маршрутизатор – получатель объединяет сообщение маршрутизации с предварительно согласованным секретным ключом и повторно вычисляет значение подписи с помощью алгоритма MD5. Если подписи совпадают, получатель принимает обновление маршрутизации, а если подписи не совпадают, отбрасывает обновление.

4.2.7. OSPF: Деление сети на зоны

Протокол OSPF может работать в крупных сетях, включающих сотни сетей и маршрутизаторов. Однако при использовании OSPF в большой сети возникает ряд проблем, ограничивающих его применение:

1. Большой размер таблицы маршрутизации (т.к. OSPF не будет суммировать сети) приведёт к тому, что каждый проход по таблице будет занимать продолжительное время.

2. Большой размер топологической базы данных (т.к. каждый маршрутизатор собирает информацию о всех каналах между всеми маршрутизаторами) приведёт к перерасходу оперативной памяти.

3. Время выполнения алгоритма SPF и поиска маршрутов сильно возрастет из-за размера LSDB; кроме того, любое изменение топологии приведёт к полному перерасчёту SPF на всех маршрутизаторах, а так как сеть большая, то такие перерасчёты могут происходить часто. Как следствие, вырастет нагрузка на процессор.

Чтобы обеспечить большую масштабируемость протоколу, в него заложена возможность деления сети на отдельный территории (area). При таком делении, многие операции выполняются внутри каждой area автономно, не влияя на устройства за её пределами, что приводит к улучшению производительности.

Зона (area) — совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны. Главной считается корневая зона (backbone area), имеющая номер 0. Именно с ней мы работаем, когда настраиваем OSPF для одной зоны. В случае использования нескольких зон, использование area 0 обязательно, остальные же зоны подключаются к ней и называются regular area (двухуровневая иерархия зон).

Такой подход позволяет преодолеть приведённые выше проблемы. Маршрутизатор получает LSA только из зон, в которые он сам входит и пересчитывать карту сети надо только в том случае, если что-то поменялось в этих зонах. При этом большинство маршрутизаторов, кроме пограничных, как правило, входят в одну единственную зону.

Нет чётких формул расчёта количества зон или маршрутизаторов, это зависит от конфигурации сети и мощности железа, но есть общие рекомендации от cisco:

- не более 50 маршрутизаторов на зону;
- не более трёх зон на маршрутизатор;
- не более 60 соседей у маршрутизатора.

4.2.8. Инверсная маска (wildcard mask)

Сетевые устройства используют различные форматы хранения настроек, в том числе сетевой маски, причем в разных режимах работы зачастую требуется ввод маски в разных форматах. Один из распространенных форматов представления сетевой маски, не рассмотренный ранее – т.н. инверсная (или шаблонная, англ. wildcard) маска, которая используется в т.ч. при конфигурировании протокола OSPF.

Инверсная маска вычисляется путем побитового вычитания стандартной сетевой маски из величины 255.255.255.255.

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
255	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
252	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**
3	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**

Пример: для маски 255.255.255.252 инверсная маска будет 0.0.0.3.

4.2.9. Команды IOS

Рассмотрим список новых команд IOS, необходимых и достаточных для выполнения лабораторной работы № 4. Более простые команды см. в описании лабораторных работ №№ 1-3, а также в контекстной справке Cisco IOS (команда ?).

Команды привилегированного режима // router#

- **show ip rip […]** – выводит подробную информацию о конфигурации и работе протокола RIP; список возможных параметров см. во встроенной справке IOS;
- **show ip ospf […]** – выводит подробную информацию о конфигурации и работе протокола OSPF; список возможных параметров см. во встроенной справке IOS;

Команды режима глобального конфигурирования // router(config)#

- **router rip** – включение протокола маршрутизации RIP и вход в режим конфигурации этого протокола;
- **router ospf [номер процесса]** – включение протокола маршрутизации OSPF с указанным номером процесса и вход в режим конфигурации этого протокола; номер процесса нужен для обеспечения возможности

запуска нескольких процессов OSPF (например, для граничных маршрутизаторов) и их различия; номер процесса имеет локальное значение и не включается в сообщения маршрутизации, следовательно номера процессов не обязательно должны совпадать на соседних маршрутизаторах;

Команды режима конфигурирования протокола RIP // router(config-router)#:

- **version [1 или 2]** – включает протокол RIP выбранной версии; напомним, что RIPv2 является протоколом бесклассовой маршрутизации и включает маску сети в маршрутные сообщения; по умолчанию используется версия 1, рекомендуется версия 2;
- **no auto-summary** – отключает автоматическое суммирование маршрутов (по умолчанию включена); рекомендуется отключать автосуммирование, т.к. оно является распространенной причиной возникновения ошибок маршрутизации, в т.ч. петель;
- **network [IP-адрес сети]** – включает протокол RIP на всех интерфейсах, входящих в указанную сеть;
- **passive-interface [интерфейс]** – переводит интерфейс в пассивный режим; пассивные интерфейсы не осуществляют рассылку маршрутных сообщений; как правило, пассивный режим включается на интерфейсах, подключенным к локальным сетям или сети провайдера, чтобы не загружать сеть бесполезным служебным трафиком;
- **default-information originate** – маршрутизатор включает в маршрутные сообщения маршрут по умолчанию; как правило, команда вводится на маршрутизаторе, подключенному к провайдеру (ISP, Interner Service Provider), таким образом он сообщит остальным маршрутизатором, что через него можно выйти в Интернет.

Команды режима конфигурирования протокола OSPF // router(config-router)#:

- **network [IP-адрес сети] [wildcard маска] area [номер зоны]** – включает данный процесс протокола OSPF на всех интерфейсах, входящих в указанную сеть, и помещает их в выбранную зону;
- **passive-interface [интерфейс]** – переводит интерфейс в пассивный режим; пассивные интерфейсы не осуществляют рассылку маршрутных сообщений;
- **default-information originate** – маршрутизатор включает в маршрутные сообщения маршрут по умолчанию;

- **area [номер зоны] authentication message-digest** – включает md5-аутентификацию для всех интерфейсов данной зоны (можно также задать метод аутентификации отдельно для каждого интерфейса, см. ниже);

Команды конфигурации интерфейса // router(config-if)#:

- **ip ospf authentication message-digest –** включает md5-аутентификацию для протокола OSPF на текущем интерфейсе; это необходимо лишь в том случае, если такой метод аутентификации уже не выбран для всех для всех интерфейсов данной зоны в режиме конфигурирования OSPF (см. выше); имеет приоритет по отношению к общему методу аутентификации для зоны – может назначать другой метод аутентификации для текущего интерфейса;
- **ip ospf message-digest-key [номер ключа] md5 [пароль – текстовая строка]** – создает md5-ключ с указанным порядковым номером и паролем; порядковый номер необходим для управления версиями ключей – при смене ключа каждый следующий номер должен быть больше предыдущего; номер и пароль должны совпадать на соседних маршрутизаторах, но не рекомендуется использовать одинаковые значения во всей зоне.

4.3. Задание на лабораторную работу

Лабораторная работа выполняется в среде Cisco Packet Tracer в предложенном Вам файле-сценарии формата pka. Сценарий содержит созданную заранее логическую топологию в виде составной сети, моделирующей корпоративную сеть условного предприятия, состоящей из двух областей (рис. 4.4). В первой области используется протокол маршрутизации RIPv2, во второй – OSPF. Для маршрутизации между зонами используются статические суммарные маршруты и маршруты по умолчанию.

Устройства не настроены.

Необходимо выполнить расчет IP-адресов локальных сетей и устройств, настроить все устройства (компьютеры и маршрутизаторы), а также маршрутизацию: адаптивную по выбранному протоколу в каждой из областей и статическую между областями.

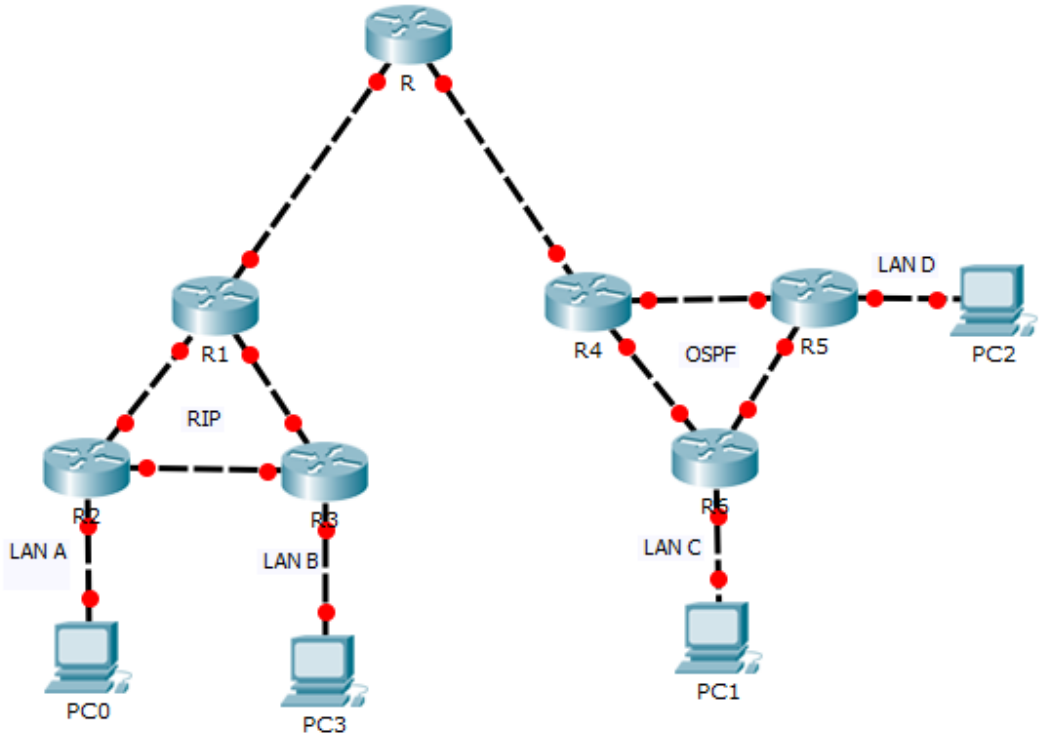

Рисунок 4.4. Топология сети

4.3.1. Расчёт IP-адресов и настройка локальных сетей

Выполнить расчет основных сетевых параметров для сетей LAN A, LAN B, LAN C и LAN D исходя из известного количества узлов в каждой из них (согласно Вашему варианту), а также известного диапазона адресов для каждой из сетей: (где X – номер Вашего варианта):

- для сети LAN A – 192.168.100+X.0/24;
- для сети LAN B – 192.168.110+X.0/24;
- для сети LAN C – 172.15+X.0.0/16;
- для сети LAN D – 172.18+X.0.0/16.

Пример: Студент с номером варианта 34 выбирает для сети A диапазон необходимой длины из пространства 192.168.134.0/24.

Рассчитанные адреса занести в отчет.

Выполнить настройку компьютеров (настроить IP-адрес, маску подсети и шлюз по умолчанию). Задать компьютерам IP-адреса из соответствующих диапазонов. Как и ранее, использовать для компьютеров **максимальные** IP-адреса из доступных.

4.3.2. Настройка маршрутизаторов

Выполнить первоначальную настройку маршрутизаторов (присвоить символьные имена, задать пароли для доступа к консоли, привилегированному

режиму и виртуальному терминалу, включить шифрование всех паролей и добавить баннер). *Подробнее о первоначальной настройке устройств см. методические рекомендации к лабораторной работе №1*.

Выполнить расчет IP-адресов для сетей, соединяющих маршрутизаторы (назовем их служебными подсетями). Для этого разбить соответствующий диапазон адресов на 8 равных подсетей. Первые четыре подсети использовать для зоны RIP, вторые – для OSPF.

Настроить интерфейсы маршрутизаторов. В локальных сетях использовать **минимальные** IP-адреса из доступных. В остальных подсетях использовать минимальный адрес для маршрутизатора с меньшим порядковым номером.

Пример. Пусть R56 имеет три активных интерфейса: f0/0 в локальной сети LAN Z, f0/1 в общем сегменте с R55 и f0/2 в общем сегменте с R57. Тогда необходимо на f0/0 и f0/2 назначить минимальные IP-адреса, а на f0/1 – максимальный.

Используя команды проверки конфигурации (show), убедиться в правильности введенных настроек. Присвоенные адреса занести в отчет.

4.3.3. Настройка статической маршрутизации

Просуммировать диапазоны адресов, используемые

а) в локальных сетях области RIP;

б) в локальных сетях области OSPF;

в) в служебных подсетях области RIP;

г) в служебных подсетях области OSPF.

Настроить на R статические суммарные маршруты до перечисленных сетей. Настроить на R1 и R4 статические маршруты по умолчанию. ВНИМАНИЕ! Использование иных статических маршрутов, кроме перечисленных, в данном сценарии запрещено.

4.3.4. Настройка протокола RIP

На маршрутизаторах R1- R3 (область RIP) настроить маршрутизацию по протоколу RIP (версия 2):

- включить адаптивную маршрутизацию по протоколу RIP;
- выбрать версию 2;
- отключить автоматическое суммирование маршрутов;
- настроить маршрутизацию RIP на всех интерфейсах маршрутизаторов R1-R3, кроме соединения с R;

- включить рассылку маршрута по умолчанию там, где это необходимо;
- настроить пассивные интерфейсы там, где это необходимо.

Используя команды проверки конфигурации (show) и tcp echo пакеты (ping), убедиться в правильности введенных настроек. Убедиться в наличии маршрута по умолчанию в таблицах всех маршрутизаторов области RIP. На этом этапе должна быть связь между всеми устройствами области RIP и устройством R.

4.3.5. Настройка протокола OSPF

На маршрутизаторах R4-R6 (область OSPF) настроить маршрутизацию по протоколу OSPF. Номер процесса OSPF задать равным номеру варианта. Использовать корневую зону. Пошаговая инструкция по настройке маршрутизаторов:

- включить адаптивную маршрутизацию по протоколу OSPF;
- настроить маршрутизацию OSPF на всех интерфейсах маршрутизаторов R4-R6, кроме соединения с R;
- включить рассылку маршрута по умолчанию там, где это необходимо;
- настроить пассивные интерфейсы там, где это необходимо;
- настроить аутентификацию md5.

Используя команды проверки конфигурации (show) и tcp echo пакеты (ping), убедиться в правильности введенных настроек. Убедиться в наличии маршрута по умолчанию в таблицах всех маршрутизаторов области OSPF. На этом этапе должна быть связь между всеми устройствами в сети.

4.4. Контрольные вопросы

1. Что такое протокол маршрутизации? Для чего они предназначены?
2. Как классифицируются протоколы маршрутизации? Приведите примеры.
3. Опишите общие принципы дистанционно-векторных протоколов.
4. Опишите принцип работы протокола RIP и область его применения.
5. Что такое маршрутная петля? Как RIP противостоит появлению петель?
6. Опишите общие принципы протоколов состояния каналов.
7. Опишите принцип работы протокола OSPF и область его применения.
8. Опишите алгоритм Дейкстры.
9. Как и зачем осуществляется аутентификация маршрутизаторов – участников процесса маршрутизации?
10. Что такое зона OSPF? Зачем предусмотрено деление сети на зоны?
11. Что такое пассивный интерфейс?
12. Как и зачем включить маршрут по умолчанию в рассылку маршрутов?

4.5. Варианты индивидуальных заданий

Номер вар.	Количество узлов в сети				Диапазон служебных адресов
	LAN A	LAN B	LAN C	LAN D	
1	136	5	675	1500	12.135.73.0 – 12.135.73.31
2	4	178	270	250	14.76.34.32 – 14.76.34.63
3	50	23	156	270	156.45.2.64 – 156.45.2.95
4	200	189	97	53	56.245.23.96 – 56.245.23.127
5	177	48	1122	512	67.100.78.128 – 67.100.78.159
6	19	45	1100	322	90.34.156.160 – 90.34.156.191
7	140	11	1353	666	86.43.223.192 – 86.43.223.223
8	78	7	265	1507	123.11.98.224 – 123.11.98.255
9	179	45	1653	4	67.43.245.96 – 67.43.245.127
10	57	100	731	9	15.54.234.32 – 15.54.234.63
11	45	30	311	765	178.234.21.0 – 178.234.21.31
12	26	78	201	754	74.35.178.192 – 74.35.178.223
13	13	67	1285	231	156.67.234.64 – 156.67.234.95
14	6	30	256	754	174.45.94.160 – 174.45.94.191
15	55	63	123	510	193.16.35.128 – 193.16.35.159

4.6. Форма отчета

Отчет о выполнении лабораторной работы оформляется в соответствии с индивидуальным вариантом задания и является обязательным требованием для допуска к защите наряду с правильно настроенным сценарием работы в программе Packet Tracer.

Отчет должен включать титульный лист, схему сети, а также заполненные таблицы, приведенные ниже.

Расчет адресов локальных сетей

Параметр	LAN A	LAN B	LAN C	LAN D
Количество узлов				
Маска (префикс)				
Маска (десятичн.)				
Маска (инверсная)				
SUBNET				
HOSTMIN (router)				
HOSTMAX (host)				
BROADCAST				
Суммарный адрес				

Расчет адресов служебных сетей

Параметр	R0-R1	R1-R2	R1-R3	R2-R3
IP-адрес /маска				
Суммарный адр. /маска				
Параметр	**R0-R4**	**R4-R5**	**R4-R6**	**R5-R6**
IP-адрес /маска				
Суммарный адр. /маска				

Сведения о конфигурации устройств

Устройство	**Интерфейс** (пассивный?)		**IP-адрес**	**Маска подсети**	**Шлюз** (где необходимо)
R0	Fa0/0				
	Fa2/0				
R1	Fa0/0				
	Fa1/0				
	Fa2/0				
R2	Fa0/0				
	Fa1/0				
	Fa2/0				
R3	Fa0/0				
	Fa1/0				
	Fa2/0				
R4	Fa0/0				
	Fa1/0				
	Fa2/0				
R5	Fa0/0				
	Fa1/0				
	Fa2/0				
R6	Fa0/0				
	Fa1/0				
	Fa2/0				
PC 0	NIC				
PC 1	NIC				
PC 2	NIC				
PC 3	NIC				

Сведения о таблицах маршрутизации (добавить необходимое число строк)

Устр-во	**SRC**	**Сеть назначения**	**AD/ Метрика**	**Маршрут**
R3				
R6				
R				