Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет телекоммуникаций

Кафедра сетей и устройств телекоммуникаций

В. Ю. Цветков, К. А. Волков

ПРОТОКОЛЫ ВНУТРЕННЕЙ МАРШРУТИЗАЦИИ: OSPF И EIGRP

*Рекомендовано УМО по образованию
в области информатики и радиоэлектроники
в качестве учебно-методического пособия для специальности
1-45 81 01 «Инфокоммуникационные системы и сети»*

Минск БГУИР 2017

УДК 004.735:621.391(076)
ББК 32.973.202я73+32.88я73
Ц27

Р е ц е н з е н т ы:
кафедра связи учреждения образования
«Военная академия Республики Беларусь»
(протокол №94 от 25.08.2014);

заместитель директора по учебной и информационно-аналитической работе
филиала Белорусского национального технического университета
«Институт повышения квалификации и переподготовки кадров
по новым направлениям развития техники, технологии и экономики БНТУ»,
кандидат технических наук, доцент И. А. Тавгень

Цветков, В. Ю.

Ц27 Протоколы внутренней маршрутизации: OSPF и EIGRP : учеб.-метод. пособие / В. Ю. Цветков, К. А. Волков. – Минск : БГУИР, 2017. – 72 с. : ил.
ISBN 978-985-543-228-0.

Рассмотрены принципы маршрутизации с использованием протоколов OSPF и EIGRP в корпоративных мультисервисных сетях.

УДК 004.735:621.391(076)
ББК 32.973.202я73+32.88я73

ISBN 978-985-543-228-0

Содержание

Введение

Проектирование корпоративных мультисервисных сетей широко востребовано в настоящее время. Этот аспект телекоммуникационной деятельности занимает важное место по ряду причин: возрастание требований к безопасности данных, необходимость соединения технологически неоднородных сегментов сети, доступность технических решений и технологий организации доступа. Появление корпоративных сетей – это иллюстрация перехода количества в качество. Неотъемлемым атрибутом корпоративной мультисервисной сети является наличие глобальных связей, гетерогенность и принадлежность одному предприятию. В корпоративной сети используются различные типы компьютеров, операционных систем, коммуникационных протоколов, систем управления базами данных (СУБД) и других приложений.

Корпоративность предполагает расширение круга услуг, предоставляемых конечному пользователю. Обычные сервисы локальных сетей (разделение файлов и принтеров) дополняются сервисами корпоративной сети, в число которых входят почтовые службы, средства коллективной работы, поддержка удаленных пользователей, факс-сервис, обработка голосовых сообщений, организация видеоконференций, IP-телефония и т. д.

Широкое распространение в корпоративных мультисервисных сетях получил протокол маршрутизации OSPF. Это открытый протокол, основанный на анализе состояния каналов. Он описан в нескольких стандартах инженерной группы Internet Engineering Task Force (IETF), последним из которых является стандарт RFC 2328.

Термин «открытый» в протоколе OSPF отражает тот факт, что он стандартизован и не является фирменным протоколом. В настоящее время протоколу OSPF, вследствие его масштабируемости, все чаше отдается предпочтение перед протоколом информации о маршрутах (Routing Information Protocol – RIP) при выборе для сети протокола внутреннего шлюза (Interior Gateway Protocol – IGP).

Для определения наилучшего пути к пункту назначения протокол OSPF использует алгоритм выбора кратчайшего пути. В этом алгоритме наилучшим является маршрут с наименьшей метрикой. Этот алгоритм был создан голландским компьютерным специалистом Дейкстра (Dijkstra) и обнародован в 1959 году. В этом алгоритме сеть рассматривается как множество узлов, соединенных каналами типа «точка – точка». Каждому каналу присваивается некоторое значение метрики. Каждый узел имеет полную базу данных всех каналов, поэтому всем узлам известна вся информация о физической топологии сети. Алгоритм выбора кратчайшего пути вычисляет свободную от петель топологию, используя узел в качестве начальной точки и последовательно анализируя информацию о смежных узлах.

Протокол OSPF может быть использован в крупномасштабных сетях, в отдельной зоне в небольших сетях и в нескольких зонах для больших сетей.

Еще один важный аспект корпоративных сетей – распределенность ресурсов (соединение через глобальную сеть некоторого числа локальных сетей под общим управлением, принадлежащих одной организации). Для объединения таких сетей необходимы протоколы внешней маршрутизации. Часто используемым протоколом внешней маршрутизации является EIGRP, который также рассматривается в данном учебно-методическом пособии.

1. ПРОТОКОЛ ВНУТРЕННЕЙ МАРШРУТИЗАЦИИ OSPF

1.1. Принципы построения и функционирования протокола OSPF

1.1.1. Терминология протокола OSPF

Протокол OSPF является протоколом состояния каналов и функционирует иначе, чем дистанционно-векторные протоколы [1, 2]. Маршрутизаторы канального уровня идентифицируют соседние маршрутизаторы и обмениваются с ними информацией. С протоколом OSPF связан набор новых терминов. Они приведены на рис. 1.1.

Информация, собранная от соседних маршрутизаторов OSPF не является полной таблицей маршрутизации. Каждый OSPF-маршрутизатор сообщает своим соседям информацию о состоянии своих соединений или каналов. Эта информация распространяется методом лавинной рассылки. Под лавинной рассылкой понимают отправку одной и той же информации со всех портов, за исключением порта, на который она поступила. Маршрутизатор OSPF объявляет о состоянии своих каналов и передает далее полученную им информацию о состоянии каналов других маршрутизаторов.

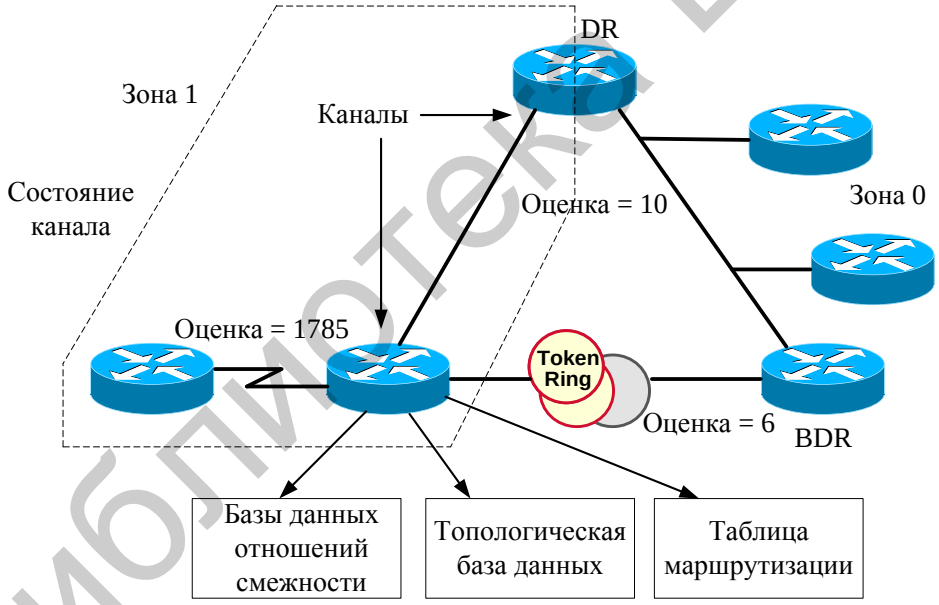


Рис. 1.1. Терминология протокола OSPF

Маршрутизаторы в зоне 1 обрабатывают эту информацию и строят свою топологическую базу данных, называемую также базой данных состояния каналов. Все маршрутизаторы в одной OSPF-зоне имеют одну и ту же базу данных состояния каналов. Каждый маршрутизатор имеет, таким образом, одну и ту же информацию о состоянии каналов и базу данных о своих соседях. Автономная система (Autonomous System – AS) может быть подразделена на ряд зон, представляющих собой группы связных (непрерывных) сетей и подсоединенных к ним устройств. Маршрутизаторы с несколькими интерфейсами могут быть

участниками нескольких зон. Эти маршрутизаторы, называемые граничными маршрутизаторами зон (Area Border Routers), поддерживают отдельные топологические базы данных для каждой зоны.

После этого каждый маршрутизатор применяет алгоритм выбора кратчайшего пути (Shortest Ppath First – SPF algorithm), также называемый алгоритмом Дейкстры, к своей копии базы данных. Эти вычисления определяют наилучший маршрут к пункту назначения. Алгоритм SPF складывает стоимости (оценки) для отдельных переходов, которые обычно базируются на ширине полосы пропускания, как показано на рис. 1.1. Минимальная оценка маршрута добавляется к таблице маршрутизации, также называемой таблицей пересылки.

OSPF-маршрутизаторы записывают информацию о своих соседях в таблицу смежных устройств. Для уменьшения объема информации, которой обмениваются соседние устройства в одной и той же сети, маршрутизаторы OSPF избирают назначенный маршрутизатор (Designated Router – DR) и резервный назначенный маршрутизатор (Backup Designated Router – BDR). Эти маршрутизаторы служат фокусными точками при обмене информацией маршрутизации.

1.1.2. Состояния протокола OSPF

OSPF-маршрутизаторы устанавливают связи или состояния (states) со своими соседями для эффективного совместного использования информации канального уровня. Иначе функционируют дистанционно-векторные протоколы маршрутизации, такие RIP, которые широковещательно рассылают полностью свои таблицы маршрутизации со всех своих интерфейсов в надежде, что эту таблицу получит требуемый маршрутизатор. В стандартном режиме маршрутизаторы протокола RIP каждые 30 с рассылают только один тип сообщения – свою полную таблицу маршрутизации. В отличие от них маршрутизаторы OSPF используют пять различных типов пакетов для идентификации своих соседей и обновления информации маршрутизации канального уровня. В табл. 1.1 описаны типы пакетов протокола OSPF. Эти пять типов пакетов позволяют протоколу OSPF осуществлять разнообразные и сложные типы связей.

Ключевым фактором при проектировании OSPF-сетей и при устранении ошибок в них является понимание связей, или состояний, которые возникают между OSPF-маршрутизаторами. Интерфейсы OSPF-маршрутизаторов могут находиться в одном из приведенных ниже семи состояний. Связи между соседними OSPF-маршрутизаторами последовательно проходят эти состояния сверху вниз в приведенном ниже списке:

– состояние отключения (Down);
– инициализация (Init);
– двустороннее соединение (Two-way);
– ExStart;
– обмен (Exchange);
– загрузка (Loading);
– состояние установки полной связи между соседними (смежными) устройствами (Full Adjacency).

Таблица 1.1

Типы пакетов протокола OSPF

Тип пакета протокола OSPF	Описание
Тип 1 – Hello	Используется для создания и поддержки таблицы соседних устройств
Тип 2 – Пакет описания базы данных (Database Description Packet – DBD)	Описывает содержимое базы данных состояния каналов OSPF-маршрутизатора
Тип 3 – Запрос информации о состоянии каналов	Запрашивает отдельные фрагменты базы данных состояния каналов маршрутизатора
Тип 4 – Обновление состояния каналов (Link-state Update – LSU)	Передает объявления о состоянии каналов (Link-state Advertisements – LSA) соседним маршрутизаторам
Тип 5 – Подтверждение получения объявления о состоянии каналов (Link-stale Acknowledgement – LSACK)	Подтверждает получение от соседнего устройства объявления LSA

Состояние отключения (Down State) имеет место в том случае, когда обмен информацией между соседними устройствами не происходил. Маршрутизаторы ожидают перехода в следующее состояние – состояние инициализации.

В состоянии инициализации (Init State) OSPF-маршрутизаторы регулярно (обычно каждые 10 с) посылают пакеты первого типа (Hello) для установки связи с соседними маршрутизаторами. Когда некоторый интерфейс получает первый Hello-пакет, соответствующий маршрутизатор переходит в состояние инициализации (Init) – это означает, что маршрутизатору известно о наличии у него соседнего устройства и он ожидает перехода связи с ним в следующее состояние.

Существует два типа связи между маршрутизаторами: двусторонняя связь и состояние полной связи соседних устройств, хотя между этими двумя состояниями находятся несколько промежуточных состояний. Перед тем как станет возможной установка какого-либо типа связи, маршрутизатор должен получить от своего соседа сообщение Hello.

Состояние двусторонней связи является базовым состоянием двух соседних устройств протокола OSPF, однако в этом состоянии совместное использование маршрутизаторами информации маршрутизации еще не происходит. Для того чтобы узнать о состоянии каналов других маршрутизаторов и в конечном итоге создать таблицу маршрутизации, каждый OSPF-маршрутизатор должен образовать по крайней мере одно соединение (состояние смежности) с соседним устройством. Состояние смежности представляет собой более тесную связь между OSPF-маршрутизаторами и включает в себя ряд последовательных состояний, которые базируются не только на Hello-сообщениях, но и на других

четырех типах OSPF-пакетов. Маршрутизаторы, которые пытаются стать смежными друг для друга устройствами, обмениваются информацией маршрутизации еще до того, как будет полностью установлено состояние смежности. Первым этапом установки состояния полной смежности является состояние ExStart.

В техническом аспекте в момент, когда маршрутизатор и его соседнее устройство входят в состояние ExStart, их связь характеризуется как состояние смежности, однако в действительности эти устройства еще не являются полностью смежными. Состояние ExStart устанавливается с помощью пакетов описания базы данных (Database Description – DBD) (пакетов второго типа). Эти пакеты также обозначаются как пакеты DDP.

Для обсуждения того, какой маршрутизатор в данном соединении будет ведущим («master»), а какой ведомым («slave»), маршрутизаторы используют пакеты Hello, а для обмена содержимым баз данных используются пакеты DBD (рис. 1.2).

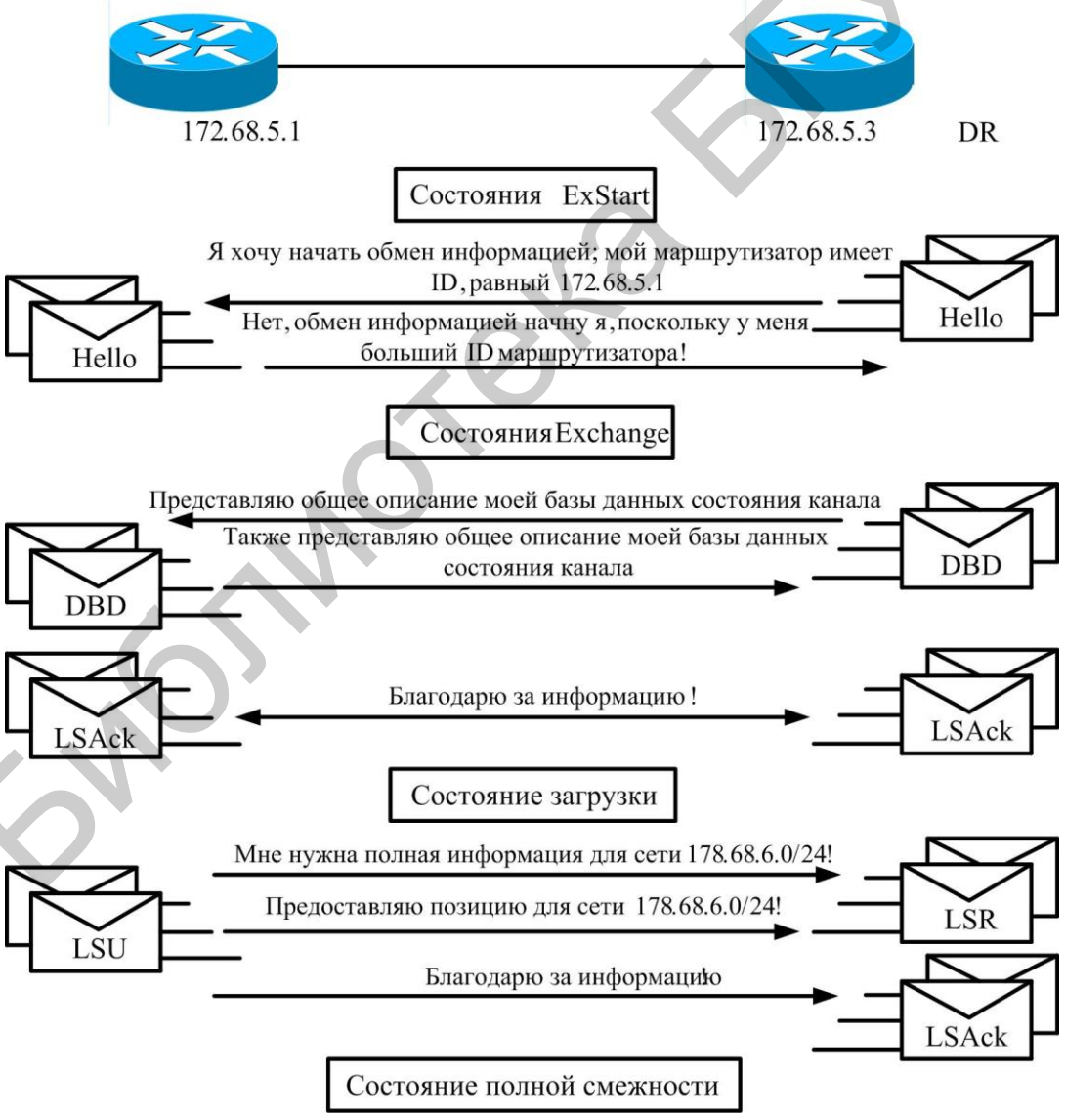


Рис. 1.2. Обнаружение маршрутизатора по протоколу OSPF

Маршрутизатор с максимальным значением OSPF-идентификатора (ID) становится ведущим. Когда два соседних маршрутизатора определяют свои роли как ведомого и ведущего, они входят в состояние обмена (Exchange) и начинают отправлять друг другу информацию маршрутизации.

В состоянии обмена Exchange соседние маршрутизаторы используют пакеты второго типа (DBD) для отправки друг другу своей информации о состоянии каналов, как показано на рис. 1.2. Маршрутизаторы описывают друг другу свои базы данных состояния каналов. При этом маршрутизаторы сравнивают полученную информацию с информацией, содержащейся в их собственных базах данных состояния каналов. Если какой-либо из маршрутизаторов получает информацию о канале, которая пока отсутствует в его базе данных, то он запрашивает у соседнего маршрутизатора полное обновление. Полный обмен информацией происходит в состоянии загрузки (Loading). После того как оба маршрутизатора описали друг другу свои базы данных, они могут запросить более полную информацию, используя пакеты третьего типа – запросы состояния каналов (Link-state Request – LSR). Когда маршрутизатор получает запрос, он отвечает отправкой обновления маршрутизации, используя пакет четвертого типа – пакет обновления состояния каналов (Link-state Update – LSU). Эти LSU-пакеты четвертого типа содержат объявления актуального состояния каналов (Link-state Advertisement – LSA), которые составляют сущность протоколов маршрутизации состояния каналов. Как показано на рис. 1.2, подтверждение получения LSU-пакетов пятого типа осуществляется с помощью пакетов пятого типа, называемых подтверждением состояния каналов (Link-state Acknowledgment – LSAck).

После того как полностью реализовано состояние загрузки (Loading), маршрутизаторы являются полностью смежными. Каждый маршрутизатор поддерживает свой список смежных соседних маршрутизаторов, называемый также базой данных смежных устройств. Эту таблицу смежных устройств не следует смешивать с базой данных состояния каналов или с базой данных пересылки. В табл. 1.2 перечислены важные базы данных протокола OSPF.

Таблица 1.2

Базы данных протокола OSPF

База данных	Описание
База данных о смежных устройствах	Список всех соседних устройств, с которыми данный маршрутизатор установил двусторонние соединения
База данных канального уровня (топологическая база данных)	Информация обо всех маршрутизаторах сети. Эта база данных отражает текущую сетевую топологию. Все маршрутизаторы одной и той же области имеют идентичные базы данных канального уровня

Окончание табл. 1.2

База данных	Описание
База данных пересылки (таблица маршрутизации)	Список маршрутов, генерируемый при выполнении алгоритма маршрутизации, к базам данных канального уровня. Таблица маршрутизации каждого маршрутизатора уникальна и содержит информацию о том, каким образом и по каким маршрутам следует отправлять пакеты, предназначенные другим маршрутизаторам

1.1.3. Типы сетей протокола OSPF

Для того чтобы совместно использовать информацию о маршрутизации, OSPF-маршрутизаторы должны установить связь с соседними устройствами; каждый маршрутизатор пытается установить отношения смежности или соседства по крайней мере с одним маршрутизатором каждой IP-сети, к которой подсоединены его порты. Некоторые маршрутизаторы могут попытаться установить отношения смежности со всеми соседними маршрутизаторами, в то время как другие – только с одним или двумя. OSPF-маршрутизаторы определяют, с какими иными маршрутизаторами им следует установить отношения смежности на основе типа сети, которая их соединяет.

После того как между соседними устройствами установлены отношения смежности, между ними происходит обмен информацией о состоянии канала. Как показано на рис. 1.3 и перечислено в приводимом ниже списке, интерфейсы OSPF-маршрутизаторов распознают три типа сетей:

– широковещательные сети множественного доступа;

– нешироковещательные сети множественного доступа (Nonbroadcast Multiaccess – NBMA);

– сети с каналами типа «точка – точка».

Сетевой администратор может сконфигурировать на каком-либо интерфейсе и четвертый тип сетей – сеть типа «точка – несколько точек». В табл. 1.3 приведены типы OSPF-сетей. В сети множественного доступа (Multiaccess Network) невозможно заранее узнать, сколько маршрутизаторов будут соединены друг с другом. В сетях типа «точка – точка» (point-to-point) могут быть соединены только два маршрутизатора. Если все маршрутизаторы установят отношения смежности со всеми остальными и будут обмениваться информацией о состоянии каналов, то объем служебных сообщений станет слишком большим. Например, пяти маршрутизаторам потребуется установить 10 отношений смежности и соответственно будут рассылаться 10 сообщений о состоянии каналов. Десяти маршрутизаторам потребуется 45 отношений смежности. В общем случае потребуется установить (nn–1)/2 отношений смежности.

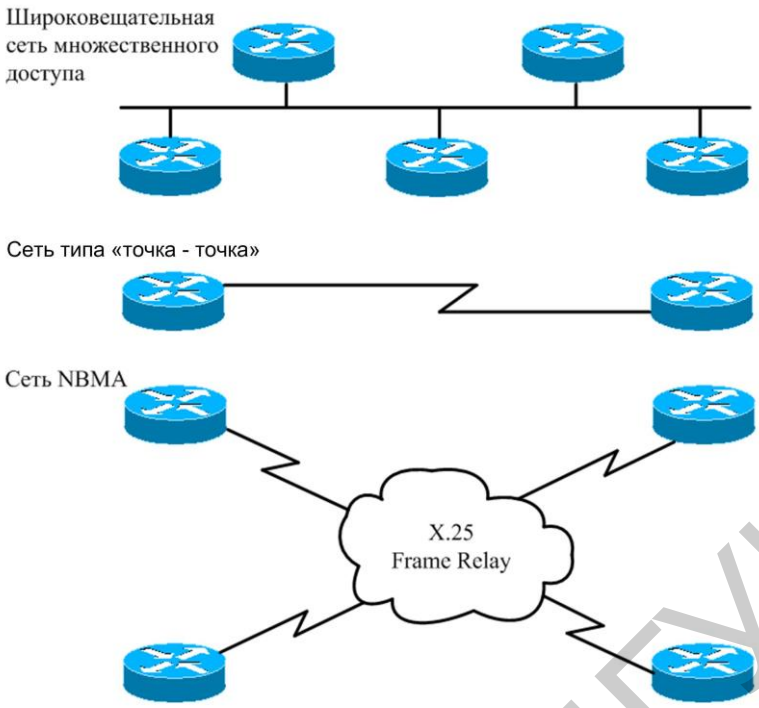


Рис. 1.3. Типы OSPF-сетей

Таблица 1.3

Типы сетей OSPF

Тип сети	Определяемые характеристики	Есть ли выбор DR-маршрутизатора?
Широковещательный множественный доступ	Ethernet. Token Ring, или FDD1	Да
Нешироковещательный множественный доступ	Frame Relay, X.25, SMDS	Да
«Точка – точка»	PPP, HDLC	Нет
«Точка – несколько точек»	Конфигурируется сетевым администратором	Нет

Возникающая проблема большого объема служебных сообщений может быть решена выбором назначенного маршрутизатора (Designated Router – DR).

Этот назначенный маршрутизатор становится смежным устройством для всех маршрутизаторов широковещательного сегмента. Все остальные маршрутизаторы этого сегмента посылают информацию о состоянии канала назначенному маршрутизатору. В этом случае назначенный маршрутизатор DR становится источником информации для данного сегмента. В рассмотренных выше примерах потребуется рассылка соответственно 5 и 10 сообщений о состоянии канала. Назначенный маршрутизатор DR рассылает информацию о состоянии каналов всем другим маршрутизаторам сегмента, используя адрес многоадресатной рассылки 224.0.0.5 для всех OSPF-маршрутизаторов. Однако, несмотря

на повышение эффективности работы сети, которое обеспечивается использованием назначенного маршрутизатора, в данном подходе присутствует и недостаток – назначенный маршрутизатор представляет собой точку, от которой зависит работа всего сегмента и в случае выхода его из строя весь сегмент становится неработоспособным. Поэтому выбирается также резервный назначенный маршрутизатор (Backup Designated Router – BDR), который принимает на себя выполнение функций назначенного маршрутизатора в случае отказа последнего. На рис. 1.4 показаны маршрутизаторы DR и BDR, получающие сообщения LSA. Для того чтобы оба маршрутизатора DR и BDR получали все сообщения о состоянии канала, посылаемые в сегмент, используется адрес многоадресатной рассылки 224.0.0.6.

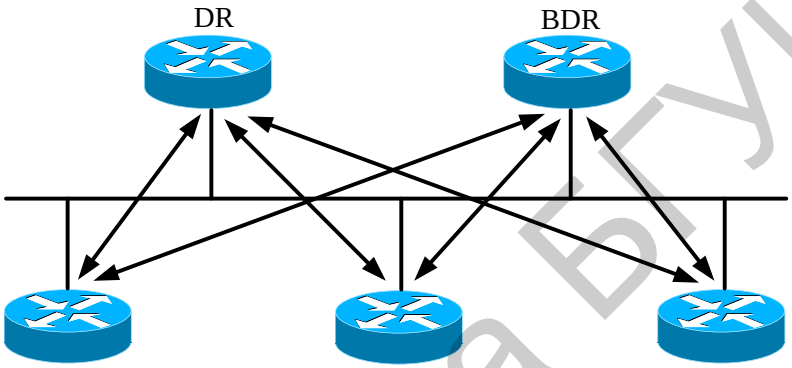


Рис. 1.4. Маршрутизаторы DR и BDR получают сообщения LSA

В сетях типа «точка – точка» существуют только два узла и поэтому маршрутизаторы DR и BDR не выбираются. Оба маршрутизатора соединения типа «точка – точка» являются друг для друга полностью смежными устройствами.

1.1.4. Протокол приветствия (Hello) стека протоколов OSPF

Начиная процесс OSPF-маршрутизации, маршрутизатор посылает пакет приветствия Hello на интерфейс и далее регулярно рассылает такие пакеты.

Правила обмена пакетами OSPF Hello в совокупности называются протоколом Hello (Hello protocol). На третьем уровне эталонной модели OSI пакеты Hello рассматриваются как пакеты многоадресатной рассылки с адресом 224.0.0.5. Этот адрес можно рассматривать как рассылку «всем OSPF-маршрутизаторам». OSPF-маршрутизаторы используют пакеты Hello для инициирования новых отношений смежности и для того, чтобы удостовериться в том, что соседние маршрутизаторы по-прежнему функционируют. По умолчанию пакеты Hello рассылаются каждые 10 с по широковещательным сетям множественного доступа и по сетям соединений типа «точка – точка». На интерфейсах, подсоединенных к сетям NBMA, пакеты Hello рассылаются каждые 30 с. В сетях множественного доступа, согласно протоколу OSPF, выбирается

назначенный маршрутизатор (DR) и резервный назначенный маршрутизатор (BDR).

Хотя пакет Hello имеет небольшой размер, он содержит заголовок пакета OSPF, как показано на рис. 1.5. В поле тип пакета Hello содержится значение 1.

Версия	Тип	Длина пакета
ID маршрутизатора		
ID зоны		
Контрольная сумма		Тип аутентификации
Данные аутентификации		

Рис. 1.5. Заголовок пакета OSPF

1.1.5. Операции протокола OSPF

В процессе своего функционирования OSPF-маршрутизаторы должны выполнять следующие операции.

1) Установить отношения смежности с другими маршрутизаторами.

2) Выбрать назначенный маршрутизатор (DR) и резервный назначенный маршрутизатор (BDR) (если в этом есть необходимость).

3) Проанализировать возможные маршруты.

4) Выбрать оптимальные маршруты для дальнейшего использования.

5) Поддерживать текущее состояние информации маршрутизации.

1.1.6. Конфигурирование протокола OSPF для одной зоны

Для того чтобы сконфигурировать на маршрутизаторе протокол OSPF, необходимо включить этот протокол и сконфигурировать сетевые адреса маршрутизатора и задать информацию о зоне, выполнив следующие действия.

Этап 1. Включить на маршрутизаторе использование протокола OSPF, используя команду `router(config)# router ospf` *`process-id`*.

Идентификатор ID процесса (аргумент *`process-id`*) является номером процесса на локальном маршрутизаторе. Этот идентификатор ID используется для идентификации одного процесса среди нескольких процессов, работающих на одном и том же маршрутизаторе. Этот номер может быть любым значением из диапазона от 1 до 65535. Нумерация процессов не обязательно должна начинаться с 1. Большинство сетевых администраторов используют один и тот же ID процесса во всей автономной системе AS. На одном и том же маршрутизаторе могут выполняться несколько OSPF-процессов, однако это не рекомендуется, поскольку в этом случае создается несколько экземпляров баз данных, которые увеличивают служебную нагрузку на маршрутизатор.

Этап 2. Идентифицировать IP-сети на маршрутизаторе, используя команду `router (conf ig-router) # network` *`address wildcard-mask`* `area` *`area-id`*.

Для каждой сети необходимо задать зону, к которой принадлежит эта сеть. Значение *address* может быть адресом сети, подсети или адресом интерфейса.

О том, как следует интерпретировать адрес, маршрутизатор узнает путем сравнения его с маской шаблона. Эта маска необходима, потому что протокол OSPF, в отличие от протоколов RIPv1 и IGRP, поддерживает маршрутизацию CIDR и VLSM. Аргумент *area-id* является обязательным даже в том случае, когда протокол OSPF конфигурируется лишь в одной отдельной зоне. Вновь следует отметить, что к одной зоне могут принадлежать несколько IP-сетей. Проектирование и реализация больших сетей OSPF начинается с конфигурирования маршрутизации OSPF в отдельной зоне. Протокол OSPF конфигурируется аналогично другим протоколам маршрутизации. Некоторые отличия состоят в том, как отдельные сети анонсируются и включаются в директиву `network`. Это вызвано тем, что протокол OSPF является протоколом состояния канала, а не дистанционно-векторным (как, например, протоколы RIPvl и IGRP).

Для успешного функционирования протоколу OSPF требуются идентификатор процесса (process identifier – process ID) и идентификатор маршрутизатора (Router Identifier – router ID). Идентификатор маршрутизатора берется с активного интерфейса. Если этот интерфейс выходит из строя, то данный процесс OSPF продолжаться не может. Для обеспечения устойчивой работы протокола OSPF в качестве идентификатора маршрутизатора конфигурируется адрес петлевого интерфейса (Loopback Address). Дополнительно в сетях множественного доступа выбирается назначенный маршрутизатор (Designated Router – DR). При распространении информации о состоянии канала этот маршрутизатор выступает от имени всех остальных маршрутизаторов. Возможна ситуация, когда в качестве назначенного маршрутизатора требуется выбрать некоторый заранее указанный маршрутизатор. В этом случае данному маршрутизатору присваивается наивысший приоритет.

1.1.7. Конфигурирование адреса петлевого интерфейса

Когда начинается процесс функционирования протокола OSPF, операционная система IOS Cisco использует наибольший локальный IP-адрес в качестве идентификатора своего OSPF-маршрутизатора. Если конфигурируется адрес петлевого интерфейса, то, независимо от его значения, используется этот адрес. IP-адрес петлевого интерфейса может быть назначен с помощью следующих команд:

```
router(config)#interface loopback number
router(config-if)#ip address ip-address subnet-mask
```

ID маршрутизатора, полученный с петлевого интерфейса, обеспечивает устойчивость сети, поскольку на его функционирование не влияют возможные сбои в работе канала. Адрес петлевого интерфейса должен быть сконфигурирован до того, как OSPF-процесс начнет искать интерфейс, который заменит интерфейс с наибольшим IP-адресом. Рекомендуется использовать адрес петлево-

го интерфейса на всех ключевых маршрутизаторах OSPF-сети. Для того чтобы избежать проблем с маршрутизацией, рекомендуется при конфигурировании IP-адреса петлевого интерфейса использовать 32-битовую маску подсети, как показано в примере 1.

Пример 1. Конфигурирование петлевого интерфейса с использованием маски узла:

```
router (config)#interface loopback0
router(config-if)#ip address 192.168.1.1
255.255.255.255
```

32-битовая маска иногда называется маской узла, поскольку она относится только к одному узлу, а не к сети или подсети.

1.1.8. Изменение приоритета OSPF-маршрутизатора

На выбор маршрутизаторов DR/BDR пользователь может повлиять путем конфигурирования на маршрутизаторе значения приоритета, отличного от значения по умолчанию (равного единице). Присвоение маршрутизатору значения приоритета, равного нулю, гарантирует, что этот маршрутизатор не будет выбран в качестве назначенного маршрутизатора (DR) или резервного (BDR). Каждый OSPF-интерфейс может иметь свое, отличное от других, значение приоритета. Значение приоритета (число в интервале от 0 до 255) может быть сконфигурировано с помощью команды `priority`, имеющей следующий синтаксис:

```
Router(config-if)#ip ospf priority number
```

Для задания интерфейсу EO приоритета, равного нулю (с тем чтобы он не был выбран в качестве маршрутизатора DR/BDR), следует использовать команды, привенные в примере 2.

Пример 2. Задание маршрутизатору приоритета, равного нулю:

```
RTB(config)#interface e0
RTB(config-if)#ip ospf priority 0
```

Для того чтобы значение приоритета было учтено в процессе выбора маршрутизатора DR/BDR, оно должно быть установлено до того, как этот выбор будет производиться. Значение приоритета и другая существенная информация могут быть выведены с помощью команды `show ip`.

Чем выше приоритет маршрутизатора, тем более вероятно, что он будет выбран в качестве назначенного (DR). Изменить приоритет интерфейса, участвующего в работе протокола OSPF, можно с помощью команды `ip ospf priority`.

1.1.9. Изменение метрики, используемой протоколом OSPF для присвоения оценки каналу

Протокол OSPF использует оценку в качестве метрики при определении наилучшего маршрута. Операционная система IOS Cisco автоматически вычис-

ляет оценку на основе ширины полосы пропускания интерфейса. Для вычисления оценки используется следующая формула:

$$10^8 / (\text{ширина полосы пропускания})$$

Для того чтобы протокол OSPF правильно вычислял характеристики маршрутов, необходимо, чтобы все интерфейсы, подсоединенные к какому-либо каналу, договорились о его оценке. Эта оценка может быть изменена, для того чтобы оказать влияние на результат вычисления протоколом OSPF его оценки. Наиболее типичной ситуацией, в которой требуется изменять оценку, является использование маршрутизаторов разных производителей. Это связано с тем, что оценки канала, сделанные различными устройствами, могут оказаться отличными друг о друга.

Каналы имеют оценки по умолчанию, которые присваиваются на основе технологии, используемой для реализации данного канала. Сетевой администратор может изменить метрику оценки канала, используемую протоколом OSPF. В табл. 1.4 приведены оценки каналов, принимаемые по умолчанию.

Таблица 1.4

Стандартные оценки протокола OSPF

Передающая среда	**Оценка**
Последовательный канал 56 кбит/с	1785
T1 (последовательный канал 1,544 Мбит/с)	64
E1 (последовательный канал 2,048 Мбит/с)	48
Сеть Ethernet 10 Мбит/с	10
Сеть Token Ring 16 Мбит/с	6
100 Mbps Fast Etherner, FDDI	1

Задание оценки каналу осуществляется с использованием следующей команды конфигурирования интерфейса:

```
Router(config-if)#ip ospf coat number
```

Значение параметра *number* может находиться в интервале от 1 до 65535. Альтернативным способом влияния на оценку канала протоколом OSPF является задание на интерфейсе значения полосы пропускания. Чем меньше число, тем лучшим считается канал.

Пример 3. Задание ширины полосы пропускания в протоколе OSPF:

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
```

Для данного последовательного интерфейса стандартным значением ширины полосы пропускания является 1544.

1.1.10. Конфигурирование аутентификации в протоколе OSPF

Уровень безопасности в сети повышается, если известно, что информация о маршрутизации поступила из конкретного источника. Протокол OSPF позволяет маршрутизаторам выполнять взаимную аутентификацию. По умолчанию

маршрутизатор полагается на то, что информация о маршрутах поступает от того маршрутизатора, который должен ее отправлять. Маршрутизатор также полагается на то, что в процессе передачи эта информация не была искажена. Для того чтобы гарантировать это, на маршрутизаторах одной зоны может быть сконфигурирована взаимная аутентификация.

Аутентификация представляет собой другой тип конфигурирования отдельных интерфейсов. Каждому OSPF-интерфейсу маршрутизатора может быть задан отличный от других ключ аутентификации, который выполняет функции пароля для маршрутизаторов OSPF одной и той же зоны. При конфигурировании OSPF-аутентификации используется команда со следующим синтаксисом:

```
router(config-if)#ip ospf authentication-key password
```

После того как сконфигурирован пароль, в зоне можно включить функцию аутентификации с помощью команды (эта команда должна быть выполнена на всех маршрутизаторах, участвующих в аутентификации), имеющей следующий синтаксис:

```
router(config-router)#area number authentication
[message-digest]
```

Хотя ключевое слово `message-digest` не является обязательным, рекомендуется всегда использовать его в данной команде. По умолчанию пароли аутентификации пересылаются открытым текстом. Поэтому анализатор пакетов (packet sniffer) легко может перехватить пакет OSPF и расшифровать пароль. Однако при использовании ключевого слова `message-digest` вместо самого пароля пересылается дайджест сообщения, или хеш пароля. Если у получателя сконфигурирован соответствующий ключ аутентификации, то потенциальный взломщик не сможет понять смысл этого дайджеста.

Если выбрана аутентификация с использованием дайджеста сообщения, то ключ аутентификации не используется. Вместо этого на интерфейсе OSPF-маршрутизатора должен быть сконфигурирован ключ дайджеста сообщения. Эта команда имеет следующий синтаксис:

```
router(config-if)#ip ospf message-digest-key key-id
md5 [encryption-type] password
```

Аутентификация MD5 создает дайджест сообщения. Он представляет собой кодированные данные, созданные на базе пароля и содержания пакета. Маршрутизатор-получатель использует для восстановления дайджеста совместно используемый пароль и этот пакет. Если дайджесты совпадают, то маршрутизатор считает, что источнику пакета можно доверять и содержимое пакета не было искажено или подделано в процессе передачи.

Тип аутентификации указывает вид аутентификации, если она используется. В случае аутентификации с использованием дайджеста сообщения пакет данных аутентификации содержит идентификатор ключа и длину приложенного к пакету дайджеста. Дайджест сообщения можно сравнить с водяным знаком, который не может быть подделан.

1.1.11. Распространение в сети маршрута по умолчанию

Для получения доступа к сетям, которые не присутствуют в таблице маршрутизации, на граничном маршрутизаторе должен быть задан маршрут по умолчанию. Эта информация о маршруте по умолчанию должна быть распространена между всеми маршрутизаторами зоны протокола OSPF.

При использовании OSPF-маршрутизации таблицы маршрутизации домена позволяют получить доступ ко всем входящим в него сетям. Однако пользователям домена OSPF необходимо также получать доступ к сетям, не принадлежащим этому домену (например, к глобальной сети Интернет).

Существует необходимость в стандартном маршруте, который бы позволял маршрутизаторам пересылать пакеты с неизвестными адресами в направлении маршрутизатора, в таблице маршрутизации которого, возможно, имеется адрес сети получателя для данного пакета. Сконфигурированный стандартный маршрут используется маршрутизаторами для генерирования «шлюза последней надежды» («Gateway of Last Resort»). `B` приведенной ниже команде конфигурируется стандартный статический маршрут к сети `0.0.0.0` с маской подсети `0.0.0.0`:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [interface
| next-hop address]
```

Этот маршрут соответствует любому сетевому адресу, поскольку согласно правилу адрес шлюза получается путем применения операции AND к адресу пункта назначения и маске подсети.

При использовании этой команды все маршрутизаторы данной зоны протокола OSPF будут знать этот стандартный маршрут при условии, что функционирует интерфейс граничного маршрутизатора, соединенный с этим стандартным маршрутом.

1.1.12. Тестирование конфигурации протокола OSPF

Для тестирования конфигурации протокола OSPF используется ряд команд show. Эти команды приведены в табл. 1.5.

1.1.13. Виртуализация сетей

Виртуальная локальная сеть (Virtual Local-area Network – VLAN) представляет собой группу устройств одной или более локальных сетей LAN, которые конфигурируются с использованием управляющего программного обеспечения таким образом, чтобы они могли осуществлять связь между собой, как если бы они находились в одном сегменте локальной сети, в то время как они фактически находятся в различных сегментах.

Таблица 1.5

Команды протокола OSPF и команды вывода статистических данных

Команда	Описание
`show ip protocol`	Отображает параметры таймеров, фильтров, метрики, параметры сети и другую информацию, относящуюся ко всему маршрутизатору
`show ip route`	Отображает известные маршрутизатору маршруты и источники, из которых они получены. Использование этой команды является одним из лучших способов проверить соединение локального маршрутизатора с остальной частью объединенной сети
`show ip ospf interface`	Проверяет, были ли сконфигурированы интерфейсы в требуемых зонах. Если не указан адрес петлевого интерфейса, то адрес этого интерфейса рассматривается как идентификатор данного маршрутизатора. Эта команда также выводит значения интервалов таймеров, включая интервал рассылки сообщений Hello и отображает отношения смежности с соседними устройствами
`show ip ospf`	Выводит число выполнений алгоритма выбора кратчайшего пути (Shortest Path First – SPF). Она также выводит значение интервала рассылки сообщений об изменениях в состоянии канала в условиях, когда изменений в топологии сети не происходит
`show ip ospf neighbor detail`	Отображает подробный список соседних устройств, их приоритеты и состояние
`show ip ospf database`	Отображает содержимое топологической базы данных, поддерживаемой данным маршрутизатором. Эта команда также отображает ID маршрутизатора и ID OSPF-процесса. При использовании в данной команде различных ключевых слов может быть отображен ряд типов баз данных
`clear ip route`	Очищает всю IP-таблицу маршрутизации
`clear ip route a.b.c.d`	Удаляет из таблицы маршрутизации только маршрут, заданный адресом a.b.c.d
`debug ip ospf`	Выполняет отладку операций протокола OSPF

Одной из важных функций, реализуемых в технологии Ethernet, являются виртуальные локальные сети VLAN, в которых для объединения рабочих станций и серверов в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN-сети, возможна только с устройствами этой же сети, поэтому сеть с коммутацией функционирует как несколько индивидуальных, не соединенных друг с другом локальных сетей LAN.

Трудно дать общее строгое определение сетей VLAN, поскольку разные производители используют различные подходы к созданию таких сетей.

Компании часто используют сети VLAN в качестве способа логической группировки пользователей. Это можно сравнить с традиционной организацией рабочих мест, в которой несколько отделов группируются в локальный департамент и локальная сеть решает задачи связи для этого департамента. В настоящее время сотрудники часто не связаны с конкретным физическим рабочим местом, поэтому сети VLAN создают не физическую, а логическую группу пользователей. Например, сотрудники, работающие в отделе маркетинга, объединены VLAN-сетью маркетинга, а сотрудники инженерного подразделения – VLAN-сетью инженерных служб.

Сети VLAN решают задачи масштабирования сети, обеспечения безопасности и сетевого управления. В сетях с топологией VLAN маршрутизаторы обеспечивают фильтрацию широковещания, решают задачи защиты сети и управления потоками данных.

Сеть VLAN представляет собой группу сетевых устройств и служб, не ограниченную физическим сегментом или коммутатором. Сети VLAN логически сегментируют сети, использующие коммутацию, на основе их организационных функций, принадлежности к различным рабочим коллективам (группам) или используемым приложениям, а не на базе физического или географического расположения. Например, все рабочие станции и серверы, используемые некоторой рабочей группой, могут быть объединены в одну и ту же сеть VLAN, независимо от их физического подсоединения к сети или расположения на территории предприятия.

На рис. 1.6 показано физическое проектирование сети VLAN, основанное на различных рабочих группах компании и их расположении на различных этажах офиса. В данном случае сеть VLAN создается для каждого отдела (инженерный отдел, отдел маркетинга и отдел учета), в каждом из которых имеется свой коммутатор.

Соединения клиентской рабочей станции, находящейся в сети VLAN, ограничены только файловыми серверами, принадлежащими этой же сети VLAN. Сеть VLAN можно рассматривать как широковещательный домен, который существует в определенном наборе коммутаторов. Сети VLAN состоят из ряда конечных систем, таких, как рабочие станции или сетевые устройства (мосты и маршрутизаторы), соединенных друг с другом через отдельный мостовой домен. Мостовой домен поддерживается различными сетевыми устройствами, такими, например, как коммутаторы сетей LAN, которые работают по мостовым протоколам; при этом для каждой сети VLAN имеется своя мостовая группа.

Сети VLAN создаются для реализации служб сегментации, которые в традиционных LAN-конфигурациях обычно обеспечиваются маршрутизаторами. В топологиях сетей VLAN маршрутизаторы обеспечивают фильтрацию широковещания (broadcast), защиту сети и управление потоками данных. Коммутаторы не могут осуществлять мостовые соединения между сетями VLAN,

поскольку это нарушило бы целостность широковещательного домена сети VLAN. Маршрутизация потоков данных должна происходить только при передаче данных между сетями VLAN.

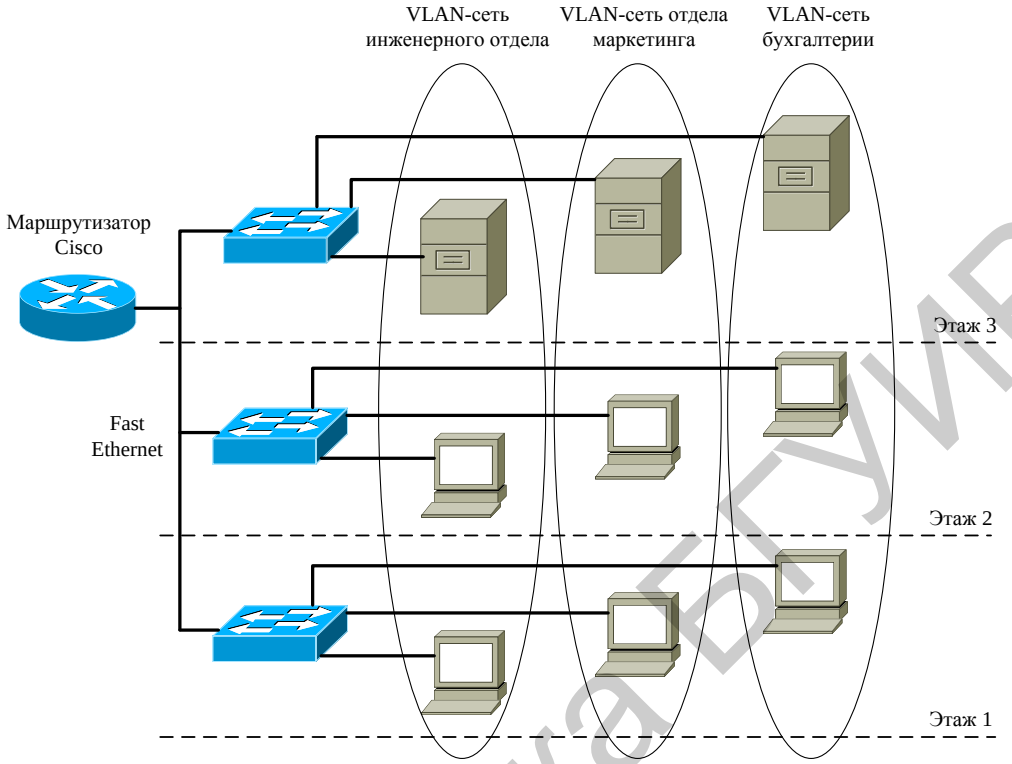


Рис. 1.6. Сети VLAN охватывают определенное физическое пространство

1.1.14. Функционирование сети VLAN

Сеть VLAN представляет собой сеть коммутации, которая логически сегментируется в соответствии с выполняемыми функциями, объединением сотрудников в группы или согласно используемым приложениям, независимо от физического расположения пользователей. Сети VLAN может быть выделен любой порт коммутатора. Порты, выделенные одной и той же сети VLAN, имеют общее пространство широковещания.

Порты, не принадлежащие этой сети VLAN, не получают эти широковещательные сообщения. Это повышает общую производительность сети, поскольку уменьшается количество ненужных широковещательных сообщений, которые потребляют полосу пропускания сети. Сети VLAN создаются двумя способами: статически и динамически.

Статические сети – этот способ также называется членством на базе порта. Назначение портов сетям VLAN создает статическое распределение VLAN. Когда устройство подсоединяется к порту, оно автоматически попадает во VLAN-сеть этого порта. Если устройство меняет порт своего подключения, но ему требуется доступ к той же самой сети VLAN, то сетевой администратор должен сделать назначение порта сети VLAN для нового соединения.

Динамические сети VLAN – сети, которые создаются с использованием пакетного программного обеспечения, такого, как CiscoWorks 2000. С помощью

сервера политик управления сетями VLAN (VLAN Management Policy Server – VMPS) можно назначать порты коммутатора сетям VLAN динамически – на основе MAC-адреса устройства-источника, подсоединенного к данному порту. Когда устройство присоединяется к сети, оно делает запрос в базу данных на сервере VMPS относительно своей принадлежности к данной сети VLAN.

Принадлежность устройства к статической сети VLAN на основе портов проиллюстрировано на рис. 1.7. Конкретной сети VLAN назначается порт, который не зависит от пользователя или системы, подсоединенной к данному порту. Это означает, что все пользователи, подсоединенные к данному порту, должны быть членами одной и той же сети VLAN. Отдельная рабочая станция пользователя или концентратор, к которому подсоединены несколько рабочих станций, могут быть подсоединены к отдельному порту коммутатора. Назначение портов сетям VLAN обычно осуществляет сетевой администратор. Конфигурация порта в этом случае является статической, и переключение порта на другую VLAN не может быть выполнено автоматически без реконфигурирования коммутатора. Следует обратить внимание на то, что каждая сеть VLAN находится в отдельной подсети, а маршрутизатор используется для связи между этими подсетями.

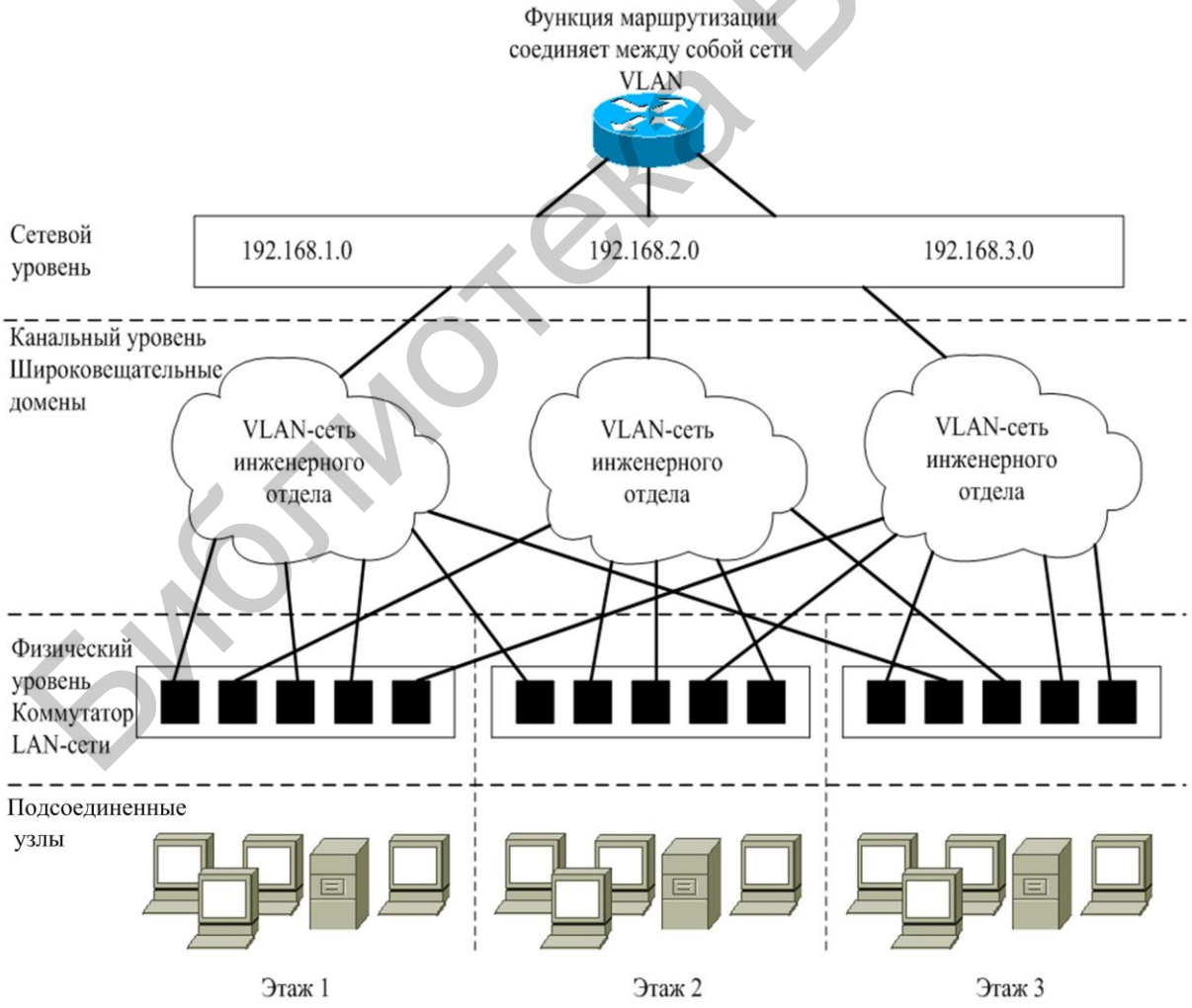


Рис. 1.7. Статические виртуальные сети на основе портов

Когда пользователи подсоединяются к этому совместно используемому сегменту, как это происходит в традиционных основанных на концентраторах сетях LAN, все они после этого используют общую полосу пропускания. На каждого дополнительного пользователя, который подсоединяется к совместно используемой среде передачи, приходится меньше доступной полосы пропускания, поскольку все пользователи находятся в одном и том же коллизионном домене. Если количество пользователей, использующих одну и ту же полосу пропускания становится слишком большим, то начинаются частые коллизии и работа приложения пользователя становится малопроизводительной.

Коммутаторы уменьшают вероятность коллизий за счет обеспечения выделенной полосы пропускания между устройствами с помощью микросегментации; однако коммутаторы по-прежнему рассылают всем пользователям широковещательные сообщения, такие, как сообщения протокола ARP. Сети VLAN обеспечивают пользователям большую полосу пропускания в совместно используемой сети путем создания отдельных широковещательных доменов.

По умолчанию на каждом порте коммутатора имеется сеть VLAN1 или сеть VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Следует помнить о том, что каждый интерфейс коммутатора ведет себя как порт моста и в целом коммутатор можно рассматривать как многопортовый мост. Мосты отфильтровывают потоки данных, которые не требуется направлять в иные сегменты, кроме того, из которых они поступили. Если фрейм необходимо переслать через мост и MAC-адрес получателя известен, то мост направляет этот фрейм на соответствующий интерфейс и не направляет на все остальные. Если мосту или коммутатору не известно расположение получателя, то происходит лавинная рассылка фрейма со всех портов в данный широковещательный домен (VLAN), за исключением того порта, с которого этот фрейм поступил.

Каждой виртуальной сети VLAN должен быть присвоен уникальный адрес 3-го уровня (сети или подсети). Это помогает осуществлять коммутацию пакетов между сетями VLAN, в которых имеются маршрутизаторы. Сети VLAN могут выступать в качестве сквозных сетей (end-to-end network), которые охватывают всю среду коммутатора, и существовать в определенных географических границах.

1.1.15. Конфигурирование статических VLAN-сетей

Под статическими VLAN понимаются порты коммутатора, которым вручную назначаются сети VLAN путем использования управляющего программного обеспечения или непосредственным конфигурированием коммутатора. Эти порты поддерживают назначенную им конфигурацию VLAN сетей до тех пор, пока она не будет изменена системным администратором. Хотя статические VLAN требуют внесения изменений вручную, они безопасны, легко

конфигурируются и удобны для мониторинга. Этот тип VLAN хорошо работает в сетях, в которых соблюдаются следующие условия:

– перемещения станций легко контролируются и управляются;

– имеется надежное управляющее программное обеспечение для конфигурирования портов коммутатора;

– имеется нежелательная дополнительная служебная нагрузка, требуемая для поддержки MAC-адресов конечных станций и типовых таблиц фильтрации.

Динамические VLAN, в отличие от статических, не используют порты, на которых назначаются конкретные VLAN-сети. Вместо этого назначение VLAN-сетей портам основывается на MAC-адресах, логической адресации или типе протокола. При конфигурировании статических VLAN-сетей на маршрутизаторах Cisco 29xx следует помнить следующие основные положения:

– максимальное количество подключаемых VLAN-сетей зависит от типа коммутатора и ограничивается количеством его портов;

– сеть VLAN1 является одной из VLAN-сетей, создаваемых по умолчанию производителем;

– по умолчанию VLAN1 является VLAN-сетью;

– по сети VLAN1 рассылаются анонсирования маршрутов протокола обнаружения устройств Cisco (Cisco Discovery Protocol – CDP) и магистрального протокола VLAN (VLAN Trunking Protocol – VTP);

– на всех коммутаторных магистралях, принимающих участие в работе VLAN-сетей, должен быть сконфигурирован один и тот же протокол инкапсуляции, такой, как 802.1Q или ISL;

– команды конфигурирования VLAN-сетей зависят от номера модели;

– IP-адреса для моделей Catalyst 29xx находятся в широковещательном домене VLAN;

– при создании, добавлении и удалении VLAN-сетей коммутатор должен находиться в режиме VTP-сервера.

Создание на коммутаторе статической VLAN-сети является несложной задачей. При использовании коммутатора, работающего с командами IOS Cisco, следует войти в режим конфигурирования VLAN с помощью команды привилегированного EXEC-режима `vlan database`. Для создания VLAN-сети следует выполнить приведенные ниже команды.

```
Switch#vlan database
Switch (vlan)#vlan vlan_number [ vlan_name]
Switch(vlan)#exit
```

При необходимости следует также сконфигурировать имя VLAN-сети.

После выхода из режима конфигурирования на коммутаторе создается VLAN-сеть. Следующим этапом является назначение данной VLAN одному или более интерфейсам.

```
Switch(config)#interface fa 0/3
Switch(config-if)#switchport access vlan 2
```

Протестировать конфигурацию можно с помощью команды `show running-config`.

1.1.16. Тестирование и сохранение конфигурации VLAN-сети

Хорошей практикой является тестирование конфигурации VLAN-сети с помощью команд `show vlan`, `show vlan brief` или `show vlan id` *`id number`*.

При работе с VLAN-сетями следует руководствоваться следующими положениями:

– созданная VLAN-сеть остается неиспользуемой до тех пор, пока она не будет логически связана с портами коммутатора;

– по умолчанию все порты Ethernet находятся в сети VLAN1;

– между номерами портов не следует вводить пробелы; в этом случае коммутатор выдает сообщение об ошибке, поскольку пробел отделяет другой аргумент, который не является структурной частью команды.

Полезно иметь копию конфигурации VLAN-сети в виде текстового файла в качестве резервной копии и для целей аудита. Если в файле конфигурации окажутся скопированными посторонние символы, то их следует удалить. Ниже описаны действия, которые следует выполнить для копирования конфигурации VLAN-сети.

Этап 1. С консоли коммутатора перейти в привилегированный режим конфигурирования коммутатора.

Этап 2. В окне программы HyperTerminal выбрать опцию Transfer (Передача).

Этап 3. Выбрать опцию Capture Text.

Этап 4. Выбрать место сохранения файла конфигурации.

Этап 5. Задать имя файла конфигурации VLAN-сети.

Этап 6. Выбрать опцию Start.

Этап 7. На коммутаторе выполнить команду show run.

Этап 8. После того как будут выполнены команды файла конфигурации, (для окончания их выполнения следует нажать несколько раз клавишу пробел), вернуться к опции Transfer окна программы HyperTerminal, выбрать опцию Capture Text, а затем опцию Stop для сохранения и закрытия файла.

Этап 9. Удалить посторонние символы.

1.2. Алгоритм Дейкстры

1.2.1. Описание алгоритма Дейкстры

Основой любого протокола маршрутизации является алгоритм маршрутизации. Для протокола OSPF – это алгоритм поиска кратчайшего расстояния Дейкстры. С точки зрения математики алгоритм Дейкстры является алгоритмом поиска на графе (поиска кратчайших путей), а сеть ассоциируется с графом, вершины которого образуют узлы сети, а ребра – соединительные линии между

узлами. Каждому ребру назначается метрика (метка), ассоциируемая с длинной пути между двумя соседними вершинами. В алгоритмах маршрутизации в качестве длины пути используется количество «хопов» (узлов, через которые проходит пакет).

Алгоритм Дейкстры выполняется только для графов с положительными ребрами и состоит из двух частей: инициализирующей и итерационной.

В инициализирующей части определяются начальные значения меток для всех вершин и назначается вершина графа, для которой будет производиться поиск кратчайших путей до всех остальных вершин.

Итерационная часть включает циклы, внутри которых выполняется обработка текущей вершины и вычисляются кратчайшие пути до всех вершин, соседствующих с обрабатываемой. В каждом цикле обрабатывается (посещается) одна вершина и делается попытка уменьшить значения меток ее соседей. Метка в данном случае – это кратчайший путь от рассматриваемой вершины до исходной. Условием выхода из цикла и прекращения выполнения алгоритма Дейкстры является посещение всех вершин.

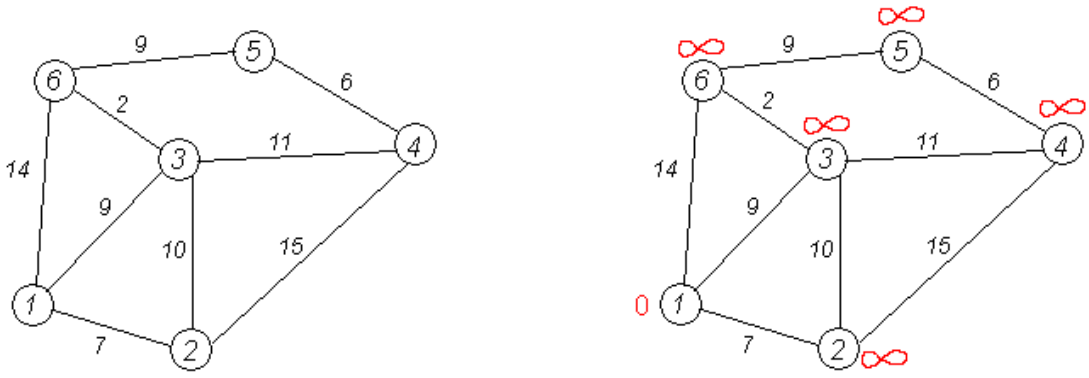
Алгоритм выполняется следующим образом. При инициализации метка исходной вершины, для которой выполняется поиск кратчайших путей до других вершин, полагается равной нулю. Метки остальных вершин полагаются равными бесконечности. Это отражает тот факт, что расстояния от исходной вершины до других вершин неизвестны. Все вершины графа помечаются как непосещенные.

Затем выполняется некоторое количество циклов обработки соседних вершин – по одному циклу на каждую вершину графа. В конце каждого цикла соответствующая обработанная вершина помечается как посещенная.

Каждый цикл начинается с поиска непосещенных вершин. Если непосещенных вершин в графе нет, то выполняется выход из цикла и завершение алгоритма. В противном случае из еще непосещенных вершин выбирается вершина с минимальной меткой. Вершины, в которые ведут ребра из выбранной вершины, образуют множество соседей выбранной вершины. Для каждой соседней вершины, кроме отмеченных как посещенные, вычисляется новая длина пути, равная сумме значений текущей метки выбранной вершины и длины ребра, соединяющего выбранную вершину с ее рассматриваемой соседней вершиной. Если полученное значение длины меньше значения метки соседней вершины, выполняется замена значения метки на значение полученной длины пути. Далее выбранная вершина помечается как помеченная и осуществляется переход в начало следующего цикла обработки.

1.2.2. Пример выполнения алгоритма Дейкстры

В качестве примера выполнения алгоритма Дейкстры рассмотрим поиск кратчайших путей от вершины 1 до остальных вершин для графа, представленного на рис. 1.8, *а*. Вершины графа обозначены кругами с номерами. Ребра графа обозначены линиями. Для каждого ребра указана метка, означающая длину пути.



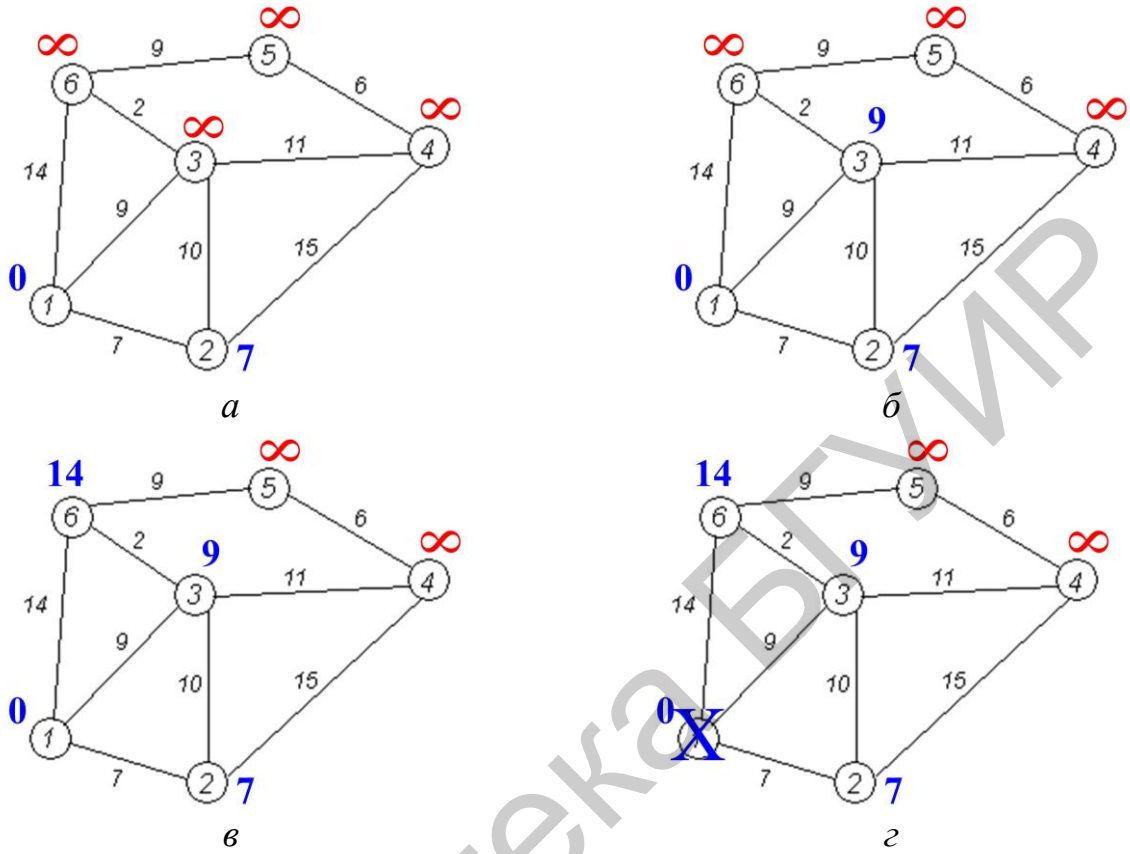
а *б*

Рис. 1.8. Графы для поиска кратчайших путей:
а – исходный граф; *б* – граф после инициализации

При инициализации вершине 0 присваивается метка 0, так как эта вершина является исходной при поиске кратчайших путей (рис. 1.8, *б*). Остальным вершинам графа присваиваются метки «бесконечность», что означает неопределенность путей до этих вершин. Все вершины графа считаются непосещенными (необработанными).

В цикле 1 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат. Осуществляется поиск вершины с минимальной меткой. Выбирается вершина 1, так как она имеет нулевую метку, а остальные вершины имеют метки «бесконечность». Определяются непосещенные соседние вершины для выбранной вершины 1. Это вершины 2, 3 и 6. Все эти соседние вершины имеют одинаковые метки «бесконечность». Поэтому для обработки может быть выбрана любая вершина. Пусть это будет вершина 2 (рис. 1.9, *а*). Для вершины 2 рассчитывается длина пути 1-2. Это сумма значений метки выбранной вершины 1 и метки ребра 1-2, равная 0 + 7 = 7. Длина пути 1-2 сравнивается с меткой вершины 2. Так как длина пути 1-2 меньше значения метки вершины 2, осуществляется замена метки «бесконечность» в вершине 2 на метку 7. Из двух оставшихся соседних вершин 3 и 6 минимальную метку ребра, соединяющего каждую из этих вершин с выбранной вершиной 1, имеет вершина 3 (метка 9). Поэтому, следующей обрабатывается вершина 3 (рис. 1.9, *б*). Для вершины 3 рассчитывается длина пути 1-3. Это сумма значений метки выбранной вершины 1 и метки ребра 1-3, равная 0 + 9 = 9. Длина пути 1-3 сравнивается с меткой вершины 3. Так как длина пути 1-3 меньше значения метки вершины 3, осуществляется замена метки «бесконечность» в вершине 3 на метку 9. Для выбранной вершины 1 остается необработанной соседняя вершина 6, ребро 1-6 которой имеет метку 14. Для вершины 6 рассчитывается длина пути 1-6 (рис. 1.9, *в*). Это сумма значений метки выбранной вершины 1 и метки ребра 1-6, равная 0 + 14 = 14. Длина пути 1-6 сравнивается с меткой вершины 6. Так как длина пути 1-6 меньше значения метки вершины 6, осуществляется замена метки «бесконечность» в вершине 6 на метку 14. Так как все соседние вершины для выбранной вершины 1 уже обработаны, вершина 1 помечается как посещенная (вычеркивается из списка обработки) и цикл

обработки завершается (рис. 1.9, *г*). В результате выполнения цикла 1 устанавливаются кратчайшие маршруты от исходной вершины 1 до вершин 2, 3 и 6. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9, маршрут 1-6 длиной 14.



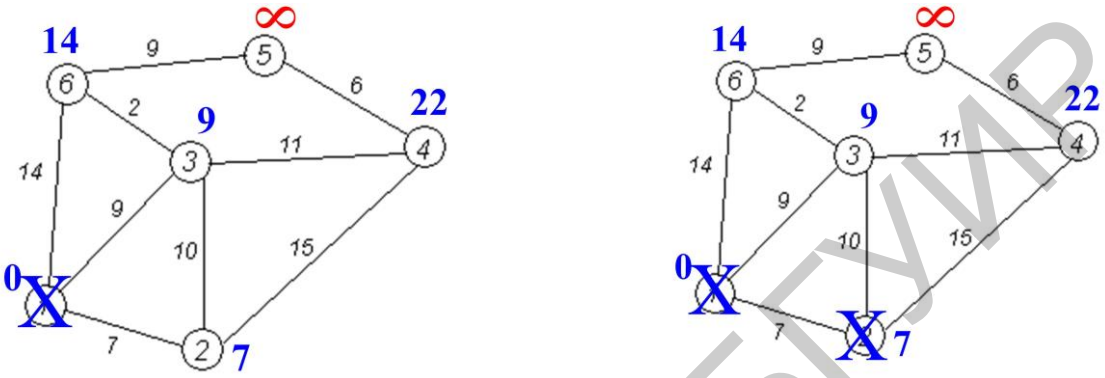
а *б*

в *г*

Рис. 1.9. Цикл 1 поиска кратчайших путей на графе:
а – обработка вершины 2; *б* – обработка вершины 3;
в – обработка вершины 6; *г* – «вычеркивание» вершины 1

В цикле 2 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат. Осуществляется поиск вершины с минимальной меткой. Выбирается вершина 2, так как она имеет метку 7, а остальные вершины имеют метки с большими значениями. Определяются непосещенные соседние вершины для выбранной вершины 2. Это вершины 3 и 4. Соседняя вершина 3 имеет меньшее значение метки (метка 9), чем соседняя вершина 4 (метка «бесконечность»). Поэтому первой обрабатывается вершина 3 (см. рис. 1.9, *г*). Для вершины 3 рассчитывается длина пути 1-2-3. Это сумма значений метки выбранной вершины 2 и метки ребра 2-3, равная 7 + 10 = 17. Длина пути 1-2-3 сравнивается с меткой вершины 3. Так как длина пути 1-2-3 больше значения метки вершины 3, то замена метки 9 в вершине 3 на метку 17 не осуществляется. Для выбранной вершины 2 остается необработанной соседняя вершина 4, ребро 2-4 которой имеет метку 15. Для вершины 4 рассчитывается длина пути 1-2-4 (см. рис. 1.9, *б*). Это сумма значений метки выбранной вершины 2 и метки ребра 2-4, равная 7 + 15 = 22. Длина пути 1-2-4 сравнивается с меткой вершины 4. Так как длина пути 1-2-4 меньше значения метки вер-

шины 4, осуществляется замена метки «бесконечность» в вершине 4 на метку 22 (рис. 1.10, *а*). Так как все соседние вершины для выбранной вершины 2 уже обработаны, вершина 2 помечается как посещенная (вычеркивается из списка обработки) и цикл обработки завершается (рис. 1.10, *б*). В результате выполнения цикла 2 устанавливаются кратчайшие маршруты от исходной вершины 1 до вершины 4. Это маршрут 1-2-4 длиной 22. Остаются актуальными кратчайшие маршруты от исходной вершины 1 до вершин 2, 3 и 6. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9, маршрут 1-6 длиной 14.

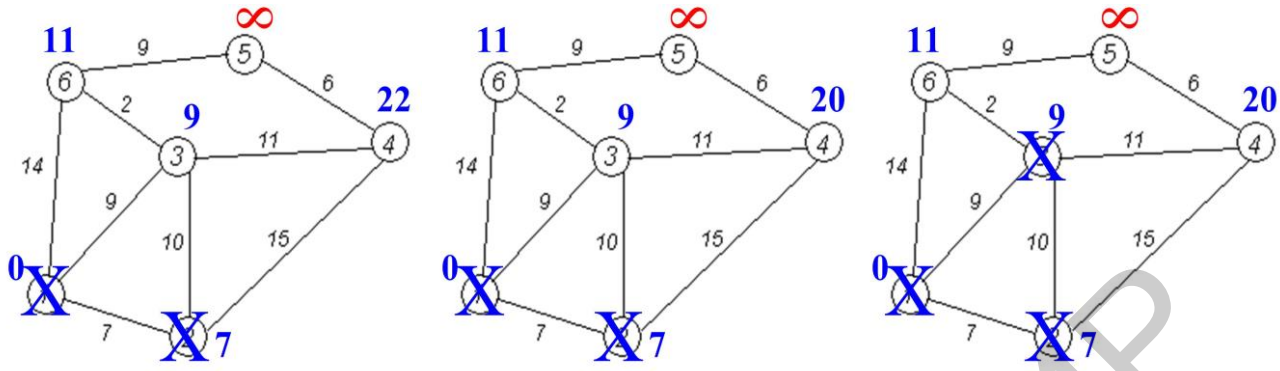


а *б*

Рис. 1.10. Цикл 2 поиска кратчайших путей на графе:
а – обработка вершины 4; *б* – «вычеркивание» вершины 2

В цикле 3 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат. Осуществляется поиск вершины с минимальной меткой. Выбирается вершина 3, так как она имеет метку 9, а остальные вершины имеют метки с большими значениями. Определяются непосещенные соседние вершины для выбранной вершины 3. Это вершины 4 и 6. Соседняя вершина 6 имеет меньшее значение метки (метка 14), чем соседняя вершина 4 (метка 22). Поэтому первой обрабатывается вершина 6 (см. рис. 1.10, *б*). Для вершины 6 рассчитывается длина пути 1-3-6. Это сумма значений метки выбранной вершины 3 и метки ребра 3-6, равная 9 + 2 = 11. Длина пути 1-3-6 сравнивается с меткой вершины 6. Так как длина пути 1-3-6 меньше значения метки вершины 6, то осуществляется замена метки 14 в вершине 6 на метку 11 (рис. 1.11, *а*). Для выбранной вершины 3 остается необработанной соседняя вершина 4, ребро 3-4 которой имеет метку 11. Для вершины 4 рассчитывается длина пути 1-3-4. Это сумма значений метки выбранной вершины 3 и метки ребра 3-4, равная 9 + 11 = 20. Длина пути 1-3-4 сравнивается с меткой вершины 4. Так как длина пути 1-3-4 меньше значения метки вершины 4, осуществляется замена метки 22 в вершине 4 на метку 20 (рис. 1.11, *б*). Так как все соседние вершины для выбранной вершины 3 уже обработаны, вершина 3 помечается как посещенная (вычеркивается из списка обработки) и цикл обработки завершается (рис. 1.11, *в*). В результате выполнения цикла 3 переопределяются кратчайшие маршруты от исходной вершины 1 до вершин 4 и 6. Это соответственно маршрут 1-3-4 длиной 20 и маршрут 1-3-6 длиной 11. Остаются ак-

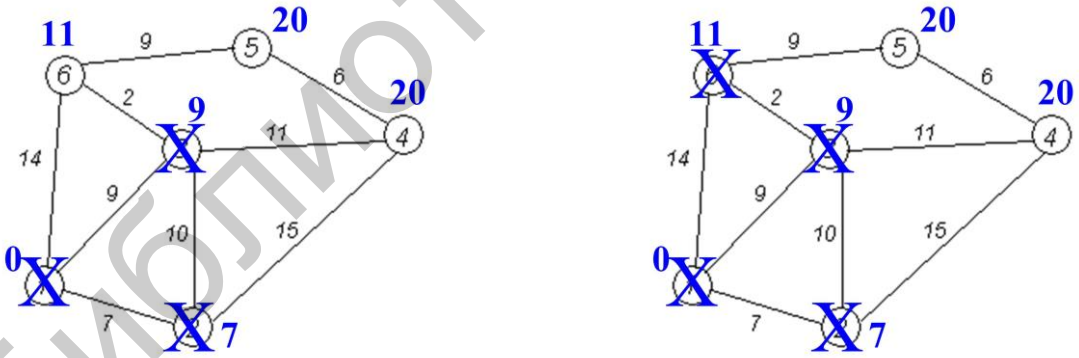
туальными кратчайшие маршруты от исходной вершины 1 до вершин 2 и 3. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9.



а *б* *в*

Рис. 1.11. Цикл 3 поиска кратчайших путей на графе:
а – обработка вершины 6; *б* – обработка вершины 4;
в – «вычеркивание» вершины 1

В цикле 4 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат (см. рис. 1.11, *в*). Осуществляется поиск вершины с минимальной меткой. Выбирается вершина 6, так как она имеет метку 11, а остальные вершины имеют метки с большими значениями. Определяются непосещенные соседние вершины для выбранной вершины 6. Это единственная вершина 5. Для вершины 5 рассчитывается длина пути 1-6-5 (рис. 1.12, *а*).



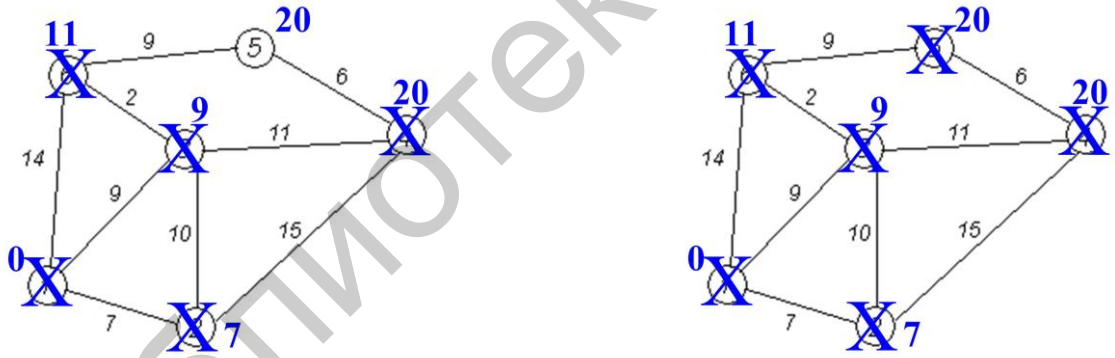
а *б*

Рис. 1.12. Цикл 4 поиска кратчайших путей на графе:
а – обработка вершины 5; *б* – «вычеркивание» вершины 6

Это сумма значений метки выбранной вершины 6 и метки ребра 6-5, равная 11 + 9 = 20. Длина пути 1-6-5 сравнивается с меткой вершины 5. Так как длина пути 1-6-5 меньше значения метки вершины 5, то осуществляется замена метки «бесконечность» в вершине 5 на метку 20. Так как все соседние вершины для выбранной вершины 6 уже обработаны, вершина 6 помечается как посещенная (вычеркивается из списка обработки) и цикл обработки завершается

(рис. 1.12, *б*). В результате выполнения цикла 4 определяется кратчайший маршрут от исходной вершины 1 до вершины 5. Это маршрут 1-3-6-5 длиной 20. Остаются актуальными кратчайшие маршруты от исходной вершины 1 до вершин 2, 3, 4 и 6. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9, маршрут 1-2-4 длиной 20, маршрут 1-3-6 длиной 11.

В цикле 5 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат (см. рис. 1.12, *б*). Осуществляется поиск вершины с минимальной меткой. Вершины 4 и 5 имеют одинаковые метки и для обработки может быть выбрана любая вершина. Пусть это будет вершина 4. Определяются непосещенные соседние вершины для выбранной вершины 4. Это единственная вершина 5. Для вершины 5 рассчитывается длина пути 1-4-5. Это сумма значений метки выбранной вершины 4 и метки ребра 4-5, равная 20 + 6 = 26. Длина пути 1-4-5 сравнивается с меткой вершины 5. Так как длина пути 1-4-5 больше значения метки вершины 5, то замена метки 20 в вершине 5 на метку 26 не осуществляется. Так как все соседние вершины для выбранной вершины 4 уже обработаны, вершина 4 помечается как посещенная (вычеркивается из списка обработки) и цикл обработки завершается (рис. 1.13, *а*). В результате выполнения цикла 5 остаются актуальными ранее определенные кратчайшие маршруты от исходной вершины 1 до вершин 2, 3, 4, 5 и 6. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9, маршрут 1-2-4 длиной 20, маршрут 1-3-6-5 длиной 20, маршрут 1-3-6 длиной 11.



а *б*

Рис. 1.13. Циклы 5 и 6 поиска кратчайших путей на графе:
а – «вычеркивание» вершины 4 (цикл 5); *б* – «вычеркивание» вершины 5 (цикл 6)

В цикле 6 осуществляется проверка наличия непосещенных вершин графа, которая дает положительный результат (см. рис. 1.13, *а*). Осуществляется поиск вершины с минимальной меткой. Это единственная вершина 5. Определяются непосещенные соседние вершины для выбранной вершины 5. Таких вершин нет. Вершина 5 помечается как посещенная (вычеркивается из списка обработки) и цикл обработки завершается (рис. 1.13, *б*). В результате выполнения цикла 6 остаются актуальными ранее определенные кратчайшие маршруты от исходной вершины 1 до вершин 2, 3, 4, 5 и 6. Это соответственно маршрут 1-2

длиной 7, маршрут 1-3 длиной 9, маршрут 1-2-4 длиной 20, маршрут 1-3-6-5 длиной 20, маршрут 1-3-6 длиной 11.

В цикле 7 осуществляется проверка наличия непосещенных вершин графа, которая дает отрицательный результат (см. рис. 1.13, *б*). Алгоритм Дейкстры завершен.

В результате выполнения алгоритма Дейкстры для графа, приведенного на рис. 1.8, установлены следующие кратчайшие маршруты от исходной вершины 1 до вершин 2, 3, 4, 5 и 6. Это соответственно маршрут 1-2 длиной 7, маршрут 1-3 длиной 9, маршрут 1-2-4 длиной 20, маршрут 1-3-6-5 длиной 20, маршрут 1-3-6 длиной 11.

2. ПРОТОКОЛ ВНЕШНЕЙ МАРШРУТИЗАЦИИ EIGRP

2.1. Обзор протокола EIGRP

Протокол EIGRP представляет собой фирменный протокол маршрутизации Cisco, обнародованный в 1994 году. Разработан компанией Cisco в качестве замены IGRP, отличается поддержкой бесклассовой междоменной маршрутизации (Classless Interdomain Routing – CIDR) и маски переменной длины (Variable-length Subnet Mask – VLSM), которые позволяют максимально использовать адресное пространство. Обладает быстрой сходимостью, повышенной масштабируемостью и более эффективной обработкой петель маршрутизации.

Протокол EIGRP может заменить протокол информации о маршрутах Novell (Routing Information Protocol – RIP) или протокол поддержки таблицы маршрутизации AppleTalk (Routing Table Maintenance Protocol – RTMP), повышая эффективность работы сетей IPX и AppleTalk.

Протокол EIGRP является идеальным решением для крупных многопротокольных корпоративных сетей, построенных на базе маршрутизаторов Cisco.

EIGRP – усовершенствованный дистанционно-векторный протокол динамической маршрутизации. Динамическая маршрутизация – направление данных в сети по маршрутам, созданным протоколами маршрутизации. Протоколы маршрутизации реализуются в программах. Основная их задача – создание маршрутов ко всем удаленным сетям и их автоматическое обновление при изменении топологии сети. Для этого протокол выполняет следующие действия:

1. Маршрутизатор посылает и принимает сообщения маршрутизации.
2. Маршрутизатор делится сообщениями маршрутизации и информацией маршрутизации с другими маршрутизаторами, которые используют тот же протокол.
3. Маршрутизаторы обмениваются информацией маршрутизации для изучения удаленных сетей.
4. Когда маршрутизатор определяет изменение топологии, он объявляет об изменениях другим роутерам.

Дистанционно-векторный протокол использует алгоритм вектора расстояния, с помощью которого анализируется информация, поступающая от соседних устройств, и выносится решение о создании маршрута. Алгоритм вектора расстояния использует два основных критерия:

1. Расстояние – насколько удалена сеть назначения от данного маршрутизатора.
2. Вектор – в каком направлении следует пересылать пакеты для данной сети.

Расстояние в маршруте представляется стоимостью или метрикой, которая может характеризовать один из следующих параметров:

– число участков маршрута;
– административные накладные расходы;
– полоса пропускания;

– скорость передачи;
– вероятность задержек;
– надежность.

Компонент вектора или направления в маршруте представляет собой адрес следующего участка пути к сети, указанной в маршруте. Аналогией для вектора расстояния могут быть дорожные знаки с указанием направлений на развязках автострад. Знак указывает направление к месту назначения и сообщает расстояние до него. По мере движения по автостраде появляется следующий знак, указывающий на то же место назначения, но расстояние становится короче. Если расстояния сокращаются, трафик следует по оптимальному маршруту.

2.2. Характеристики протокола EIGRP

Протокол EIGRP часто называют гибридным протоколом маршрутизации, сочетающим в себе лучшие черты дистанционно-векторных алгоритмов и алгоритмов маршрутизации по состоянию канала. Протокол EIGRP также использует лучшие функции протокола OSPF, однако отличается более простой настройкой. К основным характеристикам протокола относятся:

– быстрая сходимость благодаря рассылке инициированных частичных обновлений;
– маршрутизаторы EIGRP принадлежат одному домену маршрутизации;
– маршрутизаторы EIGRP создают и поддерживают три базы данных: смежную (adjacency), топологии (topology) и таблицу маршрутизации (forwarding);
– многоадресная и одноадресная рассылка сообщений;
– поддержка VLSM;
– поддержка множества протоколов;
– поддержка резервных маршрутов;
– независимость от протоколов канального уровня и топологии.

Сходимость достигается, когда все маршрутизаторы внутри домена маршрутизации имеют согласованную информацию о доступных маршрутах. Время, которое требуется для того, чтобы все маршрутизаторы обработали сообщения маршрутизации и обновили свои маршрутные таблицы, называется временем сходимости. EIGRP использует инициированные частичные сообщения, в которых быстро и надежно распространяет по сети только изменения в маршрутных таблицах, уменьшая время сходимости. Если в сети произошли изменения, маршрутизаторы EIGRP немедленно генерируют сообщения маршрутизации соседним маршрутизаторам EIGRP, включая в эти сообщения только измененные маршруты, а не всю маршрутную таблицу (частичное обновление маршрутов). Такая технология позволяет экономно использовать полосу пропускания, повышает эффективность и производительность сети за счет уменьшения времени сходимости. Это очень важно, так как при отказе канала или маршрутизатора данные не передаются в объединенной сети до тех пор, пока все маршрутные таблицы не будут полностью обновлены.

Протокол EIGRP включает свой домен маршрутизации (который включает все маршрутизаторы, поддерживающие EIGRP, а также сети внутри домена) с помощью номера AS (автономной системы). Маршрутизаторы EIGRP могут обмениваться информацией, только если они имеют один и тот же номер AS (т. е. они рассматриваются как члены одного и того же домена). Автономные системы EIGRP, имеющие разные номера, не могут обмениваться информацией. Номер AS назначается произвольно при настройке и запуске EIGRP на первом маршрутизаторе. После назначения номера AS все другие маршрутизаторы внутри этой автономной системы должны иметь тот же номер.

Все маршрутизаторы EIGRP внутри одной и той же автономной системы должны создать и поддерживать три различные базы данных: таблицу соседей (adjacency), топологическую базу данных (topology) и таблицу маршрутизации (forwarding). В первую очередь создается таблица соседей. Она формируется в результате обмена приветственными сообщениями между соседними маршрутизаторами EIGRP. Эта таблица содержит список всех соседей, поддерживающих EIGRP. После создания смежной базы данных маршрутизаторы могут начать обмен маршрутной информацией, в результате которого создается топологическая база данных (или карта) всей сети. В топологической базе данных сохраняются маршруты и метрики каждой сети и подсети внутри автономной системы. Затем по этой схеме запускается алгоритм маршрутизации EIGRP, в результате чего определяются лучшие маршруты, которые вносятся в таблицу маршрутизации.

Маршрутизаторы EIGRP могут применять комбинацию многоадресных (multicast) и одноадресных (unicast) сообщений для обмена маршрутной информацией вместо широковещательных (broadcast) сообщений. Широковещательные сообщения – это пакеты, которые адресуются всем устройствам системы, вынуждая всю систему прерывать работу и обрабатывать эти пакеты. Многоадресные пакеты направляются определенной группе устройств, а одноадресные сообщения используются для передачи сообщений между двумя отдельными системами («точка – точка»). Групповой адрес, используемый всеми маршрутизаторами EIGRP: 224.0.0.10. Только устройства, принадлежащие данной группе (маршрутизаторы EIGRP), могут обрабатывать эти пакеты. Благодаря использованию комбинации многоадресных и одноадресных пакетов, EIGRP уменьшает излишний трафик, вызываемый широковещательной рассылкой. Кроме того, повышается надежность рассылки EIGRP-пакетов.

EIGRP является протоколом бесклассовой маршрутизации. Маршрутизатор включает в объявления маску подсети. Включение маски подсети в адрес пункта назначения позволяет получателю точно определить, какая часть адреса относится к сети (полноклассовый адрес) и какая часть – к подсети. EIGRP автоматически суммирует маршруты до границы класса, однако предусматривает настройку суммаризации до любой границы на любом интерфейсе.

EIGRP способен быть единым протоколом маршрутизации в сети, использующей несколько различных протоколов сетевого уровня – IP, IPX, AppleTalk, используя PDM. В корпоративных сетях подобная ситуация не ред-

кость, и применение EIGRP в этом случае дает некоторые преимущества. Быстрая сходимость EIGRP и сложная структура метрик предлагает большую производительность и стабильность для внедрения IPX и AppleTalk.

Маршрутизатор EIGRP сохраняет всех своих соседей в таблице, что позволяет быстро находить альтернативные маршруты в случае пропадания основных. Если соответствующий маршрут не найден, маршрутизатор опрашивает соседей о наличии альтернативных маршрутов.

EIGRP не нуждается в дополнительной конфигурации для работы через протоколы второго уровня. Другие протоколы, такие, как OSPF, используют различные настройки для различных канальных протоколов (например, Ethernet и Frame Relay). EIGRP эффективно функционирует как в LAN, так и в WAN окружении, приспосабливается к различным скоростям и средам.

2.3. Работа протокола EIGRP

Чтобы начать обмен маршрутной информацией, маршрутизаторы EIGRP, находящиеся в одном и том же сегменте в пределах одного и того же домена маршрутизации AS, должны сформировать смежные (соседские) взаимоотношения. Маршрутизаторы становятся «соседями» после того, как они обменяются приветственными пакетами (Hello) в общей сети. Когда маршрутизатор EIGRP находится в процессе начальной загрузки, он должен распознать все другие маршрутизаторы EIGRP одного с ним сегмента и установить с ними соседские взаимоотношения. Этот процесс называется процессом распознавания (обнаружения) соседей и включает обмен приветственными сообщениями (Hello). Hello-пакеты посылаются каждые 5 с без подтверждения на групповой адрес 224.0.0.10 (всем маршрутизаторам EIGRP). В результате обмена приветственными сообщениями маршрутизатор создает локальную таблицу соседей, отслеживая всех соседей и их состояние. Если маршрутизатор не получает приветственного сообщения от соседнего маршрутизатора в течение нескольких временных интервалов (Hold Time), то он считает его «мертвым» и удаляет из своей таблицы. На рис. 2.1 представлен процесс установления соседства между двумя роутерами.

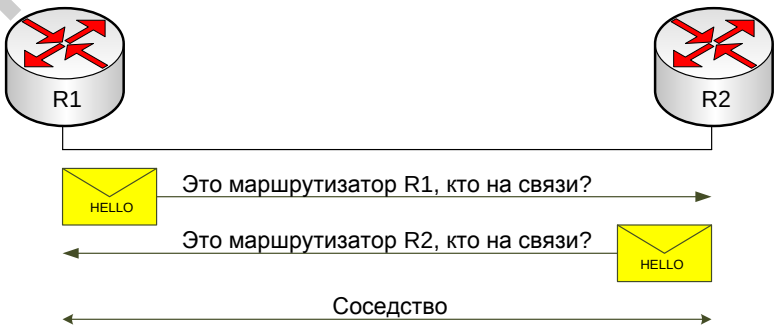


Рис. 2.1. Процесс установления соседства между роутерами

Обмен маршрутной информацией начинается после завершения установления соседских (смежных) взаимоотношений. Для распространения соседним роутерам информации маршрутизации EIGRP использует Update-пакет. Обновления маршрутизации не посылаются периодически, а только тогда, когда необходимо. Так, во время инициализации EIGRP маршрутизаторы получают полные копии маршрутных таблиц своих соседей. А далее Update-пакет содержит только необходимую информацию маршрутизации и посылается только тем роутерам, которым она необходима. За гарантированную упорядоченную доставку пакетов EIGRP отвечает надежный транспортный протокол (RTP). Надежность обеспечивается путем включения номеров пакетов в последовательности, а также использование подтверждений. Протокол поддерживает передачу пакетов как в режиме групповой рассылки, если информация требуется нескольким роутерам, так и в режиме одиночной отправки – только одному роутеру. Для подтверждения получения EIGRP-пакетов используется пакет подтверждения (Acknowledgement). Он посылается в режиме одиночной рассылки с использованием ненадежной доставки. На рис. 2.2 представлен процесс надежной доставки пакетов EIGRP.

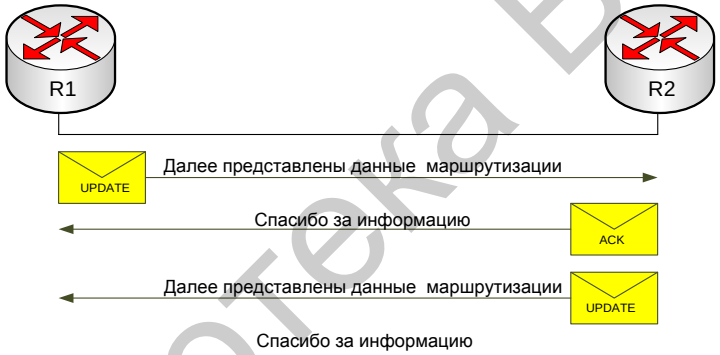


Рис. 2.2. Процесс надежной доставки пакетов

Процесс принятия решений для расчета всех маршрутов реализует алгоритм DUAL (Diffusing Update Algorithm). Алгоритм отслеживает все маршруты, объявленные всеми соседями. Все маршруты, объявленные соседними роутерами, помещаются в таблицу топологии. К каждой сети назначения привязан ее адрес и список соседей, объявивших маршрут к данной сети. К каждому соседу привязывается метрика его маршрута, которая называется представляемой дистанцией (Advertised Distance) и метрика, которую маршрутизатор будет использовать для того, чтобы достигнуть сеть назначения через этого соседа. Эта метрика является ожидаемой дистанцией (Feasible Distance) и соответствует значению представляемой дистанции соседа, увеличенной на стоимость участка пути до него.

Последующим маршрутизатором (Successor) для сети назначения будет считаться тот маршрутизатор из числа непосредственных соседей, через который проходит маршрут до данной сети, которому соответствует минимальное

значение (Feasible Distance). Этот маршрутизатор используется в качестве next hop для доставки пакетов в данную сеть. А маршрут через него объявляется основным и заносится в таблицу маршрутизации.

Потенциальным последующим маршрутизатором (Feasible Successor) для сети назначения считается тот маршрутизатор из числа непосредственных соседей, через который проходит маршрут до данной сети, которому соответствует значение Advertised Distance меньшее, чем значение Feasible Distance маршрута, проходящего через Successor (AD < FD). Если выходит из строя Successor, используется резервный маршрутизатор (Feasible Successor), через который можно попасть в сеть назначения. Таким образом, DUAL выбирает основной и резервный маршруты для каждой сети назначения.

При изменении топологии сети, вследствие потери основного маршрута, маршрутизатор обращается к резервному. Однако существуют моменты, когда маршрутизатор не имеет резервных маршрутов из-за невыполнения условия AD < FD. В результате происходит перерасчет маршрута. Таким образом, используется пакет запросов (Query) для отправки запроса соседям на наличие соответствующего маршрута. Если у них есть этот маршрут, то они отвечают ответом на запрос (Reply). Получение пакета Reply подтверждается отправкой пакета подтверждения Acknowledgement. На рис. 2.3 представлен алгоритм перерасчета маршрута.

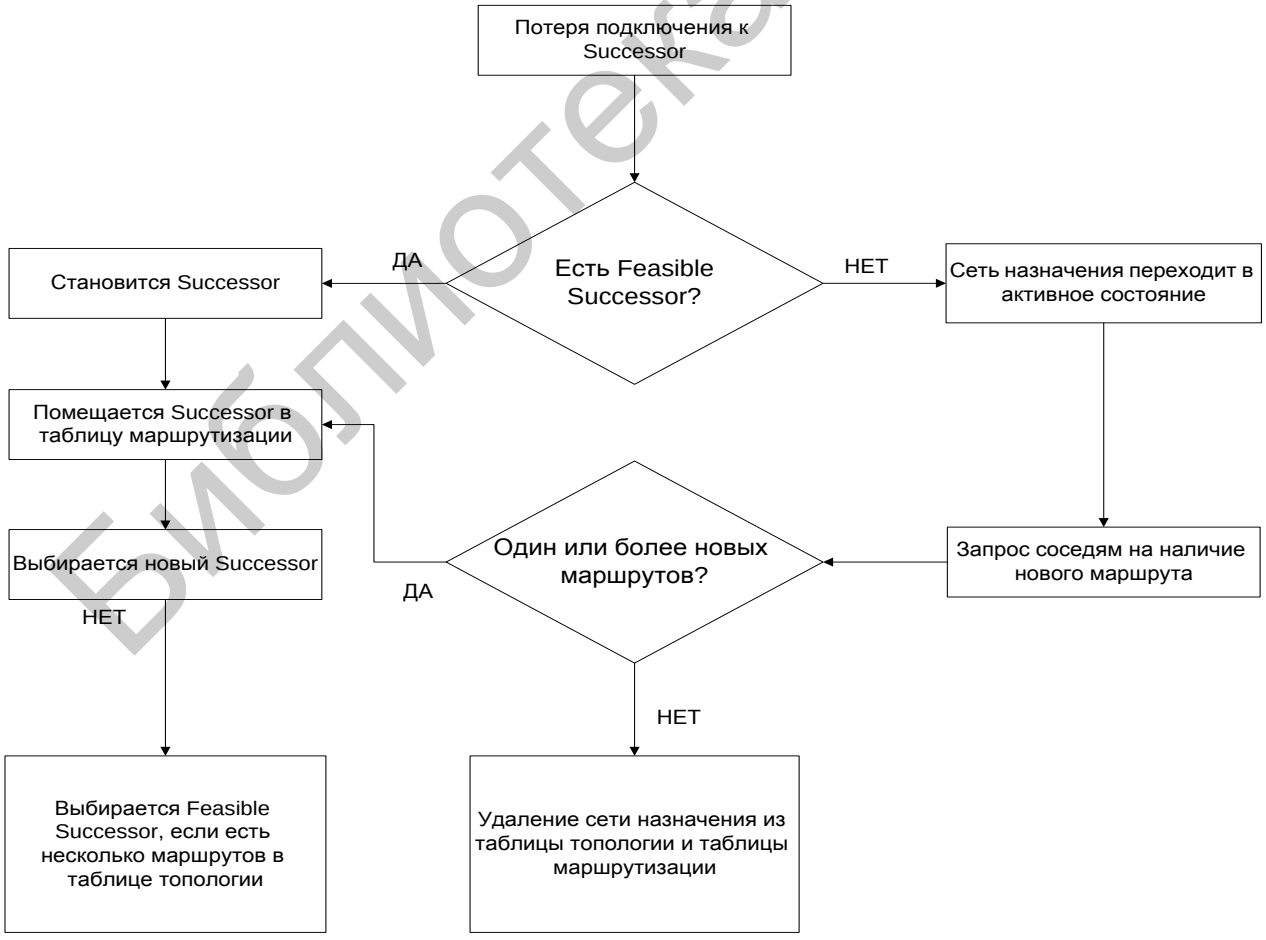


Рис. 2.3. Алгоритм перерасчета маршрута

2.4. Метрика протокола EIGRP

Метрики – это переменные параметры (показатели) сети, на основании которых принимается решение о выборе маршрута. Для некоторых протоколов маршрутизации эти метрики являются статическими величинами и не могут изменяться. При использовании других протоколов маршрутизации эти значения могут назначаться администраторами сети. В большинстве случаев к метрикам относятся следующие показатели: длина маршрута, или число пересылок (hop); ширина полосы пропускания (bandwidth); задержка (delay); надежность (reliability); нагрузка сети (load) и стоимость связи (cost).

Для вычисления стоимости маршрута EIGRP может использовать пять метрик. По умолчанию используются только две:

1. Полоса пропускания – характеристика коммуникационного канала, показывающая, какой объем данных может быть передан через этот канал в единицу времени. Пропускная способность полосы пропускания измеряется в битах, переданных в секунду. Каналы, которые поддерживают более высокую скорость передачи данных, являются более предпочтительными по сравнению с более медленными каналами.

2. Время задержки измеряется в десятках микросекунд. Это время, которое затрачивает маршрутизатор на обработку, постановку в очередь и ретрансляцию данных через интерфейс. Протокол, использующий метрику, должен определить значения времени задержки для всех каналов на протяжении всего сквозного маршрута. Наилучшим маршрутом считается путь с наименьшим суммарным значением времени задержки.

В табл. 2.1 приведены значения метрик для различных технологий канального уровня.

Таблица. 2.1

Значения полосы пропускания и задержки для различных технологий

Среда	Полоса пропускания	Задержка, мкс
ATM	155 Мбит/с	100
Fast Ethernet	100 Мбит/с	100
FDDI	100 Мбит/с	100
Token Ring	16 Мбит/с	630
Ethernet	10 Мбит/с	1000
T1 (Serial)	1,544 Мбит/с	20 000
V.92	56 кбит/с	20 000

Три остальных компонента могут быть задействованы, но не рекомендуются, так как это обычно приводит к частому перерасчету таблицы топологии.

Надежность – мера вероятности возникновения ошибки при передаче или обрыва соединения. Этот показатель может быть сконфигурирован как фиксированное значение администратором сети, однако, как правило, он определяется динамически в пределах заданного отрезка времени, например 5 с. Маршрутизаторы отслеживают присоединенные каналы и сообщают о возникающих проблемах, таких как неисправность линий связи, ошибки интерфейсов, потери данных и т. д. Каналы с наибольшим числом проблем рассматриваются как менее надежные по сравнению с другими, и поэтому маршруты по ним считаются нежелательными. Поскольку условия сети постоянно изменяются, надежность также не является постоянным показателем. Значения надежности обычно измеряются в пределах от 1 до 255, где 255 – показатель наивысшей надежности; 1 – показатель самой низкой надежности.

Нагрузка сети является переменным значением и обычно измеряется с помощью 5-секундного окна, индицирующего нагрузку по потоку сообщений специфического канала связи. Нагрузка измеряется объемом трафика в данном канале за этот промежуток времени в процентах от общего объема трафика канала. Значение 255 эквивалентно 100%-му использованию полосы пропускания. Чем выше значение, тем больше нагрузка по потоку сообщений определенного канала. Более низкие значения показывают умеренный трафик. Чем ниже значение показателя нагрузки, тем меньше перегрузка маршрута и тем он предпочтительнее. Показатель нагрузки может быть вручную задан администратором сети как статическое значение либо он может динамически отслеживаться.

Метрику протокол EIGRP вычисляет по формуле

$$metric = \left[K_1 \cdot bandwidth + \frac{K_2 \cdot bandwidth}{(256 - load)} + K_3 \cdot delay \right] \cdot \left[\frac{K_5}{reliability + K_4} \right],$$

где K_1, K_2, K_3, K_4, K_5 – весовые коэффициенты;

$bandwidth = (10000000 / bandwidth(i)) \cdot 256$ – приведенное значение полосы пропускания;

$bandwidth(i)$ – наименьшая полоса пропускания канала на участке между маршрутизатором и местом назначения;

$delay = delay(i) \cdot 256$ – приведенное значение задержки;

$delay(i)$ – суммарная задержка на протяжении всего маршрута;

$load$ – наихудшая надежность на протяжении всего маршрута;

$reliability$ – наихудшая нагрузка соединения на протяжении всего маршрута.

Стандартные значения весовых коэффициентов равны: $K_1 = 1$; $K_2 = 0$; $K_3 = 1$; $K_4 = 0$; $K_5 = 0$.

Подставляя стандартные значения коэффициентов в формулу получим следующее выражение для вычисления метрики:

$$metric = [bandwidth + delay].$$

2.5. Выбор логической топологии и схемы адресации сети

Одна из особенностей корпоративных сетей – территориальная распределенность. Так, сеть не ограничивается одной локацией, а способна охватывать значительные расстояния. Территориальные единицы корпоративных сетей могут находиться на значительном отдалении друг друга, однако это не должно влиять на возможность взаимодействия между ними. Для этого в сети используются различные технологии, что обуславливает ее гетерогенность. Обычно организация состоит из центрального офиса и нескольких удаленных филиалов, которые могут находиться в различных географических регионах. Связь между ними обеспечивается посредством использования WAN-технологий. Если необходимо постоянное высокоскоростное подключение между удаленными пользователями, используется выделенная линия, как в случае подключения предприятия к интернет-провайдеру. Она представляет собой канал типа «точка – точка», арендованный у операторов связи. Арендованная линия проходит через несущую сеть оператора и имеет пропускную способность до 2,5 Гбит/с. Основные преимущества использования выделенных каналов связи:

– постоянный доступ в Интернет с гарантированной скоростью при свободной телефонной линии;

– возможность организовать веб-сервер компании и другие сервисы (электронную почту с доменным именем организации, новости, FTP-архив и др.);

– защита данных и повышенная конфиденциальность передаваемой и принимаемой информации;

– различные прикладные решения на базе протокола IP для сокращения расходов на другие виды связи (например, телефонию);

– возможность организации видеоконференций, постоянного теле- и аудиовещания в сети Интернет;

– подключение к сети Интернет одновременно всех компьютеров локальной сети компании;

– разграничение прав доступа к интернет-ресурсам для пользователей сети;

– построение защищенной корпоративной сети по технологии VPN (Virtual Private Network – Виртуальная частная сеть).

Для связи с удаленными офисами не требуется постоянное соединение, так как передача трафика осуществляется периодически и имеет небольшие объемы. Наилучшим решением является использование каналов с установлением соединения. При установлении сеанса связи между удаленными пользователями канал коммутируется в сети общего пользования или телефонной сети. Такую возможность предоставляет служба цифровой сети интегрированных служб (ISDN).

ISDN – это цифровая сеть, которая обеспечивает интегрированное обслуживание, т. е. позволяет передавать голос, данные и даже видео по одной сети. Интерфейс базовой скорости ISDN (Basic Rate Interface, BRI), предназначенный для домашних офисов и малых предприятий, состоит из трех отдельных кана-

лов – двух опорных каналов (Bearer Channel, или B-channel) и одного канала данных. Каждый канал B имеет скорость 64 кбит/с, а канал D – 16 кбит/с. Канал D используется для сигнализации, например передачи вызова и разрыва связи. Каналы B предназначаются для передачи данных, таких, как оцифрованный голос или двоичные данные. ISDN позволяет оперировать одновременно несколькими цифровыми каналами. С помощью протоколов объединения каналов типа BONDING или многоканального PPP базовый интерфейс обмена позволяет достичь скорости передачи несжатых данных в 128 кбит/с.

Для объединения удаленных локальных сетей на основе ISDN можно использовать постоянные каналы и каналы по требованию. В первом случае имеется постоянное соединение между офисами – без учета объемов передаваемой информации. Во втором случае физическое соединение при отсутствии пакетов разрывается, однако логическое соединение остается и информация об удаленной ЛС сохраняется в устройстве. При появлении информации, которую нужно передать в удаленную локальную сеть, устройство ISDN автоматически набирает номер и в течение 1 с устанавливает физическое соединение.

Центральный офис является ядром любой организации. Там сосредоточены основные структурные элементы компании. Поэтому сеть центрального офиса – это очень ответственный участок, во многом определяющий все свойства сети в целом. Причина – через сеть центрального офиса проходят все основные пути взаимодействия между сетями рабочих групп, отделов и подразделений в том случае, если требуемые клиенту ресурсы находятся за пределами сети его рабочей группы, отдела и т. п. Применение технологии Intranet и поиск нужной информации в сети Интернет приводят к тому, что все чаще и чаще нужные пользователю ресурсы находятся за пределами его сегмента сети, а это в свою очередь резко повышает интенсивность трафика, проходящего через магистраль центрального офиса. У разных клиентских сессий могут быть существенно разные требования к качеству обслуживания. Поэтому сеть центрального офиса должна обладать высокой пропускной способностью с минимальным количеством задержек. Для этого хорошо подходит использование технологий Fast Ethernet, Gigabit Ethernet и FDDI, обеспечивающих скорости передачи данных от 100 до 1000 Мбит/с. С учетом приведенных особенностей, на рис. 2.4 представлена логическая топология корпоративной сети.

Маршрутизаторы R1, R2, R3 представляют собой оборудование центрального офиса. Они объединяют между собой сети отделов в пределах сети центрального офиса, а высокоскоростное соединение между ними на основе технологии Fast Ethernet представляет собой магистраль корпоративной сети. Роутеры R4 и R5 являются оборудованием двух удаленных филиалов организации. Каждый роутер объединяет сети отделов в пределах сети своего филиала и связывается с оборудованием центрального офиса посредством ISDN-соединений с пропускной способностью 128 кбит/с. Маршрутизатор R6 является оборудованием интернет-провайдера, который предоставляет организации доступ в Интернет по выделенной линии с пропускной способностью 1544 кбит/с.

Каждая территориальная единица сети, будь то центральный офис или удаленный филиал, имеет свою функциональную структуру, которая основана на принципе специализации организационных подструктур по функциональным признакам (производство, НИОКР, маркетинг, снабжение и др., т. е. однородных видов деятельности). Наличие отдела подразумевает наличие сети отдела, а наличие нескольких отделов – наличие сети кампуса, объединяющей сети различных отделов одного предприятия в пределах отдельного здания или в пределах одной территории (кампуса).

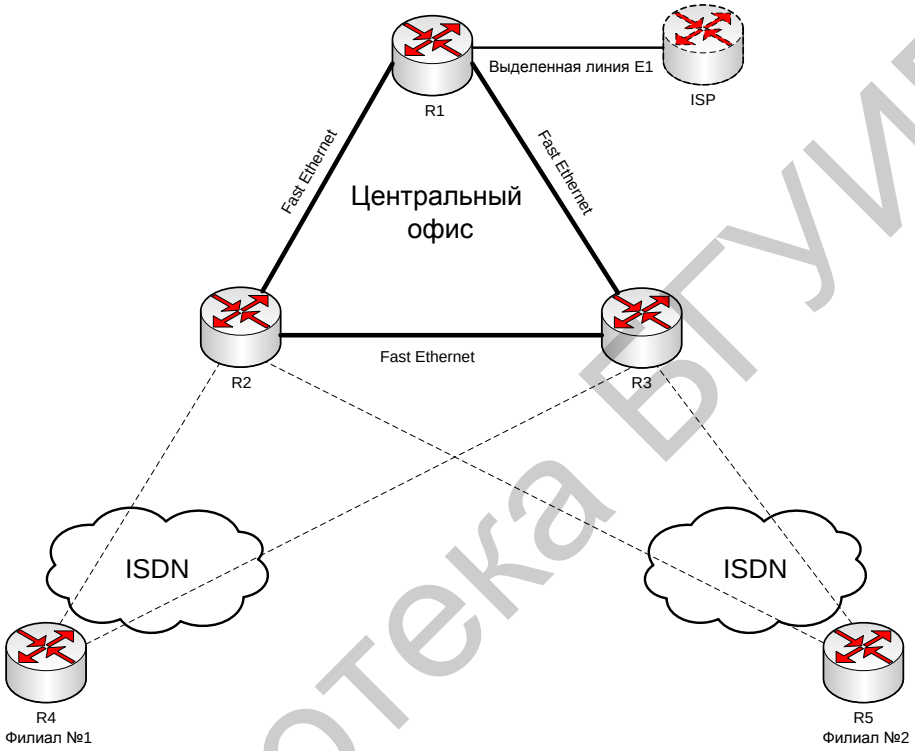


Рис. 2.4. Логическая топология корпоративной сети

В табл. 2.2 приведена функциональная структура корпоративной сети.

Для адресации корпоративной сети лучше всего использовать частные IP-адреса. Частным называется IP-адрес, принадлежащий к диапазонам, зарезервированным для использования в локальных сетях адресов, не используемых в сети Интернет. Хотя частные IP-адреса и не являются адресами сети Интернет, существует способ организации связи локальной сети, в которой используются такие адреса, с глобальной сетью. Это делается с помощью специальных аппаратных или программных маршрутизаторов, реализующих трансляцию адресов источника, известную как NAT.

Следующие диапазоны определены как частные диапазоны IP-адресов:

– 10.0.0.0 – 10.255.255.255 (10.0.0.0/8, или 10/8);

– 172.16.0.0 – 172.31.255.255 (172.16.0.0/12, или 172.16/12);

– 192.168.0.0 – 192.168.255.255 (192.168.0.0/16, или 192.168/16).

Для корпоративной сети выбрана сеть класса B с адресом 172.16.0.0/16.

При организации адресации можно руководствоваться следующими стратегиями:

– бесклассовая адресация;
– структурная схема адресации;
– географическая схема адресации;
– топологическая схема адресации.

Таблица 2.2

Функциональная структура корпоративной сети

Сеть кампуса	Сеть отдела
Центральный офис	Управление компании
	Отдел корпоративных связей
	Бухгалтерский отдел
	Планово-экономический отдел
	Отдел по работе с клиентами
	Отдел профподготовки
	Отдел охраны труда
	Отдел кадров
	Отдел производства
	Отдел продаж
	Сервисный отдел
	Отдел исследований и разработок
Филиал №1	Администрация филиала
	Бухгалтерский отдел
	Отдел продаж
	Сервисный отдел
Филиал №2	Администрация филиала
	Бухгалтерский отдел
	Отдел продаж
	Сервисный отдел

Бесклассовая адресация – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жесткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

Возможность назначения одному адресу нескольких масок подсетей предоставляет следующие преимущества:

– более эффективное использование выделенного организации адресного пространства;

– значительное уменьшение количества маршрутной информации внутри домена в одной организации за счет объединения маршрутов.

Введение маски подсети переменной длины дает возможность администратору создавать в рамках своей организации подсети требуемого размера. Так, каждой сети отдела центрального офиса присвоен префикс 26, что позволяет ей поддерживать до 64 хостов, а локальным сетям филиала – префикс 28, что позволяет им поддерживать до 16 хостов. Это является оптимальным при средней численности работников в отделе.

Географическая схема адресации позволяет распределить адресное пространство между различными региональными офисами так, чтобы каждый офис обладал собственным пространством выделяемых адресов. В итоге центральный офис обладает диапазоном адресов 172.16.0.0/22 с поддержкой 1016 хостов. Для удаленных подразделений организации предусмотрен блок адресов 172.16.4.0/24, где филиал №1 имеет диапазон адресов 172.16.4.0/26, а филиал №2 – 172.16.4.64/26. Оставшееся адресное пространство является зарезервированным по причине расширения организации путем создания новых филиалов. ISDN-каналам назначаются динамические, а не постоянно назначаемые адреса. Дело в том, что абсолютное большинство операторов связи берут деньги за регистрацию постоянного IP-адреса.

Структурная схема адресации подразумевает распределение доступного пространства между различными подразделениями организации так, чтобы каждое подразделение обладало собственным пространством выделяемых адресов. В итоге каждый отдел обладает собственным сетевым адресом.

Топологическая схема адресации заключается в распределении адресов в зависимости от маршрутизатора, к которому подключена сеть или основываясь на топологии сети. Так, локальные сети каждого маршрутизатора имеют смежные сетевые адреса, что гарантирует возможность суммирования маршрутов.

В табл. 2.3 представлена адресация каждого сегмента эмулируемой корпоративной сети с указанием технологии его построения.

2.6. Физическая топология корпоративной сети

Эмуляция – воспроизведение программными или аппаратными средствами либо их комбинацией работы других программ или устройств.

Далее воспроизведем работу протокола маршрутизации в корпоративной сети. Так как это осуществляется при помощи технологии виртуализации в исследовательских целях, то не прилагается больших требований к используемому оборудованию и программному обеспечению.

Эмуляция производится на базе существующей мультисервисной сети кафедры СиУТ с использованием дополнительных сетевых устройств. Основное требование, предъявляемое к используемым устройствам, – наличие поддержки протокола 802.1Q. Маршрутизаторы CISCO 2600 Series обладают такой возможностью. Серия Cisco 2600 представляет собой экономичную серию модульных маршрутизаторов для малых и средних офисов, включающую в себя возможность передачи голоса и факса. Предлагаемый набор модулей позволяет так же использовать Cisco 2600 в качестве серверов доступа и сетевых экранов.

В табл. 2.4 представлены технические характеристики используемого оборудования.

Таблица 2.3

Схема адресации эмулируемой сети

Сегмент сети	Адрес подсети
R1	–
Администрация	172.16.1.0/26
Отдел корпоративных связей	172.16.1.64/26
Бухгалтерский отдел	172.16.1.128/26
Планово-экономический отдел	172.16.1.192/26
R2	–
Отдел кадров	172.16.2.0/26
Сегмент сети	Адрес подсети
Отдел охраны труда	172.16.2.64/26
Отдел профподготовки	172.16.2.128/26
Отдел по работе с клиентами	172.16.2.192/26
R3	–
Отдел производства	172.16.3.0/26
Отдел продаж	172.16.3.64/26
Сервисный отдел	172.16.3.128/26
Отдел исследований и разработок	172.16.3.192/26
R4	–
Администрация	172.16.4.0/28
Бухгалтерский отдел	172.16.4.16/28
Отдел продаж	172.16.4.32/28
Сервисный отдел	172.16.4.48/28
R5	–
Администрация	172.16.4.64/28
Бухгалтерский отдел	172.16.4.80/28
Отдел продаж	172.16.4.96/28
Сервисный отдел	172.16.4.112/28
R1 – ISP	172.16.0.0/30
R1 – R2	172.16.0.4/30
R1 – R3	172.16.0.8/30
R2 – R3	172.16.0.12/30
R4 – R2	10.10.0.0/30
R4 – R3	10.10.0.4/30
R5 – R2	10.10.0.8/30
R5 – R3	10.10.0.12/30

Таблица 2.4

Технические характеристики оборудования эмулятора корпоративной сети

Наименование характеристики	Описание характеристики	
Коммутаторы		
Производитель	Cisco	
Модель	Cisco Catalyst 3560G-24TS	
Интерфейс	24.0 x Ethernet 10/100/1000BaseT– RJ-45 4.0 x GBIC – SFP	
Число поддерживаемых MAC адресов	12 000	
Скорость коммутации кадров	38,7 млн пак/с	
Буфер данных	128 Мбайт DRAM, 32 Мбайт Flash	
Способ коммутации	С промежуточным хранением (store-and-forward)	
Внутренняя пропускная способность	32 Гбит/с	
Маршрутизаторы		
Производитель	Cisco	Cisco
Модель	Cisco 2612	Cisco 2620
Интерфейсы	1.0 x Token Ring – RJ-45, 1.0 x Console – RJ-45 , 1.0 x Auxiliary – RJ-45, 1.0 x Ethernet 10Base-T – RJ-45	1.0 x Console – RJ-45 , 1.0 x Auxiliary – RJ-45, 1.0 x Ethernet 10Base-T/100Base-TX – RJ-45
Протоколы	AppleTalk , TCP/IP , UDP/IP , IP/IPX , SNA, BGP , OSPF	UDP/IP , IP/IPX , SNA , AppleTalk , TCP/IP, BGP , OSPF
Производительность	15 000 пак/с	25 000 пак/с
Буфер данных	DRAM – по умолчанию 32 Мбайт, максимум 64 Мбайт; Flash Memory – по умолчанию 8 Мбайт, максимум 16 Мбайт	DRAM – по умолчанию 32 Мбайт, максимум 64 Мбайт; Flash Memory – по умолчанию 8 Мбайт, максимум 16 Мбайт
Маршрутизаторы		
Производитель	Cisco	Cisco
Модель	Cisco 2610	Cisco 2610XM
Интерфейсы	1.0 x Console – RJ-45 , 1.0 x Auxiliary – RJ-45, 1.0 x Ethernet 10Base-T – RJ-45	1.0 x Console – RJ-45 , 1.0 x Auxiliary – RJ-45, 1.0 x Ethernet 10Base-T/100Base-TX – RJ-45
Протоколы	AppleTalk , IP/IPX, BGP, OSPF, EIGRP	AppleTalk , UDP/IP , TCP/IP , IP/IPX
Производительность	15 000 пак/с	20 000 пак/с

Окончание табл. 2.4

Наименование характеристики	Описание характеристики	
Буфер данных	DRAM – по умолчанию 128 Мбайт, максимум 256 Мбайт, Flash Memory – по умолчанию 32 Мбайт, максимум 48 Мбайт	DRAM – по умолчанию 128 Мбайт, максимум 256 Мбайт, Flash Memory – по умолчанию 32 Мбайт, максимум 48 Мбайт

Маршрутизаторы подключаются к общему широковещательному домену посредством коммутаторов. Маршрутизатор является устройством 3 уровня, поэтому основную работу производит на сетевом уровне. Коммутатор является устройством 2 уровня и не влияет на работу маршрутизаторов, а только служит для транзита пакетов между ними. На рис. 2.5 представлена физическая топология эмулятора корпоративной сети.

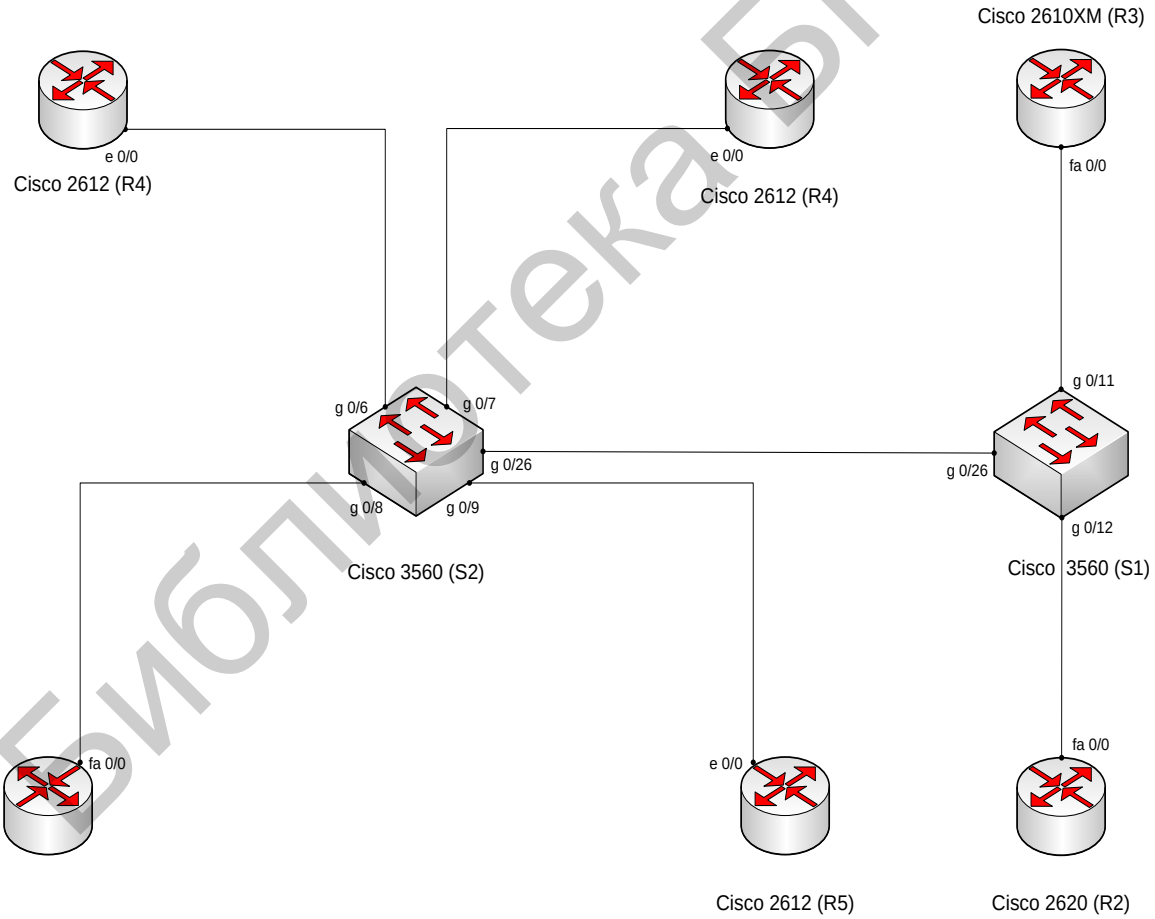


Рис. 2.5. Физическая топология эмулятора корпоративной сети

Функция маршрутизаторов – соединение различных сегментов сети. Каждая сеть, к которой подключен маршрутизатор, требует наличия у него от-

дельного интерфейса. Интерфейсы маршрутизатора используются для подключения LAN- и WAN-сетей. LAN (Local Area Network) – группа компьютеров и устройств (принтеры, сканеры и т. п.), расположенных на небольшой территории (в офисе или квартире) и соединенных в одну сеть. WAN (Wide Area Network) – глобальная сеть, которая объединяет локальные вычислительные сети (LAN), обеспечивая передачу данных на большие расстояния, например, в масштабах страны или всего мира. Количество поддерживаемых сетей и их технологии налагают аппаратные ограничения на используемое оборудование. С ростом сетей, которые может подключать маршрутизатор, и поддерживаемых им технологий растет количество интерфейсов, производительность, а следовательно, цена. Однако использование технологии виртуализации на сети помогает свести к минимуму зависимость сети от аппаратных возможностей сетевых устройств, что позволяет рассматривать различные сценарии построения сетевых топологий и реализовать работу на них различных протоколов.

Протокол маршрутизации инициирует процесс обмена между роутерами информацией о прямоподключенных сетях. Каждая подключенная сеть требует наличия соответствующего физического интерфейса на маршрутизаторе. Использование логических интерфейсов позволяет эмулировать работу физического интерфейса, что никак не влияет на работу протокола маршрутизации, но помогает преодолеть аппаратные ограничения устройства. Логический интерфейс – это виртуальный интерфейс, созданный командами системы. Виртуальные интерфейсы воспринимаются устройствами в сети как реальные. Можно сконфигурировать несколько различных логических интерфейсов: интерфейс кольцевой проверки (Loopback Interface), нулевой интерфейс (Null Interface) и туннельный интерфейс (Tunnel Interface). Для эмулирования локальных сетей, подключенных к роутеру, используется интерфейс кольцевой проверки (Loopback Interface), которому может быть назначен произвольный сетевой адрес. Так, на каждом маршрутизаторе создаются виртуальные интерфейсы по количеству принадлежащих ему локальных сетей. Каждому интерфейсу назначается IP-адрес, который соответствует адресу эмулируемой им локальной сети.

Технология VLAN позволяет разбить физическую сеть на множество виртуальных независимых сетей. Таким образом, каждому сегменту эмулируемой сети присваивается соответствующий номер виртуальной сети. Применение технологии магистральных соединений и настройка виртуальных подъинтерфейсов на одном физическом интерфейсе маршрутизатора позволяет эмулировать работу реальных WAN интерфейсов. Назначение каждому виртуальному подъинтерфейсу номера виртуальной сети и сетевого адреса эмулирует подключение к маршрутизатору нескольких сегментов эмулируемой сети. Если протокол маршрутизации EIGRP использует в качестве метрики ширину пропускания и задержку канала, то настройка этих значений на подъинтерфейсах маршрутизатора позволяет эмулировать различные WAN-технологии.

Для эмуляции требуемой логической топологии требуется организовать магистральные соединения между устройствами, провести настройку физических интерфейсов на обоих концах соединений, а также создать виртуальные

интерфейсы на маршрутизаторах. В табл. 2.5 приведены параметры настраиваемых интерфейсов оборудования и параметры их настройки.

Представленный инструментарий виртуализации способен реализовать на одной физической коммутируемой сети произвольные логические топологии сети в зависимости от особенностей эмулируемой сети и вида протокола.

Таблица 2.5

Таблица настраиваемых интерфейсов

Устройство	Интерфейс	Номер VLAN	IP-адрес	Ширина пропускания, Мбит/с	Задержка, мкс
Cisco 2620 (R1)	Fa 0/0.1	1	172.16.0.5/30	100 000	100
	Fa 0/0.2	2	172.16.0.9/30	100 000	100
	Fa 0/0.8	8	172.16.0.1/30	1544	20000
	Lo 1	нет	172.16.1.1/26	нет	Нет
	Lo 2	нет	172.16.1.65/26	нет	Нет
	Lo 3	нет	172.16.1.129/26	нет	Нет
	Lo 4	нет	172.16.1.193/26	нет	Нет
Cisco 2620 (R2)	Fa 0/0.1	1	172.16.0.6/30	100 000	100
	Fa 0/0.3	3	172.16.0.13/30	100 000	100
	Fa 0/0.4	4	10.10.0.1/30	128	20 000
	Fa 0/0.6	6	10.10.0.9/30	128	20 000
Cisco 2620 (R2)	Lo 1	нет	172.16.2.1/26	нет	Нет
	Lo 2	нет	172.16.2.65/26	нет	Нет
	Lo 3	нет	172.16.2.129/26	нет	Нет
	Lo 4	нет	172.16.2.193/26	нет	Нет
Cisco 2610XM (R3)	Fa 0/0.2	2	172.16.0.10/30	100 000	100
	Fa 0/0.3	3	172.16.0.14/30	100 000	100
	Fa 0/0.5	5	10.10.0.5/30	128	20 000
	Fa 0/0.7	7	10.10.0.13/30	128	20 000
	Lo 1	нет	172.16.3.1/26	нет	Нет
	Lo 2	нет	172.16.3.65/26	нет	Нет
	Lo 3	нет	172.16.3.129/26	нет	Нет
	Lo 4	нет	172.16.3.193/26	нет	Нет
Cisco 2612 (R4)	E 0/0.4	4	10.10.0.2/30	128	20 000
	E 0/0.5	5	10.10.0.6/30	128	20 000
	Lo 1	нет	172.16.4.1/28	нет	Нет
	Lo 2	нет	172.16.4.17/28	нет	Нет
	Lo 3	нет	172.16.4.33/28	нет	Нет
	Lo 4	нет	172.16.4.49/28	нет	Нет
Cisco 2612 (R5)	E 0/0.6	6	10.10.0.10/30	128	20 000
	E 0/0.7	7	10.10.0.14/30	128	20 000
	Lo 1	нет	172.16.4.65/28	нет	Нет
	Lo 2	нет	172.16.4.81/28	нет	Нет
	Lo 3	нет	172.16.4.97/28	нет	Нет
	Lo 4	нет	172.16.4.113/28	нет	Нет

Окончание табл. 2.5

Устройство	Интерфейс	Номер VLAN	IP-адрес	Ширина пропускания, Мбит/с	Задержка, мкс
Cisco 2612 (R6)	E 0/0.8	8	172.16.0.2/30	1544	20000
Cisco 3560 (S1)	G 0/6	8	нет	нет	Нет
	G 0/7	4,5	нет	нет	Нет
	G 0/8	1,8,2	нет	нет	Нет
	G 0/9	6,7	нет	нет	Нет
	G 0/26	1,2,4,5,6,7	нет	нет	Нет
Cisco 3560 (S2)	G 0/11	2,3,5,7	нет	нет	Нет
	G 0/9	1,3,4,6	нет	нет	Нет
	G 0/26	1,2,4,5,6,7	нет	нет	Нет

2.7. Настройка и тестирование протокола EIGRP

Для того чтобы сконфигурировать EIGRP, в сети необходимо включить протокол непосредственно на каждом маршрутизаторе, который затем начинает участвовать в процессе маршрутизации. Маршрутизаторы, использующие единый протокол маршрутизации, принадлежат к общему домену маршрутизации, что позволяет им обмениваться сообщениями маршрутизации. Поэтому всем маршрутизаторам необходимо присвоить одинаковый номер домена маршрутизации или автономной системы.

Для каждого маршрутизатора необходимо указать, какие интерфейсы будут участвовать в работе протокола EIGRP и какие сети будут анонсироваться другим маршрутизаторам.

Так, маршрутизаторы R1, R2, R3, R4 и R5, принадлежащие автономной системе под номером 1, будут участвовать в общем процессе маршрутизации. Каждый маршрутизатор анонсирует все свои непосредственно подключенные сети за все активные интерфейсы, кроме R1, который не анонсирует сеть R1-ISP и не посылает свои маршруты маршрутизатору ISP, который не принадлежит корпоративной сети, поэтому не участвует в работе протокола EIGRP.

Прежде чем начать обмен маршрутной информацией каждый EIGRP-маршрутизатор формирует взаимные отношения с соседними EIGRP-маршрутизаторами. Так, каждый маршрутизатор имеет свою таблицу соседей. На рис. 2.6 представлены таблицы соседей для маршрутизаторов R1, R2 и R5.

После того как маршрутизаторы сформировали соседские отношения, они начинают обмен маршрутной информацией между собой. Таким образом, каждый маршрутизатор получает информацию обо всех удаленных подсетях корпоративной сети, вычисляет оптимальные маршруты к ним и формирует таблицу маршрутизации.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO  Q   Seq
                                    (sec)          (ms)       Cnt Num
0   172.16.0.6      Fa0/0           13   00:01:30  40     1000 0   21
1   172.16.0.10     Fa0/1           14   00:01:10  40     1000 0   32

R1#
```

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO  Q   Seq
                                    (sec)          (ms)       Cnt Num
0   172.16.0.5      Fa0/0           13   00:06:13  40     1000 0   30
1   172.16.0.14     Fa0/1           14   00:05:53  40     1000 0   43
2   10.10.0.2       Eth1/0          14   00:00:31  40     1000 0   7
3   10.10.0.10      Eth1/1          13   00:00:31  40     1000 0   11

R2#
```

```
R5#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO  Q   Seq
                                    (sec)          (ms)       Cnt Num
0   10.10.0.9       Eth1/0          13   00:02:59  40     1000 0   39
1   10.10.0.13      Eth1/1          12   00:02:46  40     1000 0   52

R5#
```

Рис. 2.6. Таблицы соседей для маршрутизаторов R1, R2 и R5

Протокол EIGRP автоматически обобщает маршруты на границе сети, использующей IP-адреса с классами. Суммирование маршрутов до границы класса уменьшает таблицу маршрутизации, что приводит к меньшей загрузке каналов. Однако в некоторых случаях автоматическое суммирование не является приемлемым. Например, если в сети имеются несмежные подсети, необходимо отключить автоматическое суммирование для предотвращения путаницы. Так, прямо подключенные сети маршрутизаторов R2, R3 и R4, R5 принадлежат одной полноклассовой сети 172.16.0.0/16, но они не являются смежными, так как разделены подсетями из диапазона 10.0.0.0/8. На рис. 2.7 представлена таблица маршрутизации для R2, а на рис. 2.8 – таблица маршрутизации для R5.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.0.0.0/8 is a summary, 02:26:58, Null0
C       10.10.0.0/30 is directly connected, Ethernet1/0
D       10.10.0.4/30 [90/307200] via 10.10.0.2, 02:26:58, Ethernet1/0
C       10.10.0.8/30 is directly connected, Ethernet1/1
D       10.10.0.12/30 [90/307200] via 10.10.0.10, 02:26:58, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 17 subnets, 3 masks
D       172.16.0.0/16 is a summary, 02:26:58, Null0
D       172.16.0.0/30 [90/284160] via 172.16.0.5, 02:32:40, FastEthernet0/0
C       172.16.0.4/30 is directly connected, FastEthernet0/0
D       172.16.0.8/30 [90/30720] via 172.16.0.5, 02:32:40, FastEthernet0/0
                      [90/30720] via 172.16.0.14, 02:32:19, FastEthernet0/1
C       172.16.0.12/30 is directly connected, FastEthernet0/1
D       172.16.1.0/26 [90/156160] via 172.16.0.5, 02:32:40, FastEthernet0/0
D       172.16.1.64/26 [90/156160] via 172.16.0.5, 02:32:40, FastEthernet0/0
D       172.16.1.128/26 [90/156160] via 172.16.0.5, 02:32:40, FastEthernet0/0
D       172.16.1.192/26 [90/156160] via 172.16.0.5, 02:32:40, FastEthernet0/0
C       172.16.2.0/26 is directly connected, Loopback1
C       172.16.2.64/26 is directly connected, Loopback2
C       172.16.2.128/26 is directly connected, Loopback3
C       172.16.2.192/26 is directly connected, Loopback4
D       172.16.3.0/26 [90/156160] via 172.16.0.14, 02:32:19, FastEthernet0/1
D       172.16.3.64/26 [90/156160] via 172.16.0.14, 02:32:19, FastEthernet0/1
D       172.16.3.128/26 [90/156160] via 172.16.0.14, 02:32:19, FastEthernet0/1
D       172.16.3.192/26 [90/156160] via 172.16.0.14, 02:32:19, FastEthernet0/1
R2#
```

Рис. 2.7. Таблица маршрутизации для R2

```
R5#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.0.0.0/8 is a summary, 02:33:03, Null0
D       10.10.0.0/30 [90/307200] via 10.10.0.9, 02:28:23, Ethernet1/0
D       10.10.0.4/30 [90/307200] via 10.10.0.13, 02:28:10, Ethernet1/1
C       10.10.0.8/30 is directly connected, Ethernet1/0
C       10.10.0.12/30 is directly connected, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
D       172.16.0.0/16 is a summary, 02:33:03, Null0
C       172.16.4.64/28 is directly connected, Loopback1
C       172.16.4.80/28 is directly connected, Loopback2
C       172.16.4.96/28 is directly connected, Loopback3
C       172.16.4.112/28 is directly connected, Loopback4
R5#
```

Рис. 2.8. Таблица маршрутизации для R5

Маршрутизаторы центрального офиса R1, R2, R3 не имеют маршрутов к удаленным сетям филиалов, а маршрутизаторы R4, R5 не имеют маршрутов к удаленным сетям центрального офиса. Для решения проблемы необходимо отменить автоматическое суммирование, которое EIGRP использует по умолчанию. В случае отключения автоматического суммирования каждый маршрутизатор будет иметь полную информацию обо всех удаленных сетях, в итоге таблица маршрутизации будет иметь большие размеры, а в случае изменения топологии будет произведен перерасчет маршрута для всех маршрутизаторов сети, что значительно влияет на работоспособность и производительность всей сети. Для уменьшения таблицы маршрутизации и сведения к минимуму числа обновлений маршрутной информации применяется ручное суммирование. Ручное конфигурирование обобщения маршрутов осуществляется отдельно для каждого интерфейса, который будет распространять суммарный маршрут соседям.

Для каждого участка сети существуют различные технологии проведения ручного суммирования. К наиболее оптимальным методам суммирования, улучшающим стабильность функционирования EIGRP-сети, относятся:

– суммирование адресов локальных сетей внутри каждого маршрутизатора;

– суммирование маршрутов по направлению от центрального офиса к филиалам;

– суммирование маршрутов по направлению от филиалов к центральному офису.

Суммирование адресов локальных сетей, проводимое в одних маршрутизаторах по отношению к другим, приводит к тому, что каждый базовый маршрутизатор будет обладать полной маршрутной информацией только о непосредственно подключенных к нему участках сети и всего лишь суммарными сведениями обо всех остальных сегментах. Ниже перечислены объявления маршрутов, генерируемых в маршрутизаторах сети:

– маршрутизатор R1 объявляет оставшимся маршрутизаторам сети маршрут 172.16.1.0/24 к подключенным к нему локальным сетям отделов;

– маршрутизатор R2 объявляет оставшимся маршрутизаторам сети маршрут 172.16.2.0/24 к подключенным к нему локальным сетям отделов;

– маршрутизатор R3 объявляет оставшимся маршрутизаторам сети маршрут 172.16.3.0/24 к подключенным к нему локальным сетям отделов;

– маршрутизатор R4 объявляет оставшимся маршрутизаторам сети маршрут 172.16.4.0/25 к подключенным к нему локальным сетям отделов;

– маршрутизатор R5 объявляет оставшимся маршрутизаторам сети маршрут 172.16.4.128/25 к подключенным к нему локальным сетям отделов.

Преимущество подобного подхода таково, что каждый маршрутизатор обладает полной маршрутной информацией обо всех подключенных к нему удаленных участках сети, что позволяет проводить полностью оптимизированную маршрутизацию при передаче пакетов в данные участки. На рис. 2.9 представлена таблица маршрутизации для R3 после проведения суммирования.

Маршрутизатору R1 совсем необязательно знать об удаленных сетях каждого филиала. Вместо того чтобы предоставлять маршрутизатору R1 подробную информацию об отдельных точках назначения, маршрутизаторы R2 и R3 должны суммировать каждую группу точек назначения. Так, они суммируют маршруты 172.16.4.0/26 и 172.16.4.64/26 в один маршрут 172.16.4.0/25, а сети 10.10.0.0/30, 10.10.0.4/30, 10.10.0.8/30 и 10.10.0.12/30 – в одну точку назначения 10.10.0.0/28. На рис. 2.10 представлена таблица маршрутизации для R1 после проведения суммирования.

Поскольку все суммируемые сети «спрятаны» от маршрутизатора R1, то повреждение любой их этих сетей не повлияет на него (маршрутизатор не должен будет обновлять свою таблицу маршрутизации). Сокрытие подробной информации о топологии сети от маршрутизатора R1 позволяет существенно сузить участок, на который влияет изменение топологии.

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.10.0.0/28 is a summary, 00:45:28, Null0
D       10.10.0.0/30 [90/284160] via 172.16.0.13, 00:18:37, FastEthernet0/1
C       10.10.0.4/30 is directly connected, Ethernet1/0
D       10.10.0.8/30 [90/284160] via 172.16.0.13, 00:18:37, FastEthernet0/1
C       10.10.0.12/30 is directly connected, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 15 subnets, 5 masks
D       172.16.0.0/22 is a summary, 00:18:44, Null0
D       172.16.0.0/30 [90/284160] via 172.16.0.9, 00:18:37, FastEthernet0/0
D       172.16.0.4/30 [90/30720] via 172.16.0.9, 00:18:37, FastEthernet0/0
                      [90/30720] via 172.16.0.13, 00:18:37, FastEthernet0/1
C       172.16.0.8/30 is directly connected, FastEthernet0/0
C       172.16.0.12/30 is directly connected, FastEthernet0/1
D       172.16.1.0/24 [90/156160] via 172.16.0.9, 00:18:37, FastEthernet0/0
D       172.16.2.0/24 [90/156160] via 172.16.0.13, 00:18:37, FastEthernet0/1
D       172.16.3.0/24 is a summary, 04:58:06, Null0
C       172.16.3.0/26 is directly connected, Loopback1
C       172.16.3.64/26 is directly connected, Loopback2
C       172.16.3.128/26 is directly connected, Loopback3
C       172.16.3.192/26 is directly connected, Loopback4
D       172.16.4.0/25 is a summary, 00:45:28, Null0
D       172.16.4.0/26 [90/409600] via 10.10.0.6, 00:18:36, Ethernet1/0
D       172.16.4.64/26 [90/409600] via 10.10.0.14, 00:18:39, Ethernet1/1
R3#
```

Рис. 2.9. Таблица маршрутизации для R3

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

Gateway of last resort is not set

     10.0.0.0/28 is subnetted, 1 subnets
D       10.10.0.0 [90/284160] via 172.16.0.6, 00:00:55, FastEthernet0/0
                  [90/284160] via 172.16.0.10, 00:00:10, FastEthernet0/1
     172.16.0.0/16 is variably subnetted, 12 subnets, 4 masks
C       172.16.0.0/30 is directly connected, Ethernet1/0
C       172.16.0.4/30 is directly connected, FastEthernet0/0
C       172.16.0.8/30 is directly connected, FastEthernet0/1
D       172.16.0.12/30 [90/30720] via 172.16.0.6, 00:00:55, FastEthernet0/0
                       [90/30720] via 172.16.0.10, 00:00:10, FastEthernet0/1
D       172.16.1.0/24 is a summary, 04:13:43, Null0
C       172.16.1.0/26 is directly connected, Loopback1
C       172.16.1.64/26 is directly connected, Loopback2
C       172.16.1.128/26 is directly connected, Loopback3
C       172.16.1.192/26 is directly connected, Loopback4
D       172.16.2.0/24 [90/156160] via 172.16.0.6, 00:00:55, FastEthernet0/0
D       172.16.3.0/24 [90/156160] via 172.16.0.10, 00:00:10, FastEthernet0/1
D       172.16.4.0/25 [90/28160] via 172.16.0.6, 00:00:55, FastEthernet0/0
                      [90/28160] via 172.16.0.10, 00:00:10, FastEthernet0/1
R1#
```

Рис. 2.10. Таблица маршрутизации для R1

Суммирование маршрутов по направлению от центрального офиса к филиалам – задача не менее важная, чем рассмотренное выше суммирование маршрутов по направлению от филиалов к центральному офису. Цель этого суммирования – ограничить число передаваемых удаленным маршрутизатором обновлений информации о маршрутах путем предоставления этим маршрутизаторам сведений об одном стандартном маршруте или о нескольких основных сетевых маршрутах. Отсутствие суммирования приводит к тому, что удаленным маршрутизаторам объявляется информация обо всех внутрисегментных суммарных маршрутах, что приводит к их задействованию в процессе распро-

странения запроса, это в свою очередь негативно сказывается на стабильности функционирования сети. Чрезмерное расширение области распространения запроса существенно увеличивает количество времени и ресурсов, требующихся для завершения процесса сходимости, а также может вызвать непредвиденные проблемы в случае повреждения линии связи или выхода из строя маршрутизатора. Чем больше устройств или каналов передачи информации будет задействовано в процессе сходимости, тем выше вероятность возникновения проблем, связанных со стабильностью функционирования сети.

Поскольку удаленные маршрутизаторы R4 и R5 подключаются к маршрутизаторам R2 и R3 с помощью менее скоростных каналов передачи информации, снижение требований протокола EIGRP к пропускной способности линии связи является стратегически важной задачей. Так, все маршруты центрального офиса суммируются в один суммарный маршрут 172.16.0.0/22, который объявляется маршрутизаторам филиалов. На рис. 2.11 представлена таблица маршрутизации для R5 после проведения суммирования.

```
R5#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 4 subnets
D       10.10.0.0 [90/307200] via 10.10.0.9, 00:00:59, Ethernet1/0
D       10.10.0.4 [90/307200] via 10.10.0.13, 00:00:10, Ethernet1/1
C       10.10.0.8 is directly connected, Ethernet1/0
C       10.10.0.12 is directly connected, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
D       172.16.0.0/22 [90/284160] via 10.10.0.9, 00:01:00, Ethernet1/0
                      [90/284160] via 10.10.0.13, 00:00:11, Ethernet1/1
D       172.16.4.0/26 [90/435200] via 10.10.0.9, 00:01:00, Ethernet1/0
                      [90/435200] via 10.10.0.13, 00:00:08, Ethernet1/1
D       172.16.4.64/26 is a summary, 03:51:43, Null0
C       172.16.4.64/28 is directly connected, Loopback1
C       172.16.4.80/28 is directly connected, Loopback2
C       172.16.4.96/28 is directly connected, Loopback3
C       172.16.4.112/28 is directly connected, Loopback4
R5#
```

Рис. 2.11. Таблица маршрутизации для R5

Не менее важным в функционировании сети является вопрос распространения информации о маршрутах к внешним точкам назначения, т. е. сегментам сети, не принадлежащим данной автономной системе. При подключении к сети внешнего маршрутного домена в виде сети Интернет руководствуются следующим правилом: если точка назначения с определенным адресом не принадлежит автономной системе, то она находится за ее пределами и может быть достигнута посредством стандартного маршрута. Для этого на маршрутизаторе, подключенном к интернет-провайдеру, создается статический маршрут к сети 0.0.0.0/0, который затем распространяется всем остальным маршрутизаторам автономной системы. По этому маршруту будут отправляться все пакеты с адресом назначения, для которого маршрутизатору более уточненный маршрут не известен. На рис. 2.12 представлена таблица маршрутизации для R4 после распространения по сети стандартного маршрута.

```
R4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.0.5 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 4 subnets
C       10.10.0.0 is directly connected, Ethernet1/0
C       10.10.0.4 is directly connected, Ethernet1/1
D       10.10.0.8 [90/307200] via 10.10.0.1, 00:22:36, Ethernet1/0
D       10.10.0.12 [90/307200] via 10.10.0.5, 00:21:44, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
D       172.16.0.0/22 [90/284160] via 10.10.0.1, 00:22:35, Ethernet1/0
                      [90/284160] via 10.10.0.5, 00:21:44, Ethernet1/1
D       172.16.4.0/26 is a summary, 04:13:56, Null0
C       172.16.4.0/28 is directly connected, Loopback1
C       172.16.4.16/28 is directly connected, Loopback2
C       172.16.4.32/28 is directly connected, Loopback3
C       172.16.4.48/28 is directly connected, Loopback4
D       172.16.4.64/26 [90/435200] via 10.10.0.1, 00:22:35, Ethernet1/0
                       [90/435200] via 10.10.0.5, 00:21:44, Ethernet1/1
D*EX 0.0.0.0/0 [170/540160] via 10.10.0.5, 00:00:15, Ethernet1/1
D*EX 0.0.0.0/0 [170/540160] via 10.10.0.1, 00:00:15, Ethernet1/0
R4#
```

Рис. 2.12. Таблица маршрутизации для R4

Для диагностики возможности установления связи в сетях используются протоколы типа «запрос – ответ» или протокол эхо-пакетов. Результаты работы такого протокола могут помочь в оценке надежности пути к другому устройству, величин задержек в целом и между промежуточными устройствами. Для того чтобы такая команда работала, необходимо, чтобы не только локальное сетевое устройство знало, как попасть в пункт назначения, но и чтобы устройство в пункте назначения знало, как добраться до источника. Команда ping посылает ICMP (Internet Control Message Protocol) эхо-пакеты для верификации соединения. На рис. 2.13 представлен эхо-тест к удаленным сетям для маршрутизатора R5.

```
R5#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/34/105 ms

R5#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/35/108 ms

R5#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/24 ms

R5#ping 172.16.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/21/51 ms

R5#
```

Рис. 2.13. Проведение эхо-теста к удаленным сетям для R5

Там, где эхо-тест может быть использован для проверки связи между устройствами, трассировка маршрутов может использоваться для обнаружения трактов, по которым пакеты достигают удаленных адресатов, а также точек нарушения маршрутизации. Используя трассировку, маршрутизатор отправляет данные указанному узлу сети, при этом отображаются сведения обо всех промежуточных маршрутизаторах, через которые прошли данные на пути к узлу назначения. В случае проблемы при доставке данных до какого-либо узла, трассировка позволяет определить, на каком именно участке возникли неполадки. На рис. 2.14 представлена трассировка маршрутов к удаленным сетям для маршрутизатора.

```
R1#traceroute 172.16.4.1
Type escape sequence to abort.
Tracing the route to 172.16.4.1

  1   172.16.0.6      10 msec   6 msec    5 msec
  2   10.10.0.6       14 msec   10 msec   14 msec
R1#traceroute 172.16.4.65
Type escape sequence to abort.
Tracing the route to 172.16.4.65

  1   172.16.0.6      74 msec   6 msec    6 msec
  2   10.10.0.14      16 msec   10 msec   15 msec
R1#traceroute 172.16.2.1
Type escape sequence to abort.
Tracing the route to 172.16.2.1

  1   172.16.0.6      74 msec   6 msec    6 msec
R1#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1

  1   172.16.0.10     35 msec   8 msec    3 msec
R1#
```

Рис. 2.14. Трассировка маршрутов к удаленным узлам для R1

В результате включения и настройки протокола были вычислены маршруты ко всем удаленным сетям, что обеспечивает полное взаимодействие всех узлов сети.

3. ЛАБОРАТОРНАЯ РАБОТА. ИЗУЧЕНИЕ ПРОТОКОЛА OSPF НА БАЗЕ ЭМУЛЯТОРА КОРПОРАТИВНОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

3.1. Цель работы

Систематизация и закрепление знаний и навыков планирования, создания и настройки сети с применением протокола маршрутизации OSPF, приобретение навыков конфигурирования протокола OSPF, используя предложенную схему сети.

3.2. Описание лабораторной работы

Важным элементом лабораторной работы является моделирование структур, дизайна и топологий сети, практически используемых на сетях связи. Для наиболее полного представления существующих решений, используемых операторами связи, в настоящее время предлагается построение иерархической структуры КСПД. В основу предлагаемой логической топологии положена двух-уровневая модель [3–7].

Выделение двух уровней разрабатываемой сетевой структуры обусловлено также требованиями построения и налаживания динамического протокола маршрутизации OSPF. В основу протокола заложена иерархическая структура, значение каждого уровня в которой определяется по средствам разделения сетевого пространства на области с одинаковым набором определенных свойств. Area 0 выполняет роль консолидации и сбора всей служебной информации и трафика данных. Area 1 и area 2, являясь нижними уровнями модели, отвечают за обработку и выполнение локальных задач. На рис. 3.1 представлена структурная схема логической топологии OSPF-модели.

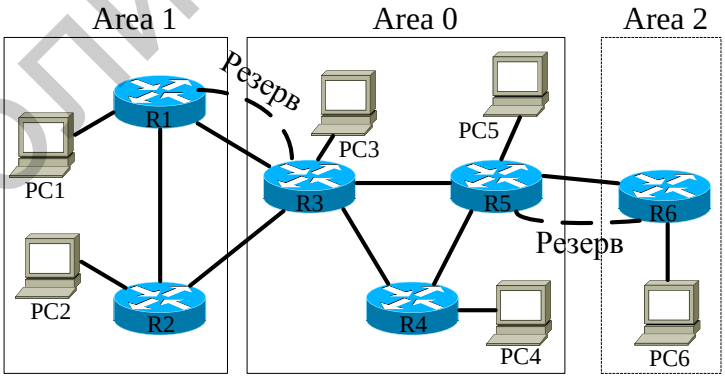


Рис. 3.1. Структурная схема логической топологии OSPF-модели

Выбор схемы адресации эмулируемой сети определяется в основном принятой топологией. Для соединений «точка – точка» принято использовать сети с маской 32, сетевое пространство разных area должно отличаться друг от друга и быть пригодным для суммаризации. В качестве диапазона используемых адресов выбрана сеть 10.0.0.0/16.

Для построения физической топологии эмулируемой сети используется коммутатор Catalyst 2960 и шесть маршрутизаторов Cisco 2600. В качестве основного средства выступает технология VLAN и использование сабинтерфейсов. Для физического моделирования предложенной топологии используются общепринятые методики построения сетей. На рис. 3.2 представлена схема соответствия топологии «кольцо» ее физической организации с помощью коммутатора и настройки VLAN.

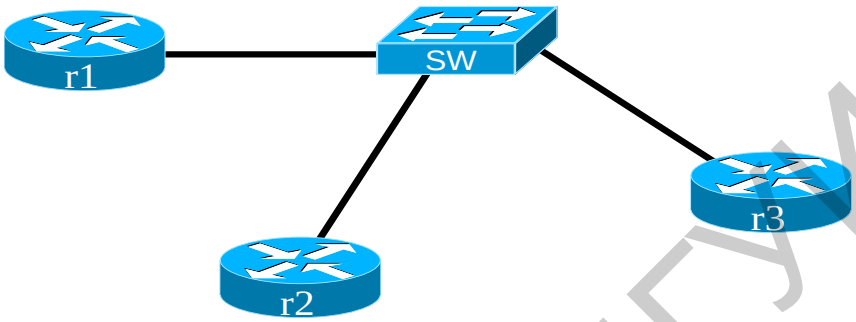


Рис. 3.2. Топология «кольца» с помощью коммутатора

На рис. 3.3 представлена схема соответствия топологии «точка – точка» ее физической организации с помощью коммутатора и настройки VLAN.

Рис. 3.3. Топология «точка – точка» с помощью коммутатора

На рис. 3.4 представлена схема физической топологии разрабатываемой модели.

3.3. Предварительное задание к лабораторной работе

1. Изучите терминологию, состояния, типы сетей, протокол приветствия стека, операции, конфигурирование и изменение метрики протокола OSPF.
2. Изучите теоретические основы технологии VLAN.

3.4. Порядок выполнения работы

Задание 1. Соберите схему сети в соответствии с приведенной физической топологией (см. рис. 3.4).

Шаг 1. Сетевые кабели должны соответствовать интерфейсам в топологии.

Необходимо использовать маршрутизаторы 2600 серии.

Шаг 2. Очистите всю конфигурацию на маршрутизаторе с помощью команды `erase startup-config`.

Шаг 3. Перезагрузите маршрутизатор.

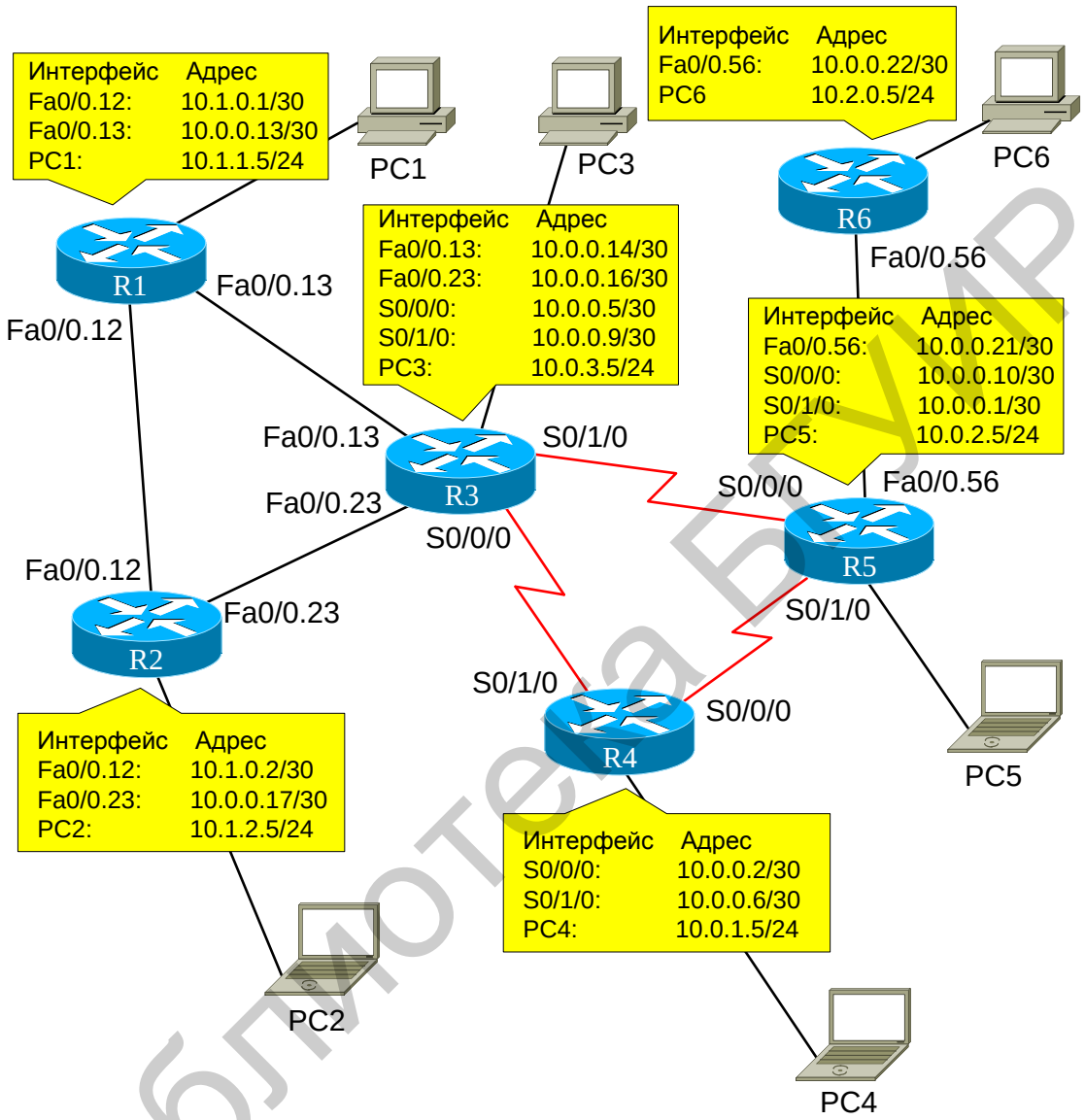


Рис. 3.4. Схема физической топологии разрабатываемой модели

Задание 2. Произведите базовую настройку маршрутизаторов и коммутатора.

1. Сконфигурируйте имена с помощью команды hostname.
2. Сконфигурируйте пароль для EXEC-режима.
3. Сконфигурируйте пароль для telnet-соединения.
4. Сконфигурируйте пароль для console-соединения.
5. Сконфигурируйте пароль VTY-соединения.

Задание 3. Настройте коммутатор SW в соответствии с приведенной логической схемой.

1. Создайте vlan 12, 13, 23, 56 с помощью команды `vlanID`, где ID – номер vlan.

2. На интерфейсах добавьте vlan с помощью следующих команд.

Для режима trunk:

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add ID
```

Для режима access:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan ID
```

```
Интерфейс fa 1/0: trunk, разрешенный vlan – 12, 13
Интерфейс fa 2/0: trunk, разрешенный vlan – 12, 23
Интерфейс fa 3/0: trunk, разрешенный vlan – 13, 23
Интерфейс fa 5/0: access, vlan – 56
Интерфейс fa 6/0: access, vlan – 56
```

Задание 4. Сконфигурируйте IP-адреса и включите интерфейсы на маршрутизаторах.

Шаг 1. Настройте интерфейсы на маршрутизаторах R1, R2, R3, R4, R5 и R6. На маршрутизаторах пропишите IP-адреса в соответствии со своим вариантом.

Шаг 2. Проверьте наличие IP-адресов в таблице интерфейсов.

Используйте команду `show ip interface brief`, проверьте правильность IP-адресов и интерфейсов.

После этого сохраните конфигурацию в памяти NVRAM маршрутизатора.

Шаг 3. Настройте интерфейсы Ethernet на компьютерах PC1, PC2, PC3, PC4, PC5 и PC6.

Настройте интерфейсы Ethernet на компьютерах с IP-адресами и шлюзами по умолчанию в соответствии со своим вариантом.

Шаг 4. Проверьте конфигурацию на компьютерах (проверьте прохождение пакетов до шлюза по умолчанию).

Задание 5. Настройте протокол OSPF на маршрутизаторе R1.

Шаг 1. Используйте команду `router ospf` в глобальном конфигурационном режиме. Введите номер процесса *process-ID*.

```
R1(config)#router ospf 1
R1(config-router)#
```

Шаг 2. Подключите непосредственно соединенные сети с помощью команды `network`.

```
R1(config-router)#network 10.0.0.16 0.0.0.3 area 0
R1(config-router)#
```

Задание 6. Аналогично произведите настройку протокола OSPF на остальных маршрутизаторах.

Задание 7. Проверьте правильность настройки протокола OSPF.

Шаг 1. На маршрутизаторе R1, используя команду `show ip ospf neighbor`, посмотрите информацию о соседних маршрутах (рис. 3.5).

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.2.1          1   FULL/DR         00:00:36    10.1.0.2        FastEthernet0/
0.12
10.0.3.1          1   FULL/BDR        00:00:36    10.0.0.14       FastEthernet0/
0.13
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.2.1          1   FULL/DR         00:00:37    10.1.0.2        FastEthernet0/
0.12
10.0.3.1          1   FULL/BDR        00:00:37    10.0.0.14       FastEthernet0/
0.13
R1#
```

Copy Paste

Рис. 3.5. Применение команды `show ip ospf neighbor`

Шаг 2. Используя команду `show ip protocols`, просмотрите информацию о протоколах (рис. 3.6).

R1

Physical Config CLI

IOS Command Line Interface

```
R1#sh ip prot

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.0.0 0.0.0.3 area 1
    10.0.0.12 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.1.1             110      00:01:40
    10.0.2.1             110      00:01:40
    10.0.3.1             110      00:01:05
    10.1.1.1             110      00:01:06
    10.1.2.1             110      00:01:05
  Distance: (default is 110)

R1#
```

Copy Paste

Рис. 3.6. Применение команды `show ip protocols`

Задание 8. Просмотрите таблицу маршрутизации, используя команду `show ip route` (рис. 3.7).

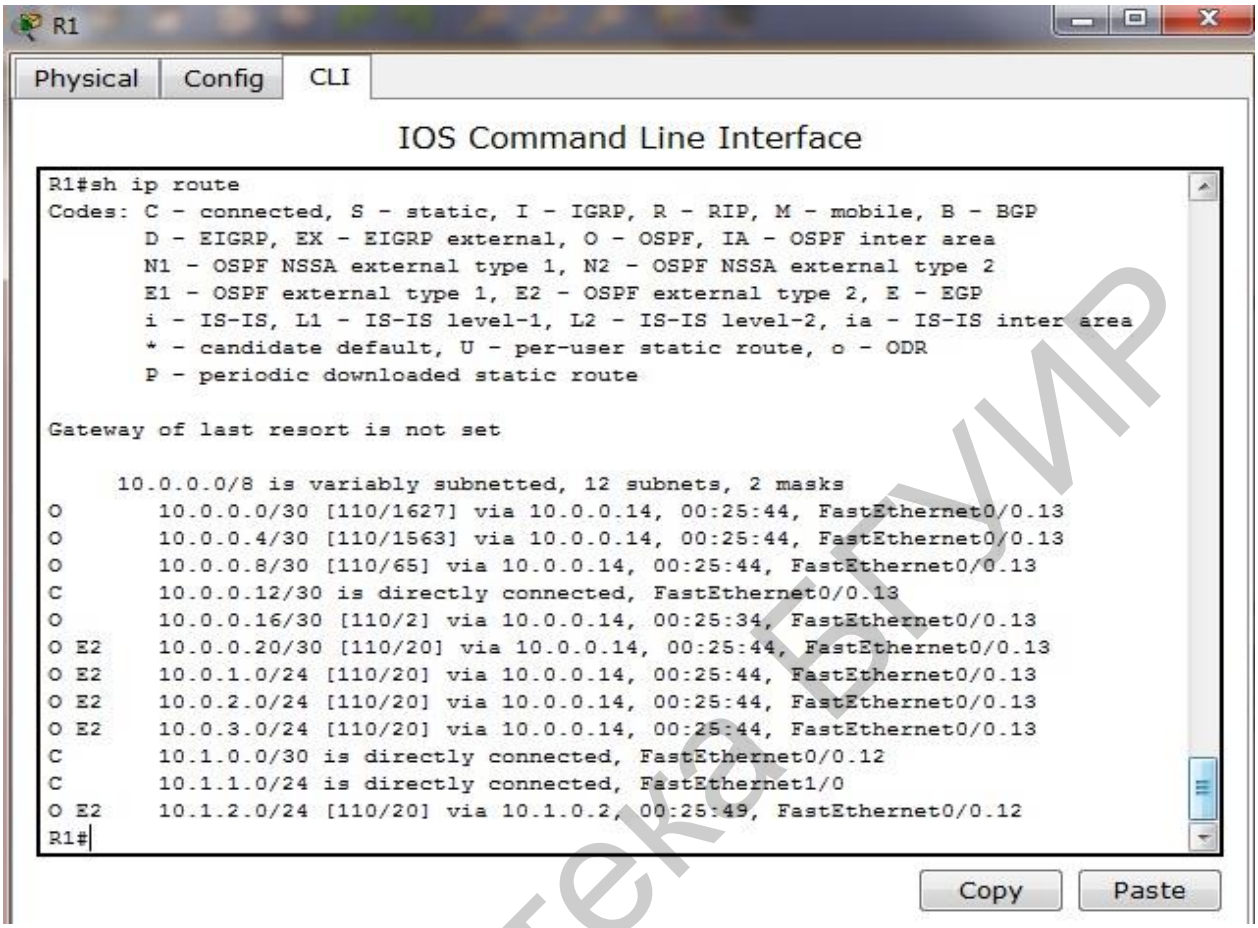


Рис. 3.7. Применение команды `show ip route`

Задание 9. С помощью команды `redistribute connected subnets` ограничьте рассылку LSA-сообщений.

Задание 10. Используя команду `bandwidth`, выберите полосу пропускания для маршрутизатора в соответствии со своим вариантом.

R1(config)#**interface serial0/0/0**
R1(config-if)#**bandwidth 64**
R1(config-if)#**interface Serial0/0/1**
R1(config-if)#**bandwidth 64**

Задание 11. Сделайте отчет по лабораторной работе.

На каждом маршрутизаторе просмотрите настроенную конфигурацию при помощи команды `show running-config`, скопируйте конфигурацию в отчет, также сделайте скриншоты таблиц маршрутизации, таблиц протоколов.

3.5. Контрольные вопросы

1. В каком состоянии находятся маршрутизаторы сети OSPF после того, как были выбраны назначенный (DR) и резервный (BDR) маршрутизаторы?

А. В состоянии ExStrart.

Б. В состоянии Full.

В. В состоянии Loading.

Г. В состоянии Exchange.

2. Какой тип пакетов OSPF используется для установки и поддержки отношений смежности между соседними маршрутизаторами?

А. Запрос информации о состоянии канала (Link-state Request).

Б. Подтверждении получения информации о состоянии канала (Link-state Acknowledgement).

В. Сообщение Hello.

Г. Описание базы данных (Database Description).

3. На чем основана принимаемая по умолчанию оценка канала в протоколе OSPF?

А. На величине задержки в канале.

Б. На величине полосы пропускания.

В. На оценке эффективности работы сети.

Г. Определяется объемом передаваемых по сети данных.

4. Какой адрес многоадресной рассылки предоставляет все OSPF-маршрутизаторы?

А. 224.0.0.6.

Б. 224.0.0.1.

В. 224.0.0.4.

Г. 224.0.0.5.

5. Какая команда может быть использована для изменения OSPF-приоритета на интерфейсе?

А. `ip priority number ospf`.

Б. `ip ospf priority number`.

В. `ospf priority number`.

Г. `set priority ospf number`.

6. Какой адрес многоадресной рассылки используется для рассылки сообщений LSU всем маршрутизаторам DR/BDR?

А. 224.0.0.6.

Б. 224.0.0.1.

В. 224.0.0.4.

Г. 224.0.0.5.

7. Какая команда позволяет маршрутизаторам сети OSPF обмениваться информацией обновления маршрутов без использования многоадресной рассылки?

А. `ip ospf neighdor`.

Б. `ospf neighbor`.

В. `neighbor`.

Г. `ip neighbor`.

8. Какая из приведенных ниже команд отображает все известные маршрутизвтору маршруты и источники, из которых они получены?

А. `show ip protocol`.

Б. `show ip route`.

В. `show ip ospf`.

Г. `show ip ospf neighbor detail`.

9. Для чего используются адреса VLAN?

А. Для обеспечения масштабируемости сети.

Б. Для обеспечения безопасности сети.

В. Для управления потоками данных.

Г. Все вышеперечисленное.

10. Что из перечисленного ниже характерно для сетей VLAN?

А. Широковещательный домен.

Б. Коллизионный домен.

В. Одновременно широковещательный и коллизионный домены.

Г. Имя домена.

11. Какова цель использования маршрутизаторов в топологиях сетей VLAN?

А. Фильтрация широковещания.

Б. Безопасность сети.

В. Управление потоками данных.

Г. Все вышеперечисленные.

12. Что из перечисленного ниже не является критерием, на котором могут базироваться сети VLAN?

А. Идентификатор ID порта.

Б. Протокол.

В. MAC-адрес.

Г. Все вышеперечисленные элементы являются критериями на которых могут базироваться сети VLAN.

13. Какое из перечисленных ниже устройств требуется для передачи пакета из одной сети VLAN в другую?

А. Мост.

Б. Коммутатор.

В. Маршрутизатор.

Г. Концентратор.

14. На каком уровне эталонной модели OSI происходит добавление к фрейму тэга?

А. На 1-м уровне.

Б. На 2-м уровне.

В. На 3-м уровне.

Г. На 4-м уровне.

15. В чем состоит важность создания VLAN-сетей?

А. Становятся более простыми удаление, добавление устройств и другие перемены в сети.

Б. Уменьшается объем передаваемых служебных данных.

В. Маршрутизатор быстрее осуществляет коммутацию.

Г. А и Б.

Литература

1. Амато, В. Основы организации сетей Cisco. В 2 т. Т. 1 / В. Амато. – М. : Вильямс, 2004. – 512 с.
2. Амато, В. Основы организации сетей Cisco. В 2 т. Т. 2 / В. Амато. – М. : Вильямс, 2004. – 464 с.
3. Дансмор, Б. Справочник по телекоммуникационным технологиям / Б. Дансмор. – М. : Вильямс, 2004. – 640 с.
4. Хьюкаби, Д. Руководство Cisco по конфигурированию коммутаторов Catalyst / Д. Хьюкаби. – М. : Вильямс, 2005. – 560 с.
5. Леинванд, А. Конфигурирование маршрутизаторов Cisco / А. Леинванд. – М. : Вильямс, 2001. – 368 с.
6. Мэрфи, К. Структура операционной системы Cisco IOS / К. Мэрфи, В. Боллапрагада. – М. : Вильямс, 2002. – 208 с.
7. Руководство по поиску неисправностей в объединенных сетях. – М. : Вильямс, 2003. – 1040 с.

Св. план 2014, поз. 57

Учебное издание

Цветков Виктор Юрьевич
Волков Кирилл Аркадьевич

ПРОТОКОЛЫ ВНУТРЕННЕЙ МАРШРУТИЗАЦИИ: OSPF И EIGRP

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. И. Герман*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 17.02.2017. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 4,42. Уч.-изд. л. 4,0. Тираж 50 экз. Заказ 389.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6