

# Протоколы маршрутизации

**Наиболее простым способом передачи пакетов по сети является так называемая лавинная маршрутизация, когда каждый маршрутизатор передает пакет всем своим непосредственным соседям, исключая тот, от которого его получил. Понятно, что это — не самый рациональный способ, так как пропускная способность сети используется крайне расточительно, тем не менее такой подход работоспособен.**

**Еще одним видом маршрутизации, не требующим наличия таблиц маршрутизации, является маршрутизация от источника (source routing). В этом случае отправитель помещает в пакет информацию о том, какие промежуточные маршрутизаторы должны участвовать в передаче пакета к сети назначения. На основе этой информации каждый маршрутизатор считывает адрес следующего маршрутизатора, и если он**

**В протоколах маршрутизации чаще всего маршрут выбирается по критерию кратчайшего расстояния. При этом расстояние измеряется в различных метриках. Чаще всего используется простейшая метрика — количество хопов, то есть количество маршрутизаторов, которые нужно преодолеть пакету до сети назначения.**

В качестве метрик применяются также пропускная способность и надежность каналов, вносимые ими задержки и любые комбинации этих метрик.

Протоколу маршрутизации обычно нужно некоторое время, называемое **временем конвергенции**, чтобы после нескольких итераций обмена служебной информацией все маршрутизаторы сети внесли изменения в свои таблицы, и в результате таблицы снова стали согласованными

**Различают протоколы, выполняющие статическую и адаптивную (динамическую) маршрутизацию.**

**При статической маршрутизации все записи в таблице имеют неизменяемый, статический статус, что подразумевает бесконечный срок их жизни. Записи о маршрутах составляются и вводятся в память каждого маршрутизатора вручную администратором сети. При изменении состояния сети администратору необходимо срочно отразить эти изменения в соответствующих таблицах маршрутизации, иначе может произойти их рассогласование, и сеть будет работать некорректно.**

**При адаптивной маршрутизации все изменения конфигурации сети автоматически отражаются в таблицах маршрутизации благодаря протоколам маршрутизации.**

**В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время называют временем жизни (TTL) маршрута. Если по истечении времени жизни существование маршрута не подтверждается протоколом маршрутизации, то он считается нерабочим и перестает использоваться.**

**Протоколы адаптивной маршрутизации бывают распределенными и централизованными.**

**Применяемые сегодня в IP-сетях протоколы маршрутизации относятся к адаптивным распределенным протоколам, которые в свою очередь делятся на две группы:**

- дистанционно-векторные алгоритмы (Distance Vector Algorithm, DVA);**
- алгоритмы состояния связей (Link State Algorithm, LSA).**

**При распределенном подходе все маршрутизаторы сети находятся в равных условиях, они находят маршруты и строят собственные таблицы маршрутизации, работая в тесной кооперации друг с другом, постоянно обмениваясь информацией о конфигурации**

**При централизованном подходе в сети существует один выделенный маршрутизатор, который собирает всю информацию о топологии и состоянии сети от других маршрутизаторов. На основании этих данных выделенный маршрутизатор (который иногда называют сервером маршрутов) строит таблицы маршрутизации для всех остальных маршрутизаторов сети, а затем распространяет их по сети, чтобы каждый маршрутизатор получил собственную таблицу и в дальнейшем самостоятельно принимал решение о продвижении каждого**

**В дистанционно-векторных алгоритмах (DVA) каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей.**

Получив от некоторого соседа вектор расстояний до известных тому сетей, маршрутизатор наращивает компоненты вектора на величину расстояния от себя до данного соседа.

Обновленное значение вектора маршрутизатор рассылает своим соседям. В конце концов каждый маршрутизатор узнает через соседние маршрутизаторы информацию обо всех имеющихся в составной сети сетях и о расстояниях до них.

Затем он выбирает из нескольких альтернативных маршрутов к каждой сети тот маршрут, который обладает наименьшим

**Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях.** В больших сетях они периодически засоряют линии связи интенсивным трафиком, к тому же изменения конфигурации не всегда корректно могут отражаться алгоритмом этого типа, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только косвенной информацией — вектором расстояний.

**Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме,**

**Алгоритмы состояния связей (LSA) обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети.**

Каждый маршрутизатор использует граф сети для нахождения оптимальных по некоторому критерию маршрутов до каждой из сетей, входящих в составную сеть. Чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор обменивается короткими пакетами HELLO со своими ближайшими соседями.

В результате служебный трафик, создаваемый протоколами LSA, гораздо менее интенсивный, чем у протоколов DVA.

Протоколами, основанными на алгоритме состояния связей, являются протокол IS-IS стека OSI (этот протокол используется также в стеке TCP/IP) и протокол OSPF стека TCP/IP.

# Протокол RIP

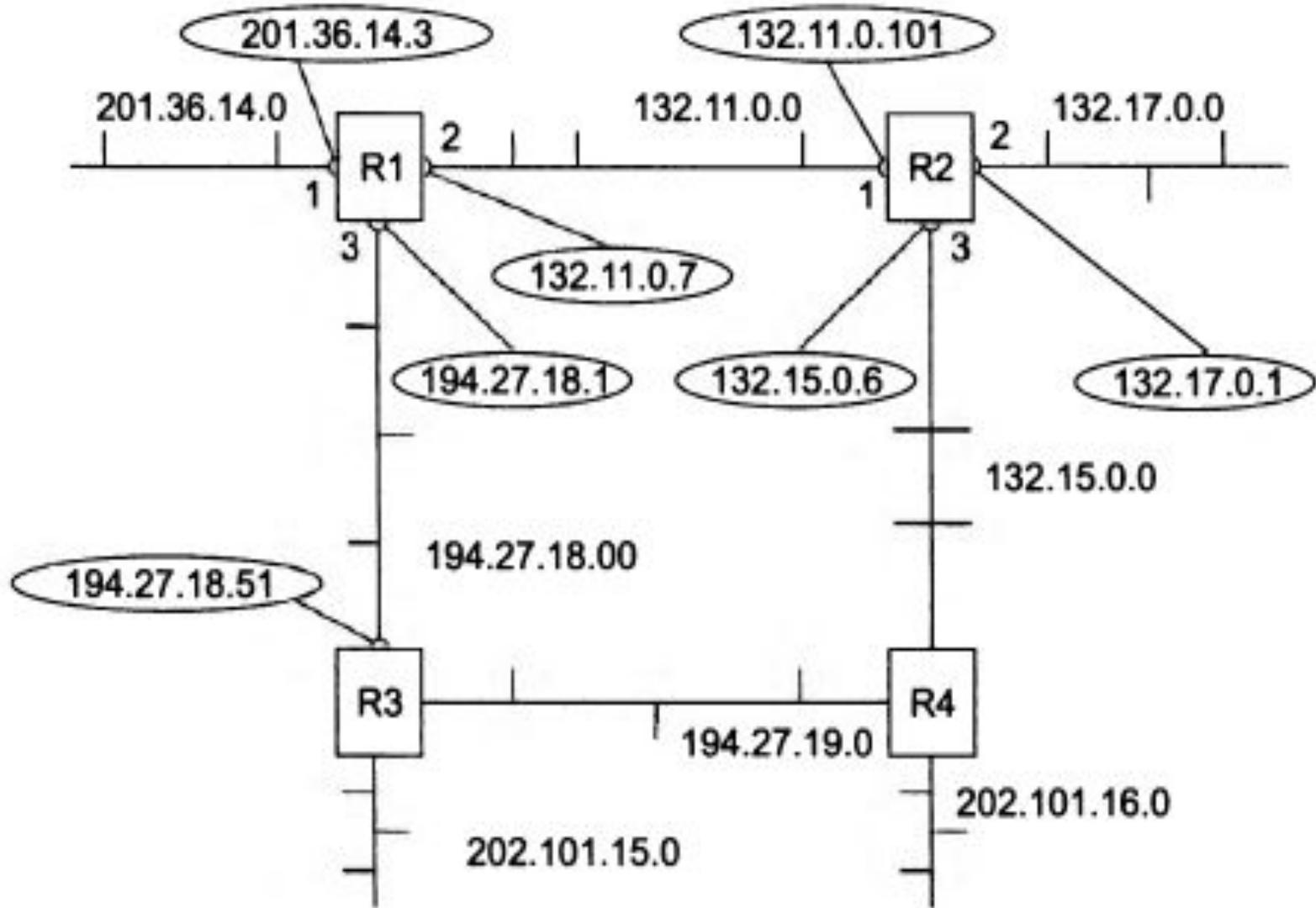
**Протокол RIP (Routing Information Protocol — протокол маршрутной информации) является внутренним протоколом маршрутизации дистанционно-векторного типа.**

Будучи простым в реализации, этот протокол чаще всего используется в небольших сетях. Для IP имеются две версии RIP — RIPv1 и RIPv2. Протокол RIPv1 не поддерживает масок. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня

# Построение таблицы маршрутизации

Для измерения расстояния до сети стандарты протокола RIP допускают различные виды метрик: **хопы**, значения **пропускной способности**, **вносимые задержки**, **надежность сетей**, а также любые комбинации этих метрик. Метрика должна обладать свойством **аддитивности** — метрика составного пути должна быть равна сумме метрик составляющих этого пути. В большинстве реализаций RIP используется простейшая метрика — количество **хопов**, то есть количество **промежуточных маршрутизаторов**, которые нужно преодолеть пакету до сети назначения.

- **Этап 1 — создание минимальной таблицы.**



**Рис. 17.1.** Сеть, построенная на маршрутизаторах RIP

**Таблица 17.1.** Минимальная таблица маршрутизации маршрутизатора R1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

**Таблица 17.2.** Минимальная таблица маршрутизации маршрутизатора R2

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
132.11.0.0	132.11.0.101	1	1
132.17.0.0	132.17.0.1	2	1
132.15.0.0	132.15.0.6	3	1

- **Этап 2 — рассылка минимальной таблицы соседям.**

**По отношению к любому маршрутизатору соседями являются те маршрутизаторы, которым данный маршрутизатор может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных маршрутизаторов.**

Таким образом, маршрутизатор R1 передает маршрутизаторам R2 и R3 следующие сообщения:

- сеть 201.36.14.0, расстояние 1;
- сеть 132.11.0.0, расстояние 1;
- сеть 194.27.18.0, расстояние 1.

- **Этап 3 — получение RIP-сообщений от соседей и обработка полученной информации**

**Таблица 17.3.** Таблица маршрутизации маршрутизатора R1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
<del>132.11.0.0</del>	<del>132.11.0.101</del>	<del>2</del>	<del>2</del>
<del>194.27.18.0</del>	<del>194.27.18.51</del>	<del>3</del>	<del>2</del>

Записи с четвертой по девятую получены от соседних маршрутизаторов, и они претендуют на помещение в таблицу. Однако только записи с четвертой по седьмую попадают в таблицу, а записи восьмая и девятая — нет. **Протокол RIP замещает запись о какой-либо сети только в том случае, если новая информация имеет лучшую метрику (с меньшим расстоянием в хопх), чем имеющаяся**

- **Этап 4 — рассылка новой таблицы соседям.**

Каждый маршрутизатор отсылает новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные обо всех известных ему сетях: как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из RIP-сообщений.

**Этап 5 — получение RIP-сообщений от соседей и обработка полученной информации.** Этап 5 повторяет этап 3 — маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы

**Таблица 17.4.** Таблица маршрутизации маршрутизатора R1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
<del>132.15.0.0</del>	<del>194.27.18.51</del>	<del>3</del>	<del>3</del>
194.27.19.0	194.27.18.51	3	2
<del>194.27.19.0</del>	<del>132.11.0.101</del>	<del>2</del>	<del>3</del>
202.101.15.0	<del>194.27.18.51</del>	<del>3</del>	<del>2</del>
202.101.16.0	132.11.0.101	2	3
<del>202.101.16.0</del>	<del>194.27.18.51</del>	<del>3</del>	<del>3</del>

## **Адаптация маршрутизаторов RIP к изменениям состояния сети**

**К новым маршрутам маршрутизаторы RIP приспособляются просто — они передают новую информацию в очередном сообщении своим соседям, и постепенно эта информация становится известна всем маршрутизаторам сети. А вот к изменениям, связанным с потерей какого-либо маршрута, маршрутизаторы RIP адаптируются сложнее. Это связано с тем, что в формате сообщений протокола RIP нет поля, которое бы указывало на то, что путь к данной сети больше не существует.**

**Для уведомления о том, что некоторый маршрут недействителен, используются два механизма:**

- истечение времени жизни маршрута;**
- указание специального (бесконечного) расстояния до сети, ставшей недоступной.**

**Механизм истечения времени жизни маршрута основан на том, что каждая запись таблицы маршрутизации, полученная по протоколу RIP, имеет время жизни (TTL). При поступлении RIP-сообщения, таймер времени жизни устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм-аута не придет новое сообщение о маршруте, он помечается как недействительный.**

Время тайм-аута связано с периодом рассылки векторов по сети. В протоколе RIP период рассылки выбран равным 30 секундам, а тайм-аут — 180 секундам.

Механизм таймаута работает в тех случаях, когда маршрутизатор не может послать соседям сообщение об отказавшем маршруте, так как либо сам неработоспособен, либо неработоспособна линия связи, по которой можно было бы передать

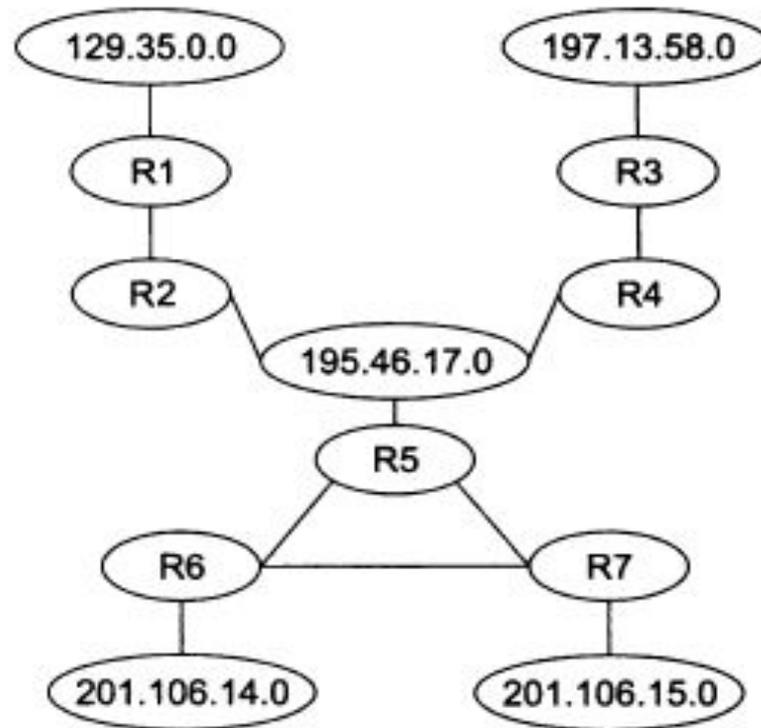
Когда же сообщение послать можно, маршрутизаторы RIP используют прием, заключающийся в указании **бесконечного расстояния до сети**, ставшей недоступной. **В протоколе RIP бесконечным условно считается расстояние в 16 хопов.** Получив сообщение, в котором расстояние до некоторой сети равно 16, маршрутизатор должен проверить, исходит ли эта «плохая» информация о сети от того же маршрутизатора, сообщение которого послужило в свое время основанием для записи о данной сети в таблице маршрутизации. Если это тот же маршрутизатор, то информация считается достоверной и маршрут помечается как

# Протокол OSPF

**Протокол OSPF (Open Shortest Path First — выбор кратчайшего пути первым) является последним протоколом, основанном на алгоритме состояния связей, и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях.**

**OSPF разбивает процедуру построения таблицы маршрутизации на два этапа, к первому относится построение и поддержание базы данных о состоянии связей сети, ко второму — нахождение оптимальных маршрутов и генерация**

**Построение и поддержание базы данных о состоянии связей сети. Связи сети могут быть представлены в виде графа, в котором вершинами графа являются маршрутизаторы и подсети, а ребрами — связи между ними. Каждый маршрутизатор обменивается со своими соседями той информацией о графе сети, которой он располагает к данному моменту. Сообщения, с помощью которых распространяется топологическая информация, называются объявлениями о состоянии связей (Link State Advertisement, LSA) сети.**



**Рис. 17.2.** Граф сети, построенный протоколом OSPF

# **Нахождение оптимальных маршрутов и генерация таблицы маршрутизации.**

Задача нахождения оптимального пути на графе является достаточно сложной и трудоемкой. В протоколе OSPF для ее решения используется итеративный алгоритм Дейкстры. Каждый маршрутизатор сети, действуя в соответствии с этим алгоритмом, ищет оптимальные маршруты от своих интерфейсов до всех известных ему подсетей. В каждом найденном таким образом маршруте запоминается только один шаг — до следующего маршрутизатора. Данные об этом шаге и попадают в таблицу маршрутизации.

**Если состояние связей в сети изменилось и произошла корректировка графа сети, каждый маршрутизатор заново ищет оптимальные маршруты и корректирует свою таблицу маршрутизации. Аналогичный процесс происходит и в том случае, когда в сети появляется новая связь или новый сосед.**

Когда состояние сети не меняется, то объявления о связях не генерируются, топологические базы данных и таблицы маршрутизации не корректируются, что экономит пропускную способность сети и вычислительные ресурсы маршрутизаторов. **Однако каждые 30 минут маршрутизаторы OSPF обмениваются всеми записями базы данных топологической информации.**

# Метрики

При поиске оптимальных маршрутов протокол OSPF по умолчанию использует метрику, учитывающую **пропускную способность каналов связи**. Кроме того, допускается применение двух других метрик, учитывающих **задержки и надежность передачи пакетов** каналами связи. **Для каждой из метрик протокол OSPF строит отдельную таблицу маршрутизации**. Выбор нужной таблицы происходит в зависимости от значений битов TOS в заголовке пришедшего IP-пакета.

Например, если в пакете бит D установлен в 1, то для этого пакета маршрут должен выбираться из таблицы, в которой содержатся маршруты, имеющие минимальную задержку.

Для преодоления вычислительной сложности с ростом сети в протоколе OSPF вводится понятие **области сети**. Маршрутизаторы, принадлежащие некоторой области, строят граф связей только для этой области, что упрощает задачу. **Между областями информация о связях не передается, а пограничные для областей маршрутизаторы обмениваются только информацией об адресах сетей, имеющихся в каждой из областей, и расстоянием от пограничного маршрутизатора до каждой сети.**

# Взаимодействие протоколов маршрутизации

В одной и той же сети могут одновременно работать несколько разных протоколов маршрутизации.

В маршрутизаторе, который поддерживает одновременно несколько протоколов, каждая запись в таблице является результатом работы одного из этих протоколов. Если информация о некоторой сети появляется от нескольких протоколов, то для однозначности выбора маршрута устанавливается приоритет протоколов.

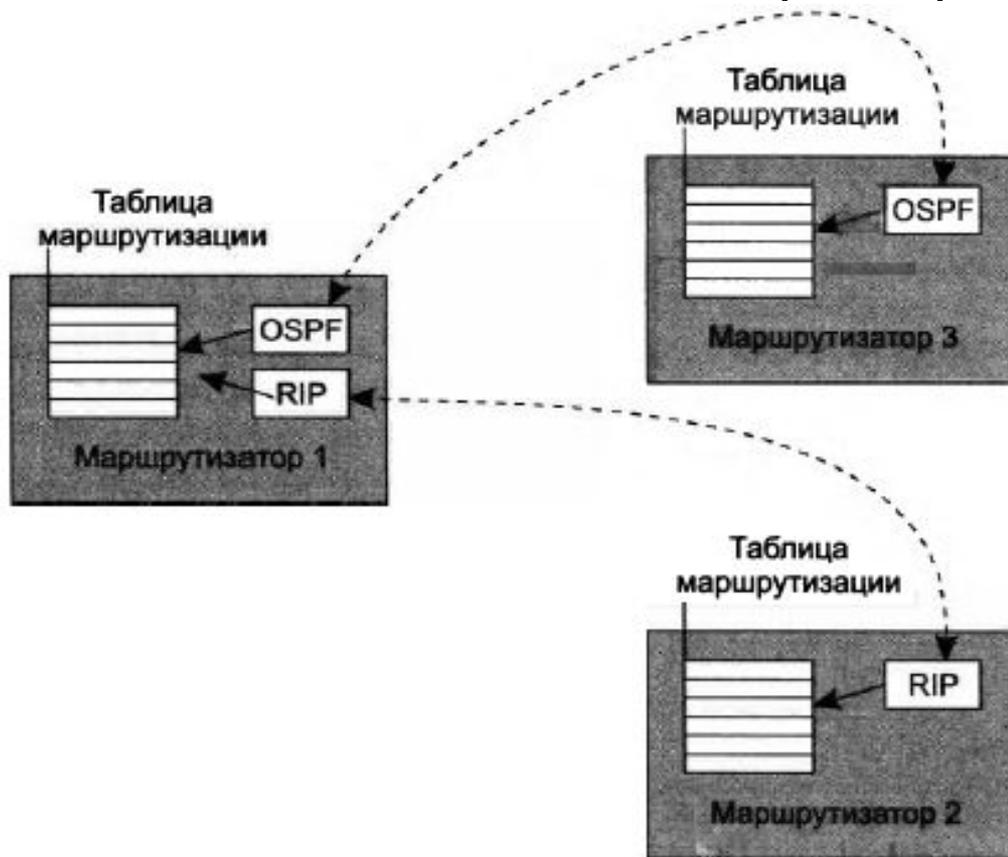


Рис. 17.3. Применение нескольких протоколов маршрутизации в одной сети

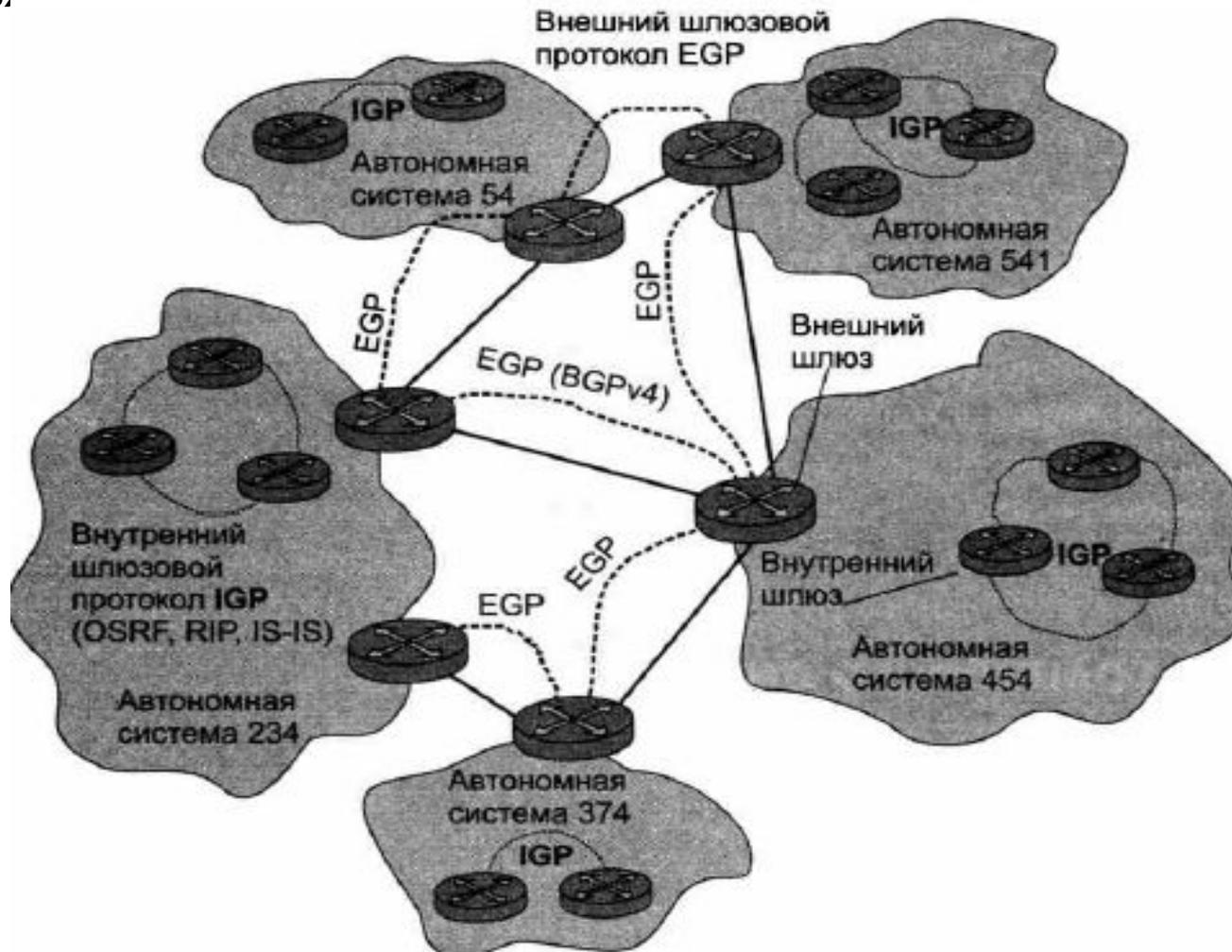
**По умолчанию каждый протокол маршрутизации, работающий на определенном маршрутизаторе, распространяет только «собственную» информацию, то есть ту информацию, которая была получена данным маршрутизатором по данному протоколу.**

Возможность обмена маршрутной информацией реализуется в особом режиме работы маршрутизатора, называемом **режимом перераспределения маршрутов**. Этот режим позволяет одному протоколу маршрутизации использовать не только «свои», но и «чужие» записи таблицы маршрутизации, полученные с помощью другого протокола маршрутизации, указанного при конфигурировании.

**Автономная система (Autonomous System, AS) — это совокупность сетей под единым административным управлением, обеспечивающую общую для всех входящих в автономную систему маршрутизаторов политику маршрутизации.**

В соответствии с этой концепцией Интернет выглядит как набор взаимосвязанных автономных систем, каждая из которых состоит из взаимосв:

ми.



**Рис. 17.4.** Автономные системы Интернета

Основная цель деления Интернета на автономные системы — **обеспечение многоуровневого подхода к маршрутизации.**

**С появлением автономных систем появляется третий, верхний, уровень маршрутизации — теперь сначала маршрут определяется как последовательность автономных систем, затем — как последовательность сетей и только потом ведет к конечному узлу.**

Выбор маршрута между автономными системами осуществляют **внешние шлюзы**, использующие особый тип протокола маршрутизации, так называемый **внешний шлюзовой протокол (Exterior Gateway Protocol, EGP)**. В настоящее время для работы в такой роли сообщество Интернета утвердило **стандартный пограничный шлюзовой протокол версии 4 (Border Gateway Protocol**

# Протокол BGP

BGP успешно работает при любой топологии связей между автономными системами, что соответствует современному состоянию Интернета.

Поясним основные принципы работы BGP на

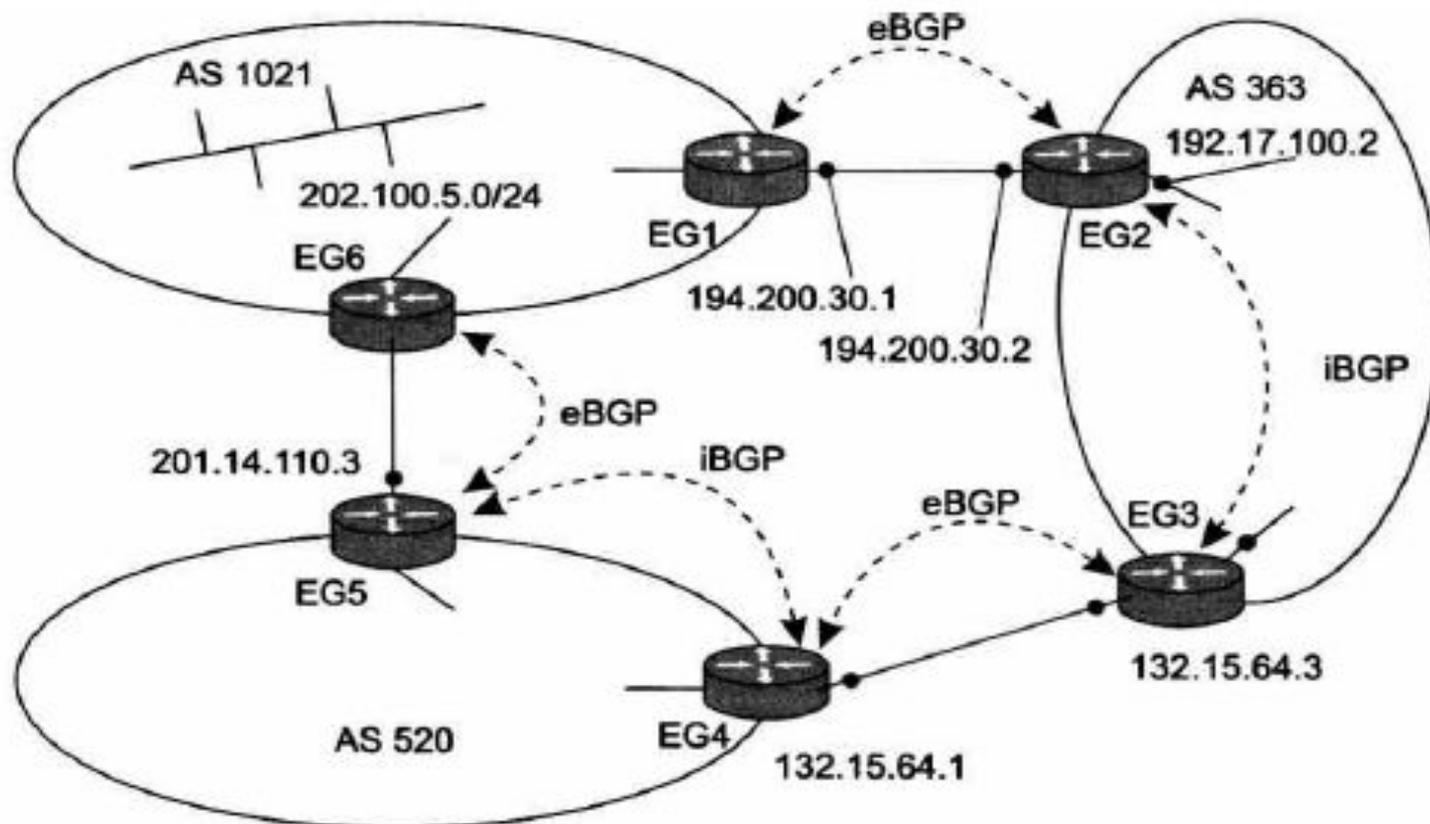


Рис. 17.5. Поиск маршрута между автономными системами с помощью протокола BGP

Такой способ взаимодействия удобен в ситуации, когда маршрутизаторы, обменивающиеся маршрутной информацией, принадлежат разным поставщикам услуг (ISP). Протоколы RIP и OSPF, разработанные для применения внутри автономной системы, обмениваются маршрутной информацией со всеми маршрутизаторами, находящимися в пределах их непосредственной досягаемости. Это означает, что информация обо всех сетях появляется в таблице маршрутизации каждого маршрутизатора, так что каждая сеть оказывается достижимой для каждой. В корпоративной сети это нормальная ситуация, а в сети ISP нет, поэтому протокол BGP и исполняет здесь особую роль, поддерживая разнообразные и гибкие политики маршрутизации.

Политика маршрутизации провайдера отражает условия по взаимной передаче трафика, имеющиеся в **соглашениях об уровне обслуживания (SLA)**, или в **пиринговых соглашениях**, которые провайдер

# Стандартная модель группового вещания IP

Основной целью группового вещания является создание эффективного механизма передачи данных от одного источника нескольким получателям.

При **индивидуальной рассылке** (unicast) на основе уникальных адресов источник данных, которые надо доставить некоторой группе узлов, генерирует их в количестве экземпляров, равном количеству узлов-получателей, состоящих в данной группе

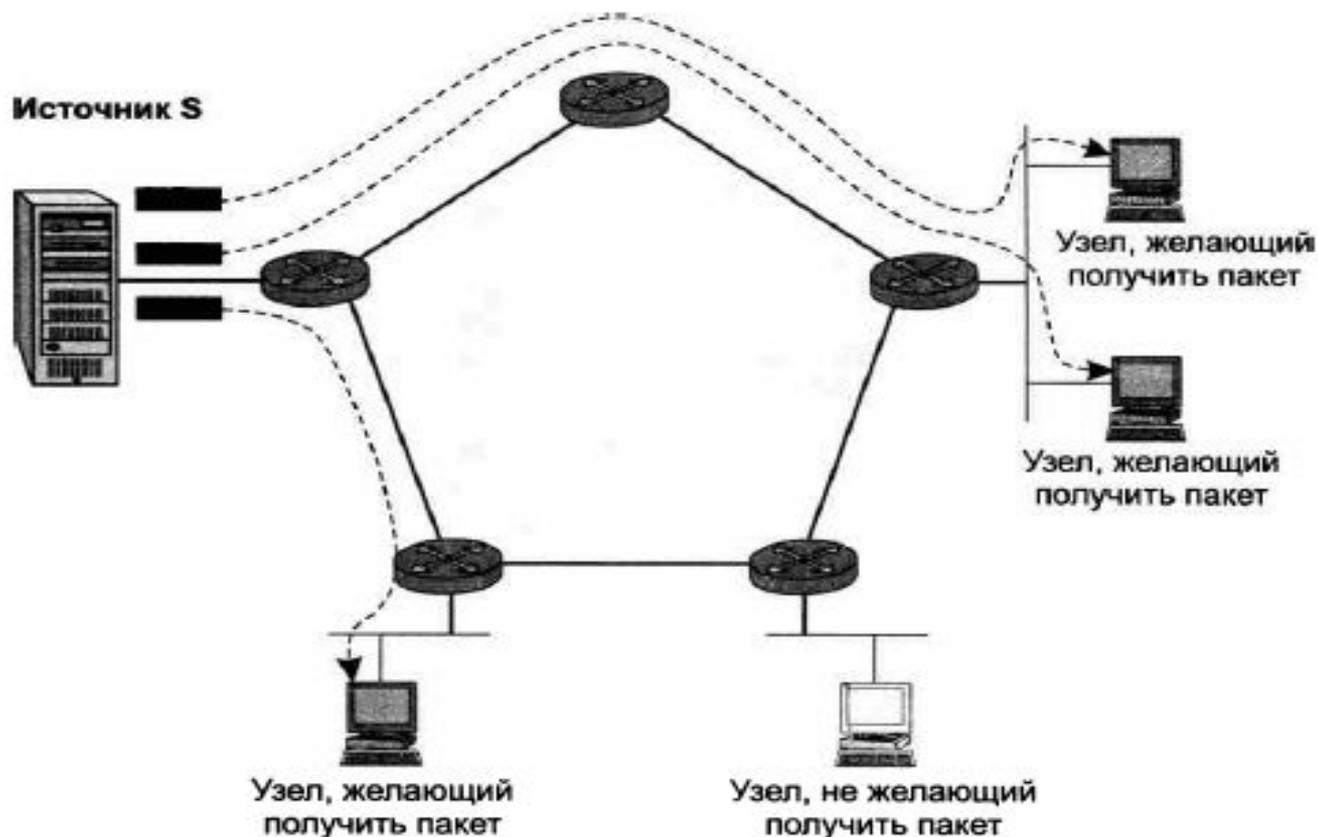


Рис. 17.6. Групповая доставка на основе индивидуальных адресов

При широковещательной рассылке (broadcast) станция направляет пакеты, используя широковещательные адреса. В этой схеме для того, чтобы доставить данные группе узлов-получателей, источник генерирует один экземпляр данных, но снабжает этот экземпляр широковещательным адресом, который диктует маршрутизаторам сети копировать данные и рассыл

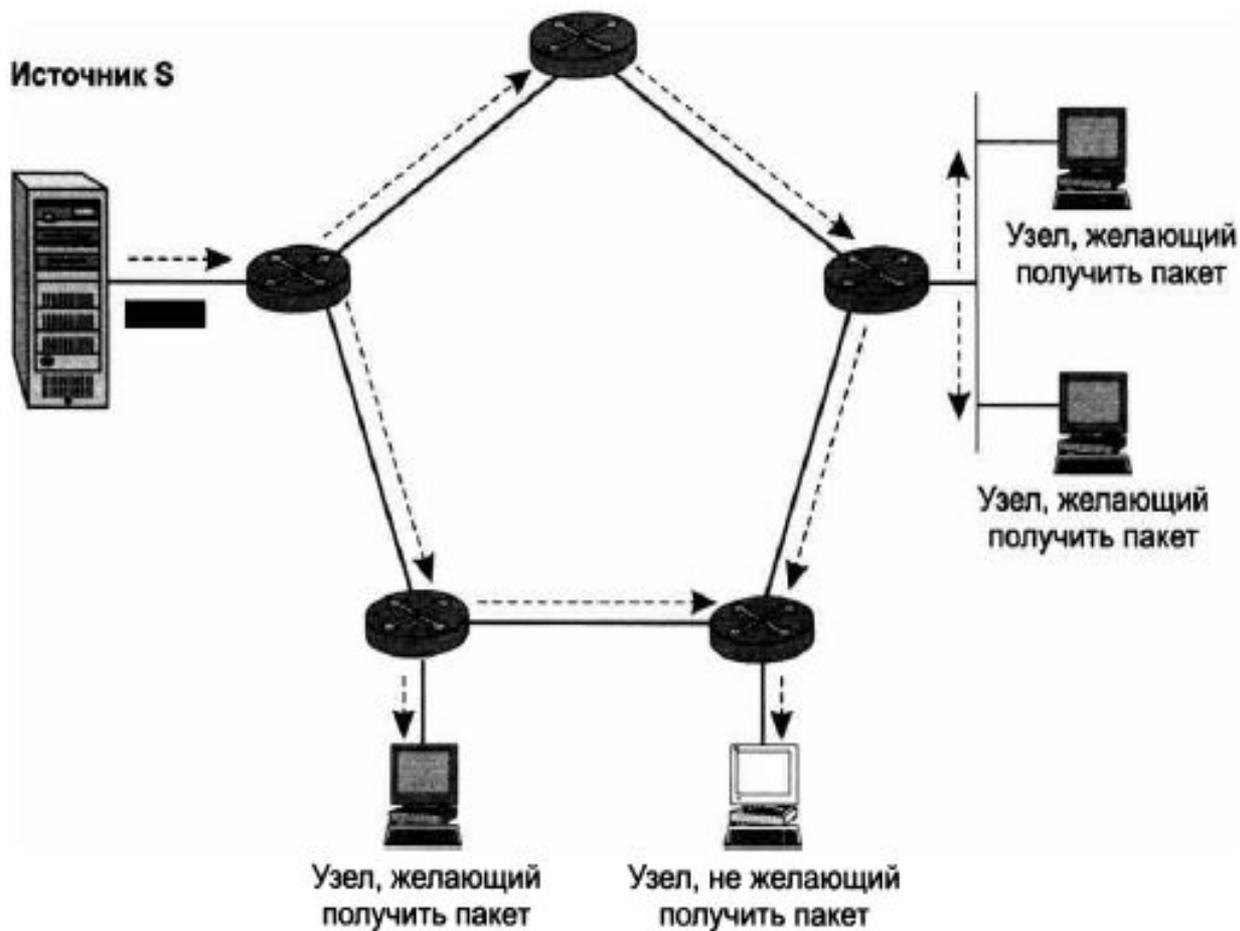


Рис. 17.7. Групповая доставка на основе широковещательного адреса

В случае привлечения сервисов прикладного уровня функции по обеспечению групповой доставки переключаются на самих членов группы. То есть источник генерирует один экземпляр данных и, используя индивидуальный адрес, передает данные одному из членов группы, который генерирует копию и направляет ее другому члену группы, и т. д.

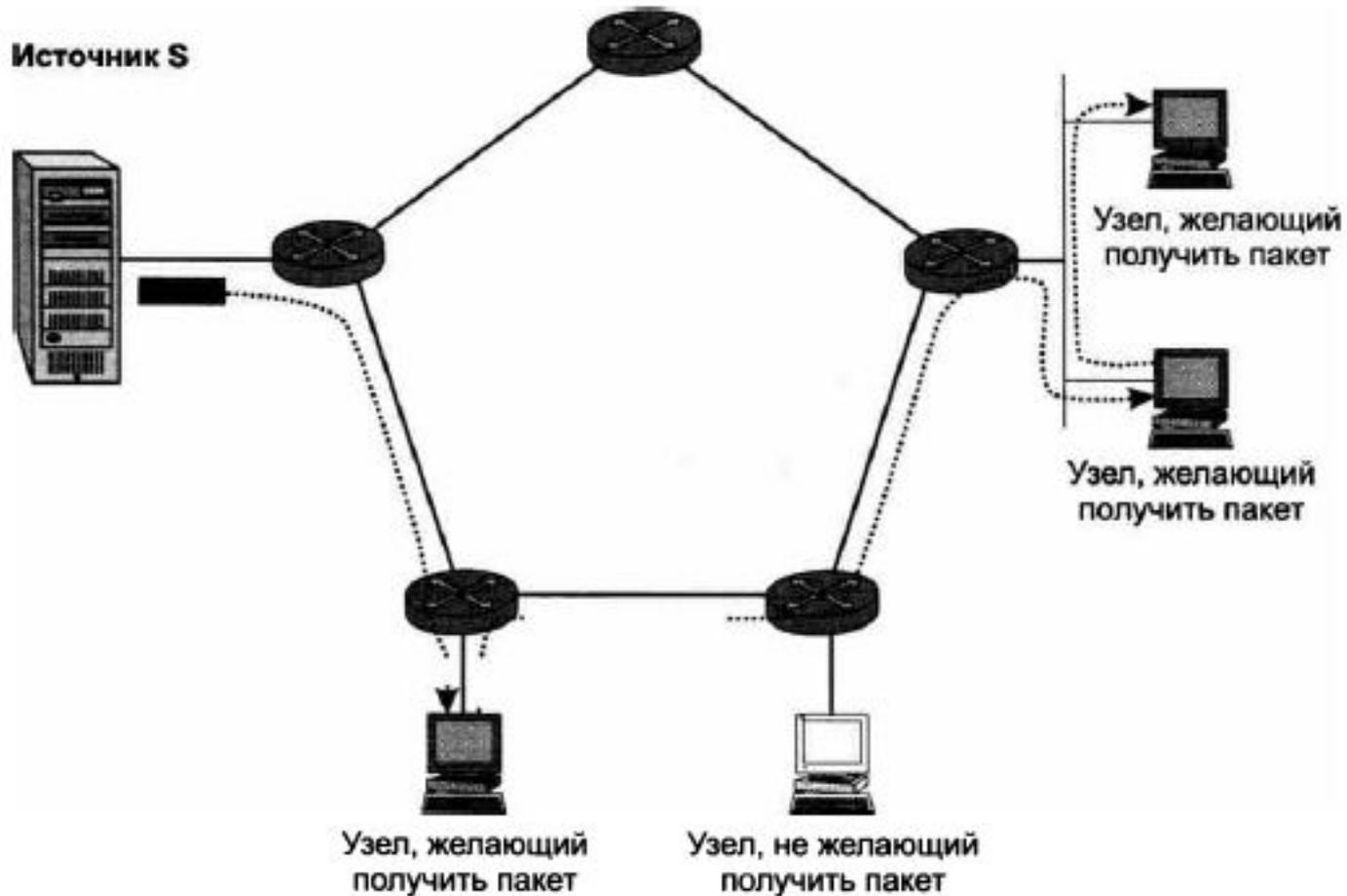


Рис. 17.8. Групповая доставка на основе сервисов прикладного уровня

Главная идея группового вещания состоит в следующем: источник генерирует только один экземпляр сообщения с групповым адресом, которое затем, по мере перемещения по сети, копируется на каждой из «развилкок», ведущих к тому или иному члену группы, указанной в адресе данного сообщения.

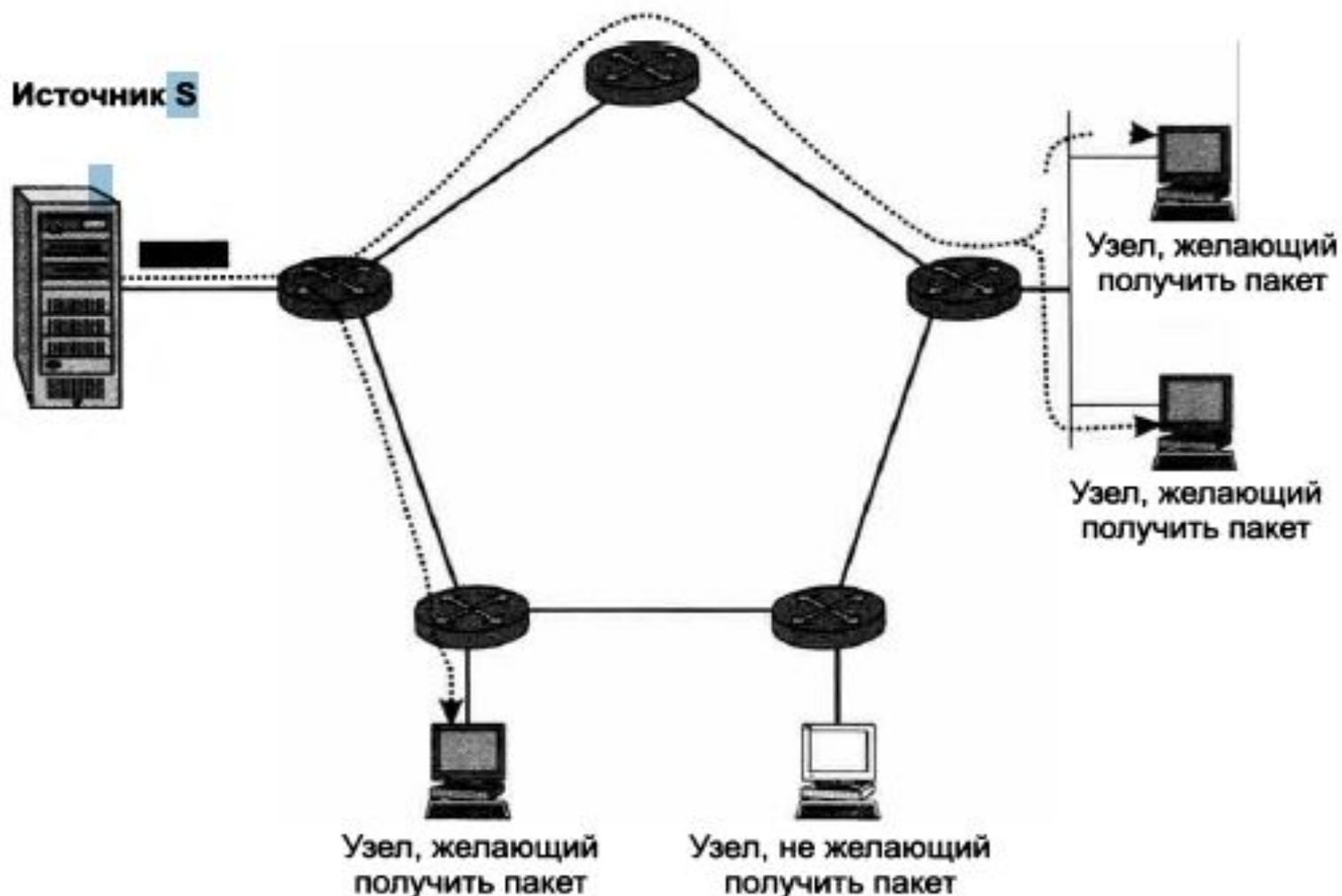


Рис. 17.9. Схема группового вещания

Пакет с групповым адресом достигает маршрутизатора, к которому непосредственно подключена сеть с хостами — членами данной группы.

Маршрутизатор упаковывает пакет с групповым адресом в кадр канального уровня, снабжая его групповым MAC-адресом, соответствующим групповому IP-адресу пакета. Кадр с пакетом группового вещания поступает в локальную сеть, распознается и захватывается интерфейсами хостов, являющихся членами данной группы. При таком подходе данные рассылаются только тем узлам, которые заинтересованы в их получении.

Есть несколько принципиальных положений, регламентирующих поведение конечных узлов сети, которые являются источниками и получателями группового трафика.

- **Дейтаграммный подход.** Источник может посылать пакеты UDP/IP в любое время без необходимости регистрировать или планировать передачи, реализуя сервис «по возможности».
- **Открытые группы.** Источники должны знать только групповой адрес. Группа может быть образована узлами, принадлежащими к разным IP-сетям и подсетям. Группа может иметь любое число источников данных.
- **Динамические группы.** Хосты могут присоединяться к группам или покидать группы без необходимости регистрации, синхронизации или переговоров с каким-либо централизованным элементом группового управления. Членство в группе является динамическим, поскольку хосты могут присоединиться к группе или выйти из группы в любой момент времени, к тому же они могут быть членами нескольких групп.

## Адреса группового вещания

Ранее в главе 14, изучая типы IP-адресов, мы отмечали, что адреса IPv4 из диапазона

0.0-239.255.255.255 относятся к классу D и зарезервированы для группового вещания.

Адреса из этого диапазона используются:

- для идентификации групп;
- для идентификации адресов источников группового вещания (в рамках модели SSM);
- для административных нужд при реализации группового вещания.

## Структурирование адресного пространства группового вещания

Протоколы группового вещания делятся на две категории. В первую входит один протокол — **протокол IGMP**, с помощью которого хосты сообщают о своей «желании» присоединиться к некоторой группе, и маршрутизатор узнает о принадлежности хостов в подсетях к той или иной группе. Вторую группу составляют **протоколы маршрутизации группового вещания**.

# Протокол IGMP

К основным функциям протокола IGMP относятся оповещение маршрутизатора о желании хоста быть включенным в группу и опрос членов группы.

**Оповещение маршрутизатора о желании хоста быть включенным в группу.** Чтобы стать получателем групповых данных, узел должен «выразить» свою заинтересованность маршрутизатору, к которому непосредственно подсоединена его сеть. Для этого хост должен установить взаимодействие с маршрутизатором по протоколу IGMP. Версия IGMP для хоста непосредственно зависит от типа операционной системы, установленной на хосте.

**Опрос членов группы.** Для выполнения этой функции один из маршрутизаторов локальной сети выбирается доминирующим. Доминирующий маршрутизатор средствами протокола IGMP периодически опрашивает все системы в непосредственно присоединенных к нему подсетях, проверяя, активны ли члены всех известных ему групп. Остальные маршрутизаторы прослушивают сеть, и если обнаруживают отсутствие сообщений-запросов, то повторяют процедуру выбора нового доминирующего

В IGMPv2 определено три типа сообщений:

- **Запрос о членстве (membership query).** С помощью этого сообщения маршрутизатор пытается узнать, в каких группах состоят хосты в локальной сети, присоединенной к какому-либо его интерфейсу.
- **Отчет о членстве (membership report).** Этим сообщением хосты отвечают маршрутизатору, который послал в сеть запрос о членстве. В сообщении содержится информация об адресе группы, в которой они состоят. Маршрутизатор, являясь членом всех групп, получает сообщения, направленные на любой групповой адрес. Для маршрутизатора, получающего ответные сообщения, важен только факт наличия членов той или иной группы (групп), а не принадлежность конкретных хостов конкретным группам.
- **Покинуть группу (leave group).** Это сообщение хост может использовать, чтобы сигнализировать «своему» маршрутизатору о желании покинуть определенную группу, в которой он до этого состоял. Получив это сообщение, маршрутизатор посылает специфический запрос о членстве членам только этой конкретной группы, и если не получает на него ответа (что говорит о том, что это последний хост в группе), то перестает передавать трафик группового вещания для этой группы.

Основываясь на информации, полученной с помощью IGMP, маршрутизаторы могут определять, в какие подключенные к ним сети необходимо передавать групповой трафик. Все типы IGMP-сообщений имеют длину 8 байт и состоят из четырех полей. В зависимости от версии протокола IGMP назначение полей может несколько меняться. На рис. 17.10 показана структура сообщения для версии IGMPv2.



**Рис. 17.10.** Структура IGMP-сообщения

# Принципы маршрутизации трафика группового вещания

Среди принципов маршрутизации трафика группового вещания можно отметить:

- маршрутизацию на основе доменов;
- учет плотности получателей группового трафика;
- два подхода к построению маршрутного дерева;
- концепцию продвижения по реверсивному пути.

**Маршрутизация на основе доменов.** Для улучшения масштабируемости предложен иерархический подход, основанный на доменах. Подобно автономным системам (доменам маршрутизации) и DNS-доменам вводятся домены группового вещания. Для доставки информации в пределах домена предлагаются одни методы и протоколы маршрутизации группового вещания, называемые внутримоменными, а в пределах

- **Учет плотности получателей группового трафика.** Внутридоменные протоколы маршрутизации разделяются на два принципиально отличных класса:

- **Протоколы плотного режима (Dense Mode, DM)** разработаны в предположении, что в сетевом домене существует большое число принимающих узлов. Отсюда следует главная идея этих протоколов: сначала «затопить» сеть пакетами группового вещания по всем направлениям, останавливая продвижение пакетов, лишь когда находящийся на пути распространения трафика маршрутизатор явно сообщит, что далее ниже по потоку членов данной группы нет.

- **Протоколы разряженного режима (Sparse Mode, SM)** рассчитаны на работу в сети, в которой количество маршрутизаторов с подключенными к ним членами групп невелико по сравнению с общим числом маршрутизаторов.

В сети, использующей протокол класса SM, необходимо существование центрального элемента, обычно называемого **точкой рандеву**, или встречи (Rendezvous Point, RP). Точка встречи должна существовать для каждой имеющейся в сети группы и быть единственной для

## **Два подхода к построению маршрутного дерева.**

Все протоколы маршрутизации группового вещания используют один из следующих двух подходов.

Для всех источников данной группы строится единственный граф связей, называемый **разделяемым деревом**. Этот граф связывает всех членов данной группы. Разделяемое дерево может включать также и необходимые для обеспечения связности маршрутизаторы, не имеющие в своих присоединенных сетях членов данной группы.

Разделяемое дерево служит для доставки трафика всем членам данной группы от каждого из источников, вещающих на данную группу.

Для каждой группы строятся несколько графов по числу источников, вещающих на каждую из этих групп. Каждый такой граф, называемый деревом с вершиной в источнике, служит для доставки трафика всем членам группы, но только от одного источника.

## **Концепция продвижения по реверсивному пути.**

Маршрутизатор проверяет, является ли входной интерфейс, получивший групповой пакет, интерфейсом, через который пролегает кратчайший путь к источнику. Он делает это с помощью обычной таблицы маршрутизации, которая содержит указания о рациональных путях ко всем сетям составной интерсети. Проверка факта выполнения данного условия называется продвижением по реверсивному пути (Reverse Path Forwarding, RPF). Только пакеты, которые прошли RPF-проверку, являются кандидатами для дальнейшего продвижения вдоль путей, ведущих к потенциальным получателям трафика группового вещания.

Концепция продвижения по реверсивному пути является главной при маршрутизации группового трафика независимо от того, какой протокол при этом использован.

## Протоколы маршрутизации группового вещания

Протоколы маршрутизации осуществляют постоянный мониторинг покрывающего дерева и время от времени отсекают ветви дерева, которые из-за изменения состояния сети уже не ведут к членам той или иной группы.

**Дистанционно-векторный протокол маршрутизации группового вещания** (Distance Vector Multicast Routing Protocol, DVMRP) можно охарактеризовать следующим образом:

- основан на дистанционно-векторном алгоритме и, следовательно, обладает всеми особенностями, свойственными данному алгоритму;
- относится к классу протоколов плотного режима, использующих проверку продвижения по реверсивному пути;
- продвигает пакеты на основе деревьев с вершинами в источниках;
- является протокольно зависимым в том смысле, что для принятия решений о продвижении пакетов он не может использовать обычные (для индивидуальной рассылки) таблицы маршрутизации.

**Протокол MOSPF** (Multicast extensions to OSPF) для поддержки группового вещания опирается на обычные механизмы OSPF. Маршрутизаторы MOSPF добавляют к информации о состоянии связей, распространяемой по протоколу OSPF, данные о членстве в группах узлов в непосредственно присоединенных сетях. Эти

**Протокол PIM-SM** является одной из двух версий протокола PIM (Protocol Independent Multicast):

- **версии плотного режима PIM-DM** (Dense Mode);
- **версии разряженного режима PIM-SM** (Sparse Mode).

Эти версии существенно отличаются друг от друга способом построения и использования покрывающего дерева, но у них есть одно общее свойство- это независимость данного протокола от конкретных протоколов маршрутизации. Если DVMRP использует в своей работе механизмы RIP, а протокол MOSPF является расширением протокола OSPF, то протокол PIM может работать совместно с любым протоколом маршрутизации.

Протокол PIM-DM похож на протокол DVMRP. Он, также являясь протоколом плотного режима, строит для доставки групповых пакетов деревья с вершиной в источнике, используя для этого проверки продвижения по реверсивному пути и технику широковещания и усечения. Основное отличие состоит в том, что протокол PIM-DM применяет готовую таблицу маршрутизации, а не строит ее сам, как это делает DVMRR.

Главной особенностью протокола PIM-SM является то, что он рассчитан на работу в разряженном режиме, то есть он посылает групповые пакеты только по явному запросу получателя. Для доставки данных каждой конкретной группе получателей протокол PIM-SM строит одно разделяемое дерево, общее для всех источников этой группы (рис. 17.11).

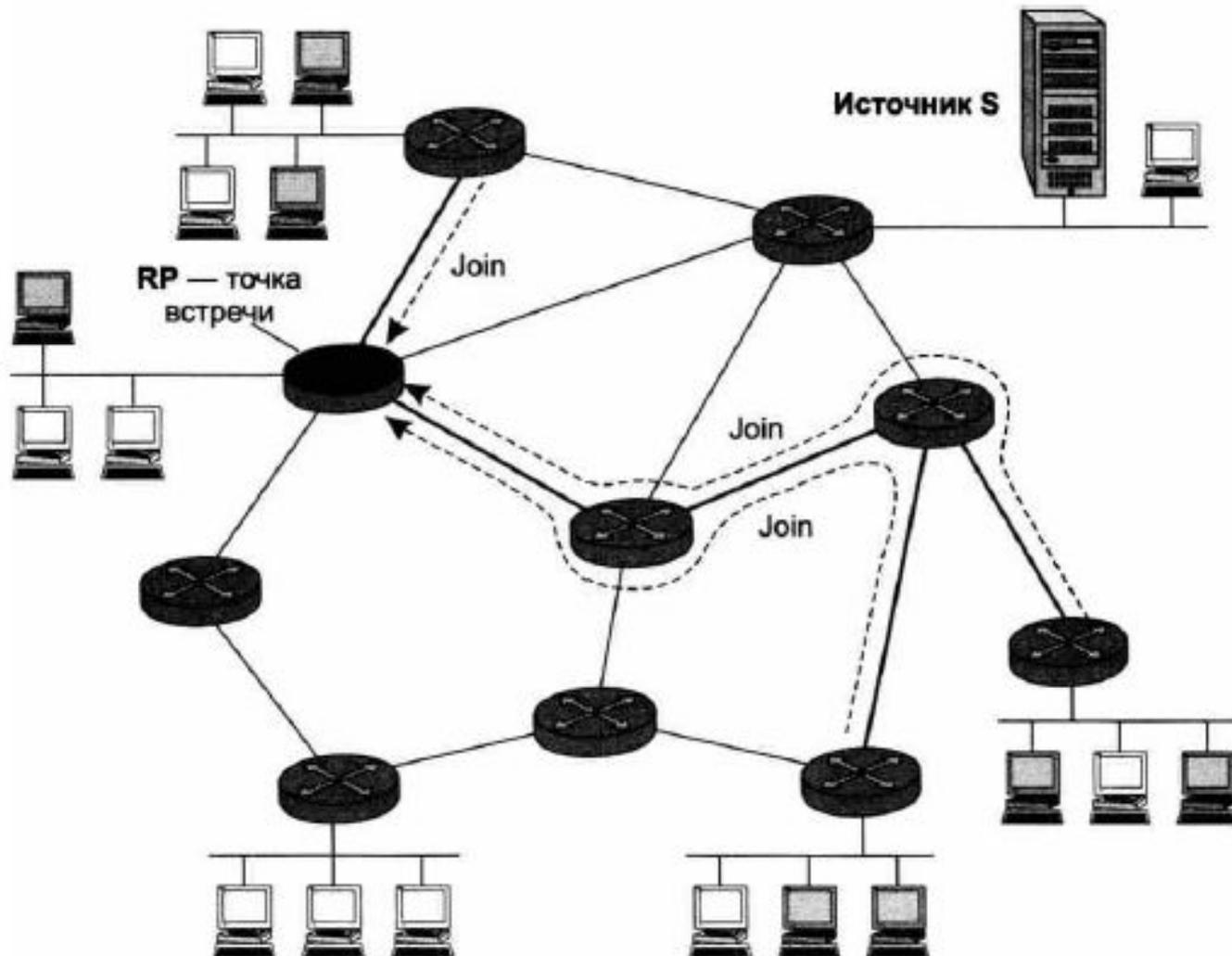


Рис. 17.11. Разделяемое дерево протокола PIM-SM

Вершина разделяемого дерева не может располагаться в источнике, так как источников может быть несколько. В качестве вершины разделяемого дерева используется специально выделенный для этой цели маршрутизатор, выполняющий функции точки встречи (RP). Все маршрутизаторы в пределах домена PIM-SM должны обладать согласованной информацией о расположении точки встречи. Различные группы могут иметь как одну и ту же, так и разные точки встречи.

Процесс доставки протоколом PIM-SM группового трафика от источника к получателям, принадлежащим некоторой группе, может быть представлен трехэтапным:

- построение разделяемого дерева с вершиной в точке встречи, которое описывает пути доставки групповых пакетов между точкой встречи и членами данной группы.
- построение дерева кратчайшего пути (Shortest Path Tree, SPT), которое будет доставлять пакеты между источником группы и точкой встречи;
- построение набора SPT-деревьев, которые ради повышения эффективности будут использованы для доставки пакетов между источником и каждым из получателей группы

# Поддержка QoS в маршрутизаторах

Были разработаны две системы стандартов QoS для IP-сетей:

- **система интегрированного обслуживания** (Integrated Services, IntServ) ориентирована на предоставление гарантий QoS для потоков конечных пользователей «из конца в конец»;
- **система дифференцированного обслуживания** (Differentiated Services, DiffServ) предоставляет гарантии QoS в агрегированной форме для классов трафика. Обе системы включают в себя все базовые элементы поддержки QoS:
  - кондиционирование трафика;
  - сигнализация, обеспечивающая координацию маршрутизаторов;
  - резервирование пропускной способности интерфейсов маршрутизаторов для потоков и классов;
  - приоритетные и взвешенные очереди.

# Система интегрированного обслуживания

Ресурсы маршрутизаторов (пропускная способность интерфейсов, размеры буферов) распределяются в соответствии с QoS-запросами приложений в пределах, разрешенных политикой QoS для данной сети. Эти запросы распространяются по сети сигнальным протоколом резервирования ресурсов (Resource Reservation Protocol, RSVP)

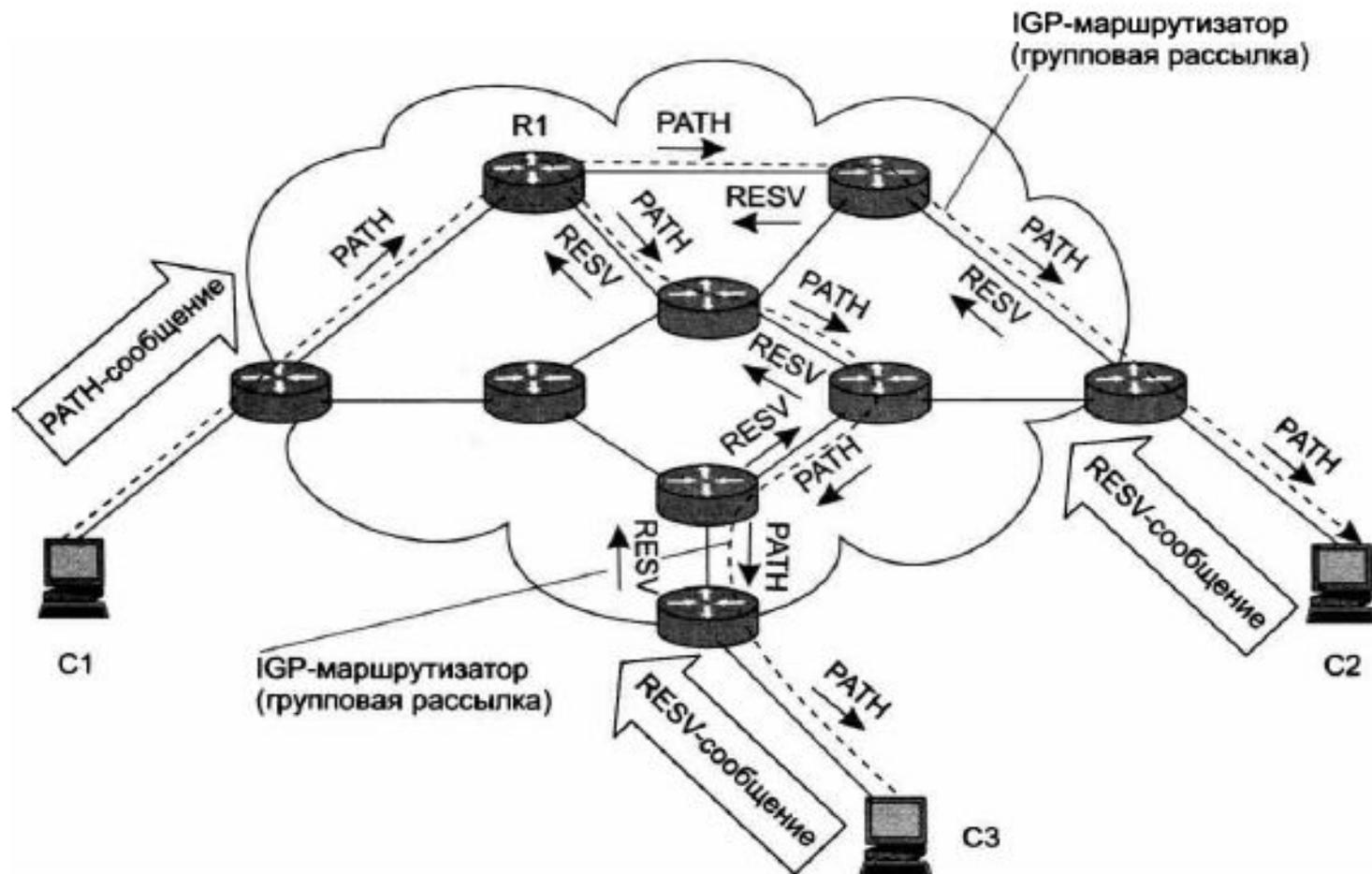


Рис. 17.12. Резервирование ресурсов по протоколу RSVP

## Система дифференцированного обслуживания

- Дифференцированное обслуживание (DiffServ) опирается на те же механизмы QoS, что и интегрированное обслуживание, однако в качестве объектов обслуживания рассматриваются не отдельные потоки, а классы трафика.
- Классом трафика называется совокупность поступающих на обработку пакетов, обладающих общими признаками, например все пакеты голосовых приложений или все пакеты с MTU в определенных пределах.
- Таким образом, в агрегированный поток некоторого класса входит некоторое (возможно большое) число под-агрегированных потоков.

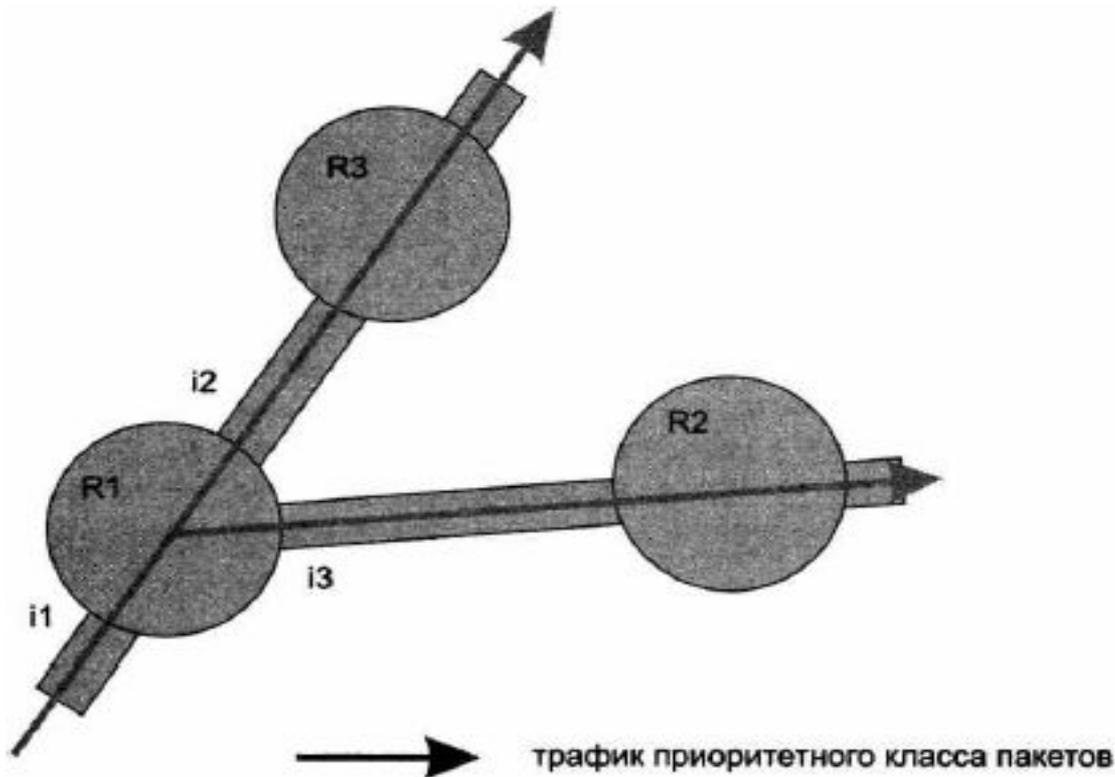


Рис. 17.13. Передача класса трафика маршрутизаторами





**Спасибо за внимание!**