Министерство образования и науки Российской Федерации

Колледж информационных технологий и экономики

КБГУ им. Бербекова

Специальность: программирование в компьютерных системах

09.02.03

РЕФЕРАТ

на тему:

Протокол маршрутизации IP

|  |  |
| --- | --- |
|  | **Выполнил:**  Студентка 3курса группы П-31  Кушхова Э. Х. |
|  | **Преподаватель**:  Оришев Х. Х. |
|  |  |

Нальчик, 2020

**Содержание**

[**Введение 3**](#_Toc41517124)

[**IP-пакет 5**](#_Toc41517125)

[**Принцип маршрутизации 10**](#_Toc41517126)

[**Примеры таблиц маршрутизации различных форматов 12**](#_Toc41517127)

[**Просмотр таблиц маршрутизации без масок 16**](#_Toc41517128)

[**Переход на версию IPv6 17**](#_Toc41517129)

[**Заключение 19**](#_Toc41517130)

[**Список использованной литературы 21**](#_Toc41517131)

# Введение

Протокол IP (Internet Protocol – межсетевой протокол) является главным протоколом семейства, он реализует распространение информации в IP-сети и выполняется на третьем (сетевом) уровне модели OSI. Протокол IP обеспечивает дейтаграммную доставку пакетов, его основная задача – маршрутизация пакетов. Он не отвечает за надежность доставки информации, за ее целостность, за сохранение порядка потока пакетов. Сети, в которых используется протокол IP, называются IP-сетями. Они работают в основном по аналоговым каналам (т. е. для подключения компьютера к сети требуется IP-модем) и являются сетями с коммутацией пакетов. Пакет здесь называется дейтаграммой.

Протокол IP является основным в иерархии протоколов TCP/IP и используется для управления рассылкой TCP/IP-пакетов по сети Internet. Среди различных функций, возложенных на IP, обычно выделяют следующие:

* определение пакета, который является базовым понятием и единицей передачи данных в сети Internet. Многие зарубежные авторы называют такой IP-пакет дейтаграммой;
* определение адресной схемы, которая используется в сети Internet;
* передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем (другими словами, преобразование транспортных дейтаграмм во фреймы канального уровня);
* маршрутизация пакетов по сети, т. е. передача пакетов от одного шлюза к другому с целью передачи пакета машине-получателю;
* фрагментация и дефрагментация пакетов транспортного уровня.

Главной особенностью протокола IP является отсутствие ориентации на физическое или виртуальное соединение. Это значит, что, прежде чем послать пакет в сеть, модуль операционной системы, реализующий IP, не проверяет возможность установки соединения, т. е. никакой управляющей информации, кроме той, что содержится в самом IP-пакете, по сети не передается. Кроме того, IP не заботится о проверке целостности информации в поле данных пакета, что заставляет отнести его к протоколам ненадежной доставки. Целостность данных проверяется протоколами транспортного уровня (TCP) или протоколами приложений.

Таким образом, вся информация о пути, по которому должен пройти пакет, определяется по состоянию сети в момент прохождения пакета. Эта процедура называется маршрутизацией в отличие от коммутации, используемой для предварительного установления маршрута следования отправляемых данных.

# IP-пакет

В каждой очередной сети, лежащей на пути перемещения пакета, протокол IP обращается к средствам транспортировки этой сети, чтобы с их помощью передать пакет на маршрутизатор, ведущий к следующей сети, или непосредственно на узел-получатель. Поддержание интерфейса с нижележащими технологиями подсетей является одной из важнейших функций протокола IP. В эти функции входит также поддержание интерфейса с протоколами вышележащего транспортного уровня, в частности с протоколом TCP, который решает все вопросы обеспечения надежной доставки данных по составной сети в стеке TCP/IP.

Протокол IP относится к протоколам без установления соединений, он поддерживает обработку каждого IP-пакета как независимой единицы обмена, не связанной с другими пакетами. В протоколе IP нет механизмов, обычно применяемых для обеспечения достоверности конечных данных. Если во время продвижения пакета происходит какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен из-за ошибки по контрольной сумме, то модуль IP не пытается заново послать потерянный пакет. Другими словами, протокол IP реализует политику доставки «по возможности».

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 бита  Номер  версии | 4 бита  Длина  заголовка | 8 бит  Тип сервиса | | | | | 16 бит  Общая длина | | | |
| PR | D | Т | R |  |
| 16 бит  Идентификатор пакета | | | | | | | 3 бита Флаги | | | 13 бит Смещение фрагмента |
|  | D | М |
| 8 бит  Время жизни | | 8 бит  Протокол верхнего уровня | | | | | 16 бит  Контрольная сумма | | | |
| 32 бита  IP-адрес источника | | | | | | | | | | |
| 32 бита  IP-адрес назначения | | | | | | | | | | |
| Параметры и выравнивание | | | | | | | | | | |

Таблица 1. Структура заголовка IP-пакета

Имеется прямая связь между количеством полей заголовка пакета и функциональной сложностью протокола, который работает с этим заголовком. Чем проще заголовок — тем проще соответствующий протокол. Большая часть действий протокола связана с обработкой той служебной информации, которая переносится в полях заголовка пакета. Изучая назначение каждого поля заголовка IP-пакета, мы не только получаем формальные знания о структуре пакета, но и знакомимся с основными функциями протокола IP. В таблице 1 показаны поля заголовка IР-пакета.

Поле номера версии занимает 4 бита и идентифицирует версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4), хотя все чаще встречается и новая версия (IPv6).

Значение длины заголовка IP-пакета также занимает 4 бита и измеряется в 32-битных словах. Обычно заголовок имеет длину в 20 байт (пять 32-битных слов), но при добавлении некоторой служебной информации это значение может быть увеличено за счет дополнительных байтов в поле параметров. Наибольшая длина заголовка составляет 60 байт.

Поле типа сервиса (Type of Service, ToS) имеет и другое, более современное название — байт дифференцированного обслуживания, или DS-байт. Этим двум названиям соответствуют два варианта интерпретации этого поля. В обоих случаях данное поле служит одной цели — хранению признаков, которые отражают требования к качеству обслуживания пакета. В прежнем варианте первые три бита содержат значение приоритета пакета: от самого низкого — 0 до самого высокого — 7. Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Следующие три бита поля ToS определяют критерий выбора маршрута. Если бит D (Delay — задержка) установлен в 1, то маршрут должен выбираться для минимизации задержки доставки данного пакета, установленный бит Т (Throughput — пропускная способность) — для максимизации пропускной способности, а бит R (Reliability — надежность) — для максимизации надежности доставки. Оставшиеся два бита имеют нулевое значение.

Стандарты дифференцированного обслуживания, принятые в конце 90-х годов, дали новое название этому полю и переопределили назначение его битов. В DS-байте также используются только старшие 6 бит, а два младших бита остаются в качестве резерва.

Поле общей длины занимает 2 байта и характеризует общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве компьютеров и сетей столь большие пакеты не используются. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной 1500 байт, умещающиеся в поле данных кадра Ethernet. В стандартах TCP/IP предусматривается, что все хосты должны быть готовы принимать пакеты длиной вплоть до 576 байт (независимо от того, приходят ли они целиком или фрагментами).

Идентификатор пакетазанимает 2 байта и используется для распознавания пакетов, образовавшихся путем деления на части (фрагментации) исходного пакета. Все части (фрагменты) одного пакета должны иметь одинаковое значение этого поля.

Флаги занимают 3 бита и содержат признаки, связанные с фрагментацией. Установленный в 1 бит DF (Do not Fragment — не фрагментировать) запрещает маршрутизатору фрагментировать данный пакет, а установленный в 1 бит MF (More Fragments — больше фрагментов) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле смещения фрагмента занимает 13 бит и задает смещение в байтах поля данных этого фрагмента относительно начала поля данных исходного (нефрагментированного) пакета. Используется при сборке/разборке фрагментов пакетов. Смещение должно быть кратно 8 байт.

Поле времени жизни (Time То Live, TTL) занимает один байт и используется для задания предельного срока, в течение которого пакет может перемещаться по сети. Время жизни пакета измеряется в секундах и задается источником. По истечении каждой секунды пребывания на каждом из маршрутизаторов, через которые проходит пакет во время своего «путешествия» по сети, из его текущего времени жизни вычитается единица; единица вычитается и в том случае, если время пребывания было меньше секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше чем за одну секунду, то время жизни можно интерпретировать как максимальное число транзитных узлов, которые разрешено пройти пакету. Если значение поля времени жизни становится нулевым до того, как пакет достигает получателя, пакет уничтожается. Таким образом, время жизни является своего рода часовым механизмом самоуничтожения пакета.

Поле протокола верхнего уровня занимает один байт и содержит идентификатор, указывающий, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета. Значения идентификаторов для разных протоколов приводятся в документе RFC 1700, доступном по адресу http://www.iana.org. Например, 6 означает, что в пакете находится сообщение протокола TCP, 17 — протокола UDP, 1 — протокола ICMP.

Контрольная сумма заголовка занимает 2 байта (16 бит) и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, поле времени жизни), контрольная сумма проверяется и повторно рассчитывается на каждом маршрутизаторе и конечном узле как дополнение к сумме всех 16-битных слов заголовка. При вычислении контрольной суммы значение самого поля контрольной суммы устанавливается в нуль. Если контрольная сумма неверна, то пакет отбрасывается, как только обнаруживается ошибка.

Поля IP-адресов источника и приемника имеют одинаковую длину — 32 бита.

Поле параметров является не обязательным и используется обычно только при отладке сети. Это поле состоит из нескольких подполей одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут, по которому маршрутизаторы должны направлять данный пакет (это называется маршрутизацией от источника), регистрировать проходимые пакетом маршрутизаторы или помещать данные системы безопасности и временные отметки. Так как число подполей в поле параметров может быть произвольным, то в конце заголовка должно быть добавлено несколько нулевых байтов для выравнивания заголовка пакета по 32-битной границе.

# Принцип маршрутизации

Принцип маршрутизации является одним из тех факторов, которые определяют гибкость сети Internet и ее преимущества по отношению к другим сетевым технологиям. Маршрутизация представляет собой ресурсоемкую процедуру, так как предполагает анализ каждого пакета, который проходит через шлюз или маршрутизатор, в то время как при коммутации анализируется только управляющая информация, устанавливается канал (физический или виртуальный), и все пакеты пересылаются по этому каналу без анализа маршрутной информации. Однако при неустойчивой работе сети пакеты могут пересылаться по различным маршрутам и затем собираться в единое сообщение. При коммутации путь придется устанавливать заново для каждого пакета, и при этом потребуется больше накладных затрат, чем при маршрутизации.

В сложных составных сетях почти всегда существуют несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании критерия выбора маршрута. В качестве критерия часто выступает задержка прохождения маршрута отдельным пакетом, средняя пропускная способность маршрута для последовательности пакетов или наиболее простой критерий, учитывающий только количество пройденных на маршруте промежуточных маршрутизаторов (ретрансляционных участков, или хостов). Полученная в результате анализа информация о маршрутах дальнейшего следования пакетов помещается в таблицу маршрутизации.

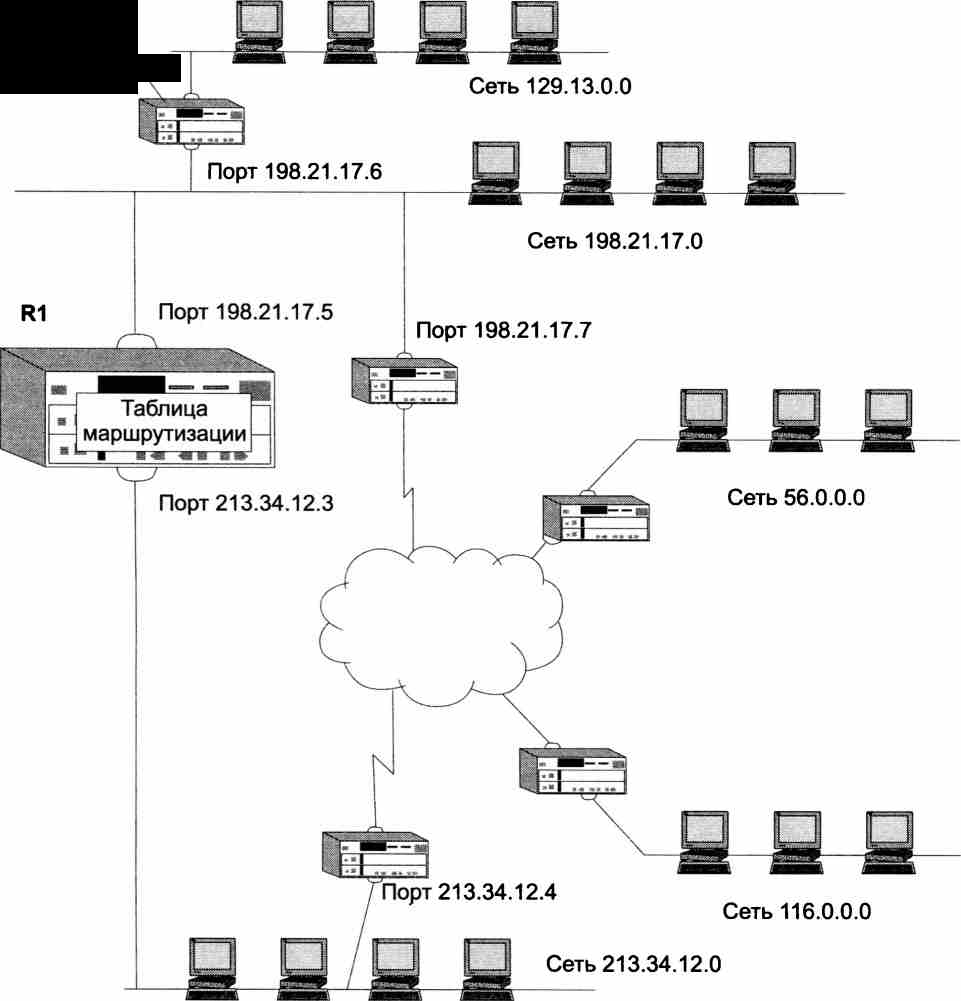
Задачу маршрутизации решают не только промежуточные узлы (маршрутизаторы), но и конечные узлы — компьютеры. Решение этой задачи начинается с того, что средствами протокола IP на конечном узле определяется, направлен ли пакет в другую сеть или адресован какому-нибудь узлу данной сети. Если номер сети назначения совпадает с номером данной сети, это означает, что пакет маршрутизировать не требуется. В противном случае маршрутизация нужна.

Структуры таблиц маршрутизации конечных узлов и транзитных маршрутизаторов аналогичны. Конечные узлы в еще большей степени, чем маршрутизаторы, пользуются приемом маршрутизации по умолчанию. Хотя они также в общем случае имеют в своем распоряжении таблицу маршрутизации, ее объем обычно незначителен, что объясняется периферийным расположением всех конечных узлов. Конечный узел часто вообще работает без таблицы маршрутизации, имея только сведения об адресе маршрутизатора по умолчанию. При наличии одного маршрутизатора в локальной сети этот вариант — единственно возможный для всех конечных узлов. Но даже при наличии нескольких маршрутизаторов в локальной сети, когда перед конечным узлом стоит проблема их выбора, часто в компьютерах для повышения производительности прибегают к заданию маршрута по умолчанию.

Еще одним отличием работы маршрутизатора и конечного узла является способ построения таблицы маршрутизации. Если маршрутизаторы, как правило, автоматически создают таблицы маршрутизации, обмениваясь служебной информацией, то для конечных узлов таблицы маршрутизации часто создаются вручную администраторами и хранятся в виде постоянных файлов на дисках.

# Примеры таблиц маршрутизации различных форматов

Вид таблицы IP- маршрутизации зависит от конкретной реализации стека TCP/IP. Приведем пример нескольких вариантов таблицы маршрутизации, с которыми мог бы работать маршрутизатор R1 в сети, представленной на рис. 1:



**Маршрутизаторы**

Начнем с «придуманного» предельно упрощенного варианта таблицы маршрутизации (табл. 2). Здесь имеются три маршрута к сетям (записи 56.0.0.0, 116.0.0.0 и 129.13.0.0), две записи о непосредственно подсоединенных сетях (198.21.17.0 и 213.34.12.0), а также запись о маршруте по умолчанию:

|  |  |  |  |
| --- | --- | --- | --- |
| **Адрес сети назначения** | **Адрес следующего маршрутизатора** | **Адрес выходного интерфейса** | **Расстояние до сети назначения** |
| 56.0.0.0 | 213.34.12.4 | 213.34.12.3 | 15 |
| 116.0.0.0 | 213.34.12.4 | 213.34.12.3 | 13 |
| 129.13.0.0 | 198.21.17.6 | 198.21.17.5 | 2 |
| 198.21.17.0 | 198.21.17.5 | 198.21.17.5 | 1 (подсоединена) |
| 213.34.12.0 | 213.34.12.3 | 213.34.12.3 | 1 (подсоединена) |
| Маршрут по умолчанию | 198.21.17.7 | 198.21.17.5 | -- |

Более сложный вид имеют таблицы, которые генерируются в промышленно выпускаемом сетевом оборудовании. Если представить, что в качестве маршрутизатора R1 в данной сети работает штатный программный маршрутизатор операционной системы Microsoft Windows, то его таблица маршрутизации могла бы выглядеть так, как табл. 2:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Сетевой адрес** | **Маска** | **Адрес шлюза** | **Интерфейс** | **Метрика** |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 0.0.0.0 | 0.0.0.0 | 198.21.17.7 | 198.21.17.5 | 1 |
| 56.0.0.0 | 255.0.0.0 | 213.34.12.4 | 213.34.12.3 | 15 |
| 116.0.0.0 | 255.0.0.0 | 213.34.12.4 | 213.34.12.3 | 13 |
| 129.13.0.0 | 255.255.0.0 | 198.21.17.6 | 198.21.17.5 | 2 |
| 198.21.17.0 | 255.255.255.0 | 198.21.17.5 | 198.21.17.5 | 1 |
| 198.21.17.5 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 198.21.17.255 | 255.255.255.255 | 198.21.17.5 | 198.21.17.5 | 1 |
| 213.34.12.0 | 255.255.255.0 | 213.34.12.3 | 213.34.12.3 | 1 |
| 213.34.12.3 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 213.34.12.255 | 255.255.255.255 | 213.34.12.3 | 213.34.12.3 | 1 |
| 224.0.0.0 | 224.0.0.0 | 198.21.17.6 | 198.21.17.6 | 1 |
| 224.0.0.0 | 224.0.0.0 | 213.34.12.3 | 213.34.12.3 | 1 |
| 255.255.255.255 | 255.255.255.255 | 198.21.17.6 | 198.21.17.6 | 1 |

Таблица маршрутизации для того же маршрутизатора R1, реализованного в виде программного маршрутизатора одной из версий ОС Unix – табл. 3:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Адрес**  **назначения** | **Шлюз** | **Флаги** | **Число**  **ссылок** | **Загрузка** | **Интерфейс** |
| 127.0.0.0 | 127.0.0.1 | UH | 1 | 154 | 1о0 |
| Маршрут по умолчанию | 198.21.17.7 | UG | 5 | 43270 | 1е0 |
| 198.21.17.0 | 198.21.17.5 | U | 35 | 246876 | 1е0 |
| 213.34.12.0 | 213.34.12.3 | U | 44 | 132435 | 1е1 |
| 129.13.0.0 | 198.21.1.7.6 | UG | 6 | 16450 | 1е0 |
| 56.0.0.0 | 213.34.12.4 | UG | 12 | 5764 | 1е1 |
| 116.0.0.0 | 213.34.12.4 | UG | 21 | 23544 | 1е1 |

Несмотря на достаточно заметные внешние различия, в «реальных» таблицах присутствуют все ключевые данные из рассмотренной упрощенной таблицы, без которых невозможна маршрутизация пакетов.

К таким данным, во-первых, относятся адреса сети назначения (столбцы «Адрес назначения» в аппаратном маршрутизаторе и маршрутизаторе Unix или столбец «Сетевой адрес» в маршрутизаторе ОС Windows).

Вторым обязательным полем таблицы маршрутизации является адрес следующего маршрутизатора (столбцы: «Шлюз» в маршрутизаторе ОС Unix или «Адрес шлюза» в маршрутизаторе ОС Windows).

Третий ключевой параметр — адрес порта, на который нужно направить пакет, в некоторых таблицах указывается прямо (столбец «Интерфейс» в таблице маршрутизатора ОС Windows), а в некоторых — косвенно. Так, в таблице маршрутизатора Unix вместо адреса порта задается его условное наименование — 1е0 для порта с адресом 198.21.17.5, le1 для порта с адресом 213.34.12.3 и 1о0 для внутреннего порта с адресом 127.0.0.1.

Стандартным решением сегодня является использование поля маски в каждой записи таблицы, как это сделано в таблице маршрутизатора ОС Windows (столбец «Маска»). Отсутствие поля маски говорит о том, что либо маршрутизатор рассчитан на работу только с тремя стандартными классами адресов, либо для всех записей используется одна и та же маска, что снижает гибкость маршрутизации.

Поскольку в таблице маршрутизации маршрутизатора Unix каждая сеть назначения упомянута только один раз, а значит, возможность выбора маршрута отсутствует, то поле метрики является не обязательным параметром. Для ОС Windows поле метрики используется только для указания на то, что сеть подключена непосредственно. Метрика 1 для маршрутизатора ОС Windows говорит маршрутизатору, что эта сеть непосредственно подключена к его порту, а другое значение метрики соответствует удаленной сети. Выбор метрики для непосредственно подключенной сети (1 или 0) является произвольным, главное, чтобы метрика удаленной сети отсчитывалась с учетом этого выбранного начального значения. В маршрутизаторе Unix используется поле признаков, где флаг G (Gateway — шлюз) отмечает удаленную сеть, а его отсутствие — непосредственно подключенную.

Признак непосредственно подключенной сети говорит маршрутизатору, что пакет уже достиг своей сети, поэтому протокол IP активизирует ARP-запрос относительно IP-адреса узла назначения, а не следующего маршрутизатора.

Флаги записей присутствуют только в таблице маршрутизатора Unix.

* U — маршрут активен и работоспособен. Аналогичный смысл имеет поле статуса в аппаратном маршрутизаторе.
* Н — признак специфического маршрута к определенному хосту.
* G — маршрут пакета проходит через промежуточный маршрутизатор (шлюз). Отсутствие этого флага отмечает непосредственно подключенную сеть.
* D — маршрут получен из перенаправленного сообщения протокола ICMP. Этот признак может присутствовать только в таблице маршрутизации конечного узла.

В таблице маршрутизатора Unix используются еще два поля, имеющих справочное значение. Поле числа ссылок показывает, сколько раз на данный маршрут ссылались при продвижении пакетов. Поле загрузки отражает количество байтов, переданных по данному маршруту.

# Просмотр таблиц маршрутизации без масок

1. Пусть на один из интерфейсов маршрутизатора поступает пакет. Протокол IP извлекает из пакета IP-адрес назначения.

2. Выполняется первая фаза просмотра таблицы — поиск конкретного маршрута к узлу. IP-адрес (целиком) последовательно строка за строкой сравнивается с содержимым поля адреса назначения таблицы маршрутизации. Если произошло совпадение, то из соответствующей строки извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса. На этом просмотр таблицы заканчивается.

3. Предположим теперь, что в таблице нет строки с адресом назначения, а значит, совпадения не произошло. В этом случае протокол IP переходит ко второй фазе просмотра — поиску маршрута к сети назначения. Из IP-адреса выделяется номер сети, и таблица снова просматривается на предмет совпадения номера сети в какой-либо строке с номером сети из пакета. При совпадении из соответствующей строки таблицы извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса. Просмотр таблицы на этом завершается.

4. Наконец, предположим, что адрес назначения в пакете был таков, что совпадения не произошло ни в первой, ни во второй фазе просмотра. В таком случае средствами протокола IP либо выбирается маршрут по умолчанию (и пакет направляется туда), либо, если маршрут по умолчанию отсутствует, пакет отбрасывается. Просмотр таблицы на этом заканчивается.

# Переход на версию IPv6

При разработке IPv6 была предусмотрена возможность плавного перехода к новой версии, когда довольно значительное время будут сосуществовать островки Интернета, работающие по протоколу IPv6, и остальная часть Интернета, работающая по протоколу IPv4. Существует несколько подходов к организации взаимодействия узлов, использующих разные стеки TCP/IP.

*Трансляция протоколов*. Трансляция протоколов реализуется шлюзами, которые устанавливаются на границах сетей, использующих разные версии протокола IP. Согласование двух версий протокола IP происходит путем преобразования пакетов IPv4 в IPv6 и наоборот. Процесс преобразования включает, в частности, отображение адресов сетей и узлов, различным образом трактуемых в этих протоколах. Для упрощения преобразования адресов между версиями разработчики IPv6 предлагают использовать специальные подтип IPv6- адреса — IРv4-совместимый IРv6-адрес, который в младших четырех байтах переносит IРv4-адрес, а в старших 12 байтах содержит нули. Это позволяет получать IРv4-адрес из IPv6-адреса простым отбрасыванием старших байтов.

*Мультиплексирование* стеков протоколов означает установку на взаимодействующих хостах сети обеих версий протокола IP. Обе версии стека протоколов должны быть развернуты также на разделяющих эти хосты маршрутизаторах. В том случае, когда IPv6-xocт отправляет сообщение 1Ру6-хосту, он использует стек IPv6, а если тот же хост взаимодействует с IPv4-xocтом — стек IPv4. Маршрутизатор с установленными на нем двумя стеками называется маршрутизатором IPv4/IPv6, он способен обрабатывать трафики разных версий независимо друг от друга.

*Инкапсуляция*, или *туннелирование*. Инкапсуляция — это еще один метод решения задачи согласования сетей, использующих разные версии протокола IP. Инкапсуляция может быть применена, когда две сети одной версии протокола, например IPv4, необходимо соединить через транзитную сеть, работающую по другой версии, например IPv6.

Переход от версии IPv4 к версии IPv6 уже идет «полным ходом». Например, по данным на 21 марта 2014 года, доступ по протоколу IPv6 к веб-сайтам Google в среднем получают 5 % пользователей. И хотя эти 5 % распределены по странам очень неравномерно — 32 % Бельгия, 16 % США, 14 % Германия,..., 0,56 % Россия, 0,34 % Великобритания, — качественная картина успешного продвижения версии IPv6 выглядит вполне убедительно.

# Заключение

Протокол IP решает задачу доставки сообщений между узлами составной сети. Поскольку он является дейтаграммным, никаких гарантий надежной доставки сообщений не дается.

Максимальная длина IP-пакета составляет 65 535 байт. Заголовок обычно имеет длину 20 байт и содержит информацию о сетевых адресах отправителя и получателя, параметры фрагментации, время жизни пакета, контрольную сумму и некоторые другие параметры.

Протокол IP в настоящее время столкнулся с рядом проблем, таких как проблема масштабируемости сети, неприспособленность протокола к передаче мультисервисной информации с поддержкой различных классов обслуживания, включая обеспечение информационной безопасности. Указанные проблемы обусловили развитие классической версии протокола IPv4 в направлении разработки версии IPv6. При этом к проблемам масштабируемости протокола IPv4 следует отнести следующие: недостаточность объема 32-битового адресного пространства; сложность агрегирования маршрутов, разрастание таблиц маршрутизации; сложность массового изменения IР-адресов; относительная сложность обработки заголовков пакетов IPv4.

Кроме того, масштабируемость IP-сетей следует рассматривать не только с точки зрения увеличения числа узлов, но и с точки зрения повышения скорости передачи и уменьшения задержек при маршрутизации.

IPv6 (Internet Protocol version 6) — это улучшенная версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Internet (разработан IETF). В настоящее время протокол IPv6 уже используется в нескольких сотнях сетей по всему миру, но пока еще не получил широкого распространения в Internet, где преимущественно используется IPv4.

Используя данные заголовка, машина может определить, на какой сетевой интерфейс отправлять пакет. Если IP-адрес получателя принадлежит одной из ее сетей, то на интерфейс этой сети пакет и будет отправлен, в противном случае пакет отправят на другой шлюз.

На основе протокола транспортного уровня IP-модуль производит экскапсуляцию информации из IP-пакета и ее передачу на модуль обслуживания соответствующего транспорта.

# Список использованной литературы

1. Максимов Н.В. Компьютерные сети: учебное пособие для студентов учреждений среднего профессионального образования / Н. В. Максимов, И. И. Попов. — 4-е изд., перераб-е и доп-е — М. : ФОРУМ, 2010. — 464 с.
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / Олифер В.Г., Олифер Н.А. — 5-е изд., СПб.: Питер, 2016. — 992 с.
3. Пятибратов А.П. Вычислительные машины, сети и телекоммуникационные системы: Учебно-методический комплекс / Пятибратов А.П., Гудыно Л.П. — М.: Изд. центр ЕАОИ. 2009. – 292 с.
4. В. Л. Бройдо. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. / В. Л. Бройдо. — СПб.: Питер, 2004. — 703 с.: ил.
5. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации: Учебник – 2-е изд. перераб. и доп. / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко; Под ред. А.П. Пятибратова – М.: Финансы и статистика, 2004 – 512 с.: ил.