ГЛАВА 3 Межсетевой уровень IP

Назначение данного уровня — маршрутизация пакетов при их пересылке между сетями сегментов канального уровня (и надстроенными над этими сегментами IP-сетями). Необходимость в этой функции вызвана тем, что, несмотря на все достоинства коммутируемых сетей Ethernet, размер сегментов Ethernet и других технологий канального уровня не может быть очень большим и тем более достигать масштабов всего интернета. Представьте вал широковещательных рассылок, связанных как с обучением коммутаторов, так и с работой протокола STP. Вспомните о соображениях информационной безопасности и необходимости выделения в отдельные сегменты подсетей подразделений с противоречивыми интересами. Подумайте о разнообразии технологий канального уровня. И вы окончательно поймете, почему интернет состоит из громадного множества сегментов канального уровня, связанных друг с другом через устройства межсетевого уровня — маршрутизаторы (router). Маршрутизаторы играют роль межсетевых шлюзов (gateway), определяющих направление дальнейшей пересылки входящих в них пакетов (к маршрутизатору обычно подключается более двух сегментов) с использованием специальных таблиц маршрутизации, создаваемых на каждом маршрутизаторе.

3.1. Система IP-адресации

Как ранее отмечалось, применимая на канальном уровне MAC-адресация не подходит для решения задач маршрутизации. Адрес, используемый для этих целей, должен содержать как минимум два поля, идентифицирующие подсеть адресата и самого адресата в этой подсети. Значение первого поля необходимо для определения каждым маршрутизатором направления (одного из нескольких возможных) пересылки IP-пакета адресату; значение второго поля — для доставки пакета конечному получателю.

В протоколе IP версии 4 (IPv4), который в настоящее время более распространен, чем протокол IP следующей версии IPv6, IP-адрес имеет длину 4 байта и при внешнем представлении записывается в виде четырех десятичных чисел в диапазоне [0, 255], разделенных символами «.». До 1981 года первый байт IP-адреса идентифицировал сеть, остальные 3 байта — компьютер этой сети. При таком разделении максимальное число различных сетей (256) быстро себя исчерпало — и были введены классы сетей, различающиеся своим размером. В 1991 году, когда этого оказалось недостаточно, была введена так называемая бесклассовая адресация.

Длящийся вот уже много лет переход к протоколу IP версии 6 позволит навсегда распрощаться с проблемой нехватки IP-адресов. Ведь адрес в IPv6 занимает целых 16 байт! В IPv6 количество различных сетей и компьютеров в них на многие порядки превышает число подключенных сегодня к интернету устройств.

3.1.1. IP-адреса и их классы в протоколе IPv4

При небольшой длине IP-адреса невозможно разбить его на два поля с фиксированной длиной таким образом, чтобы одновременно допускать существование хотя бы сотен тысяч различных подсетей с сотнями тысяч компьютеров в некоторых из них (для больших IP-сетей такая потребность актуальна). Поэтому для различения классов сетей в начале структуры IP-адреса создается третье поле: признак класса подсети. Длина этого поля различна для разных классов сетей. Структура внутреннего представления IP-адреса приведена на рис. 3.1. Более детальная информация о IP-адресах различных классов представлена в табл. 3.1.

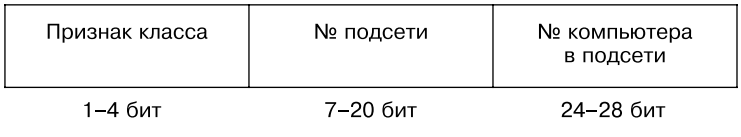

Рис. 3.1. Внутренняя структура IP-адреса

Таблица 3.1. Классы IP-адресов. Номера устройств, состоящие из всех нулей и всех единиц, зарезервированы. Подсеть 127 зарезервирована

Класс	Битовый признак класса	Диапазон значений первого байта	Длина поля № подсети (бит)	Количество подсетей	Длина поля № компьютера (байт)	Количество компьютеров в сети
A	0	0–127	7	2^7	3	$2^{32} - 2$
B	10	128–191	2	2^{14}	2	$2^{16} - 2$
C	100	192–223	3	2^{29}	1	254
D	1110	224–239	Номер группы			
F	1111	240–255	Служебный класс			

Отметим, что подсеть 127 зарезервирована. IP-адрес 127.0.0.1 (и любой другой IP-адрес, значение первого байта которого равно 127) на языке IP-адресации эквивалентен местоимению «я», то есть он адресует тот компьютер, на котором используется. Это очень удобно, например, для не требующей никакой настройки программы тестирования работы сетевых протоколов на локальном компьютере.

Все IP-адреса можно отнести к одному из трех типов: unicast (одноточечный), broadcast (широковещательный) и multicast (групповой). Все «обычные» IP-адреса указывают на конкретный компьютер и имеют тип unicast. Если в поле номера компьютера указано значение, все биты которого равны 1, то соответствующий IP-адрес считается широковещательным. Групповым является адрес класса D, он идентифицирует группы компьютеров, возможно, глобальные группы в интернете.

Отметим, что зарезервированное значение 0 в поле номера устройства подсети означает, что соответствующим IP-адресом идентифицируется вся подсеть. Адреса такого вида используются только в таблицах маршрутизации.

Далее в этой главе (кроме последнего раздела, посвященного протоколу IPv6) мы будем рассматривать только три класса «обычных» (не групповых и не служебных) IP-адресов: A, B и C.

При разработке протокола IPv4 его создатели полагали, что адресное пространство IP-сетей, предоставляемое тремя классами IP-адресов, является достаточным для более или менее отдаленного будущего. Однако в связи с постоянно возрастающим количеством подключенных к интернету подсетей (сетей различных организаций и подсетей в этих сетях) уже во второй половине 1980-х годов стало понятно, что необходимо более экономное использование адресного пространства IP-сетей. В итоге был создан метод бесклассовой адресации с помощью маски подсети и введены возможности широкого использования в подсетях специальных внутренних IP-адресов.

3.1.2. Бесклассовая адресация с использованием маски подсети

В целях экономного использования доступного адресного пространства зачастую требуется разбить подсеть некоторого класса на несколько сетей меньшего размера. Каждый физический сегмент должен быть оформлен как IP-подсеть, а компьютеров в сегменте может быть, например, менее десятка. В этом случае востребована возможность выделения такому маленькому подсегменту не всего адресного пространства подсети класса C (254 адресов сетевых устройств), а лишь части этой подсети, необходимой для адресации всех компьютеров сегмента. Еще в большей степени эта потребность разбиения подсети некоторого класса на несколько подсетей меньших размеров (не обязательно равных) актуальна для подсетей классов A и B.

Кроме того, для уменьшения размеров рассматриваемых ниже таблиц маршрутизации существует обратная потребность в объединении (агрегации) нескольких смежных сетей некоторого класса в одну общую сеть.

Обе эти задачи (разбиение на подсети и агрегация подсетей) решаются с использованием маски подсети. Маска подсети — это четырехбайтное значение, позволяющее

задать положение границы между полями номера сети и номера компьютера в IP-адресе с точностью до одного бита. Значение маски подсети — это последовательность битов 1, за которой следует последовательность нулевых битов. Количество единичных битов равно требуемой длине поля номера подсети (вместе с признаком подсети). Таким образом, если M — маска подсети, а A — IP-адрес, тогда $N_{\text{сети}} = A \,\&\, M$, а $N_{\text{комп}} = A \,\&\, (\text{not } M)$, где & — логическая операция «И», not — операция инверсии битов.

Отметим, что подсетям, подключенным к разным интерфейсам сетевого устройства, могут быть присвоены различные маски подсетей, соответствующие размерам подключаемых через эти интерфейсы сегментов. Подсети, получаемые в результате такого разбиения, могут иметь размеры, кратные степени двойки. При этом максимальное число компьютеров, которое может быть подключено к каждой из подсетей, на два меньше, чем соответствующая степень двойки.

При внешнем представлении маски подсети используют две формы ее записи. При начальной настройке компьютера, а также в командах конфигурирования интерфейсов (см. раздел 3.4) маска подсети задается в виде четырех десятичных чисел из диапазона [0, 255], разделенных точками (.). Приведем простое правило вычисления значения последнего байта задаваемой таким образом маски подсети. Пусть размер выделяемой подсети равен $N = 2^n$ ($n \le 7$). Тогда значением последнего байта маски (значения трех первых байтов совпадают с числом 255) будет $256 - N$.

В таблицах маршрутизации (для агрегации подсетей и соответствующего уменьшения строк этой таблицы) в большинстве операционных систем маска подсети задается вместе с адресом этой подсети в следующей форме: «IP-адрес подсети /N», где N — количество единичных битов в маске подсети. Это количество должно быть меньше, чем количество битов в поле номера подсети IP-адреса соответствующего класса. В системе Windows маска подсети в таблицах маршрутизации задается в форме записи IP-адреса. Более подробно об агрегации сетей в строках таблицы маршрутизации см. в подразделе 3.2.4.

В ходе использования маски подсети для разбиения сети на более мелкие подсети граница между полями IP-адреса с помощью маски как бы сдвигается вправо (единичные биты маски начинают заполнять слева часть поля номера компьютера). А при использовании маски для агрегации сетей граница между полями сдвигается влево (нулевые биты начинают заполнять справа часть поля номера сети).

3.1.3. Внутренние адреса и их использование

Еще один способ экономии применяемых IP-адресов связан с выделением в адресных пространствах IP-сетей классов A, B и C специальных диапазонов так называемых внутренних, или серых, IP-адресов. IP-адреса из этих диапазонов могут свободно использоваться внутри сети в любой из подключенных к интернету сетей

и тем самым значительно расширять размер доступного каждой из этих сетей адресного пространства. Но при этом указанные адреса не маршрутизируются через интернет: любой маршрутизатор интернета (то есть сети любого из операторов доступа к интернету) при обработке IP-пакета, содержащего в своем заголовке серые адреса, просто выбросит этот пакет. Именно поэтому внутри каждой из подключенных к интернету сетей эти адреса могут использоваться абсолютно свободно.

Однако если серые адреса не маршрутизируются в интернете, то каким образом компьютеры с такими адресами могут взаимодействовать с другими компьютерами и серверами интернета? Возможность такого взаимодействия обеспечивается специальным механизмом трансляции адресов NAT, функционирующим на пограничном маршрутизаторе сети, которая использует внутренние адреса. Подробнее об этом механизме см. в подразделе 3.5.2.

В завершение приведем три диапазона таких адресов. Для каждого диапазона укажем класс IP-адресов, начальный и конечный адреса и маску подсети:

- класс A, 10.0.0.0–10.255.255.255 /8;
- класс B, 172.16.0.0–172.31.255.255 /12;
- класс C, 192.168.0.0–192.168.255.255 /16.

3.2. Организация маршрутизации пакетов

В процессе маршрутизации и дальнейшей отправки IP-пакетов участвуют модули стека сетевых протоколов TCP/IP, представленные на рис. 3.2.

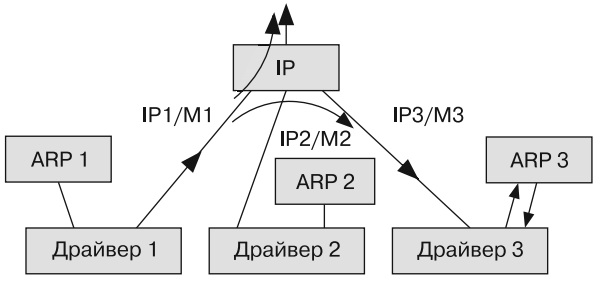

Рис. 3.2. Схема маршрутизации и отправки пакетов

Модуль IP выполняет маршрутизацию на основе заголовка принятого пакета, IP-адресов интерфейсов маршрутизатора и таблицы маршрутизации. Прежде чем описывать детали процесса маршрутизации, рассмотрим структуру заголовка IP-пакета и структуру таблицы маршрутизации.

3.2.1. Структура заголовка IP-пакета

Заголовок IP-пакета IPv4 имеет длину 20 байт и может иметь до десяти дополнительных четырехбайтных параметров (далее нами не рассматриваются). К числу основных полей заголовка IP-пакета относятся следующие:

- адрес получателя пакета (4 байта);
- адрес отправителя пакета (4 байта);
- длина пакета вместе с заголовком (2 байта). Допустима длина пакета от 20 до 65 535 ($2^{16} - 1$) байт;
- код протокола более высокого уровня, например TCP, UDP, ICMP, OSPF (1 байт);
- время жизни пакета (Time to Live, TTL) (1 байт). При прохождении пакетом каждого маршрутизатора значение этого поля уменьшается на 1 до тех пор, пока не станет равным 0. В последнем случае пакет выбрасывается, а его источнику направляется соответствующее сообщение протокола ICMP;
- байт TOS (Type of Service — тип обслуживания), к настоящему времени переименованный в DS-байт (или DSCP — DiffServ Code Point). Содержит параметры требуемого качества обслуживания пакета, в частности, трехбитовое поле приоритета пакета (precedence);
- параметры фрагментации пакета. Поскольку длина пакета может существенно превосходить MTU среды передачи, подключенной к интерфейсу, в который направляется IP-пакет, он перед передачей может разбиваться на пакеты-фрагменты длиной, не превосходящей MTU (то есть может фрагментироваться). Дефрагментация пакетов (сборка изначального пакета из фрагментов, на которые он был разбит) выполняется конечным получателем. Для обеспечения корректной дефрагментации в заголовке каждого пакета передаются три поля: двухбайтный идентификатор пакета (его значение совпадает для всех фрагментов одного исходного IP-пакета), флаги (4 бита) и смещение фрагмента (13 бит), задаваемое в блоках по 8 байт.

В качестве значения смещения последнего фрагмента можно указать такое, которое в сумме с длиной фрагмента превысит упомянутую выше максимальную длину пакета. В старых ОС в этом случае дефрагментированный пакет переполнял выделенный для приема пакетов буфер размером 65 535 байт и приводил ОС принявшего такой пакет компьютера или маршрутизатора в неработоспособное состояние. Поскольку максимальное смещение фрагмента имеет значение $(2^{16} - 1) \cdot 8 = 65\,528$, максимальная длина этого фрагмента не должна превышать $65\,535 - 65\,528 = 7$ байт. На базе рассмотренной уязвимости в середине 1990-х годов была придумана атака на отказ в обслуживании (DoS — Deny of Service), известная под названием «пинг смерти» (ping of the death). Для реализации этой атаки была выбрана команда (утилита) `ping`, поскольку она доставляет любому указанному узлу сети пакет эхо-

запроса протокола ICMP; при этом в качестве ключевого параметра `-l` команды `ping` может быть указана длина передаваемого пакета (точнее, ее превышение над минимальной длиной, равной 64). Поэтому команда вида:

```
ping -l 65510 IP-адрес-объекта-атаки
```

приведет объект атаки в неработоспособное состояние.

Способ борьбы с указанной уязвимостью состоит в предварительном подсчете длины дефрагментируемого пакета и его выбрасывании при превышении этой длиной значения 65 535. Данный способ был реализован практически во всех сетевых операционных системах уже в 1997–1998 годах. Поэтому рассмотренная уязвимость представляет лишь исторический интерес.

3.2.2. Таблица маршрутизации и способы ее создания и обновления

Решение о направлении дальнейшей пересылки пакета принимается модулем IP на основе информации, содержащейся в его таблице маршрутизации. Ее структура представлена в табл. 3.2.

Таблица 3.2. Структура таблицы маршрутизации

IP-адрес подсети/маска	Признак косвенной адресации	IP-адрес шлюза	Идентификатор интерфейса	Метрика (hops)
195.208.115.240/28	0	Игнорируется	/dev/eth0	0
195.208.115.192/24	1	195.208.115.8	/dev/eth1	1
default	1	195.208.115.5	/dev/eth2	1

Каждая строка таблицы маршрутизации соответствует описанию одного маршрута (маршрута к определенной подсети). В первом столбце (первом поле строки) заданы IP-адрес сети получателя и ее маска. Признак косвенной адресации указывает, входит ли подсеть в число сегментов, подключенных к текущему маршрутизатору (прямая адресация, признак равен 0), или доступна транзитом через другие маршрутизаторы (косвенная адресация, признак равен 1). Если задана косвенная маршрутизация, требуемая сеть доступна через указанный в третьем столбце транзитный маршрутизатор (называется межсетевым шлюзом (gateway)), подключенный к одному из сегментов маршрутизатора.

Доступ к требуемому сегменту осуществляется через интерфейс, идентификатор которого задается в четвертом поле строки таблицы. Если задана прямая адресация, получатель доступен путем широковещательной отправки IP-пакета через интерфейс, заданный в четвертом поле таблицы (при этом значение третьего поля

игнорируется). В системах UNIX идентификатором интерфейса является имя спецфайла интерфейса, содержащегося в каталоге `/dev`. И наконец, в последнем поле строки таблицы содержится расстояние до сети, адресуемой первым полем. Измеряется в количестве хопов (hop — «скачок»), то есть скачков через промежуточные маршрутизаторы, находящиеся на пути к адресату. Значение этого поля не используется в процессе маршрутизации, выполняемой модулем IP, а применяется протоколами управления маршрутизацией для автоматического динамического изменения таблицы маршрутизации при изменении состояния маршрутов к тем или иным подсетям.

Признак косвенной адресации может вычисляться через IP-адрес получателя и IP-адрес интерфейса шлюза (несовпадение подсетей в этих адресах), поэтому в некоторых реализациях IP этот признак в таблице маршрутизации явно не задается.

Очевидно, что в таблицу маршрутизации каждого шлюза невозможно занести строки, соответствующие абсолютно всем подсетям интернета. Да это и не требуется. Обычно все маршруты из текущей подсети во внешние по отношению к ней сети ведут через один и тот же межсетевой шлюз. Способ доступа к этому шлюзу описан в последней строке таблицы маршрутизации, в первом поле которой вместо адреса подсети указывается слово `default`, то есть вариант, принимаемый по умолчанию.

Создание и обновление строк таблицы маршрутизации может выполняться статически и динамически. Статически строки создаются сетевым администратором маршрутизатора с использованием соответствующей утилиты (команды оболочки ОС). В системах семейства UNIX для этой цели применяется команда `route`, имеющая следующий вид:

```
route {add | del} {IP-адрес/маска | default} [IP-адрес-шлюза ID-интерфейса
метрика]
```

В фигурных скобках заключены альтернативные значения, в квадратных — ненужные при удалении строки параметры (задается значением `del` первого параметра). Смысл параметров приведенной команды ясен без дальнейших комментариев. При использовании команды `route` без параметров она выводит на терминал (в стандартный выходной поток) таблицу маршрутизации локального компьютера.

Строки таблицы маршрутизации могут динамически обновляться протоколами управления маршрутизацией в зависимости от текущего состояния графа топологии сети. Благодаря этим протоколам сначала ARPANet, а затем и интернет может обеспечивать пути доступа к требуемым адресатам даже в «случае массового выхода из строя каналов передачи данных» (вспомните постановку задачи на создание ARPANet). Протоколам управления маршрутизацией посвящена следующая глава.

3.2.3. Алгоритм маршрутизации пакетов модулем IP

При поступлении входящего IP-пакета на один из интерфейсов маршрутизатора модуль IP после выполнения операций, связанных с проверкой корректности и возможной дефрагментацией IP-пакета, должен принять решение, в каком направлении этот пакет следует отправить дальше. Для этого модуль IP первым делом проверяет, не достиг ли IP-пакет конечной точки своего назначения, сравнивая указанный в заголовке IP-пакета адрес получателя с IP-адресами всех интерфейсов маршрутизатора (с учетом масок этих адресов). Положительный результат одного (и только одного) из сравнений свидетельствует о том, что конечная точка маршрута IP-пакета достигнута. Пакет передается вверх по стеку протокольных модулей в соответствии со значением поля «код протокола» заголовка IP-пакета, а работа модуля IP завершается.

Если IP-пакет еще не достиг пункта своего назначения, то в задачи модуля IP входит выполнение двух действий. Во-первых, он должен определить, в какой интерфейс, отличный от принявшего пакет интерфейса, следует направить пакет (IP-пакет никогда не отправляется в тот интерфейс, из которого был принят). Во-вторых, необходимо определить, какому сетевому устройству (компьютеру/маршрутизатору) из подключенного к этому интерфейсу сегмента должен быть направлен пакет, и осуществить отправку пакета.

Для принятия такого решения IP-модуль сопоставляет указанный в заголовке пакета адрес получателя со значением первого поля строк таблицы (при этом сопоставлении обязательно учитывается указанная в этом поле маска подсети), последовательно просматривая строки таблицы до тех пор, пока результат сопоставления не окажется успешным. Поскольку значение `default` успешно сопоставляется с любым IP-адресом, искомая строка обязательно будет найдена.

После нахождения строки таблицы маршрутизации, сопоставимой с IP-адресом получателя, модуль IP вначале проверяет, не совпадает ли значение поля «идентификатор интерфейса» выбранной строки таблицы с идентификатором интерфейса, принявшего IP-пакет. Факт такого совпадения свидетельствует о временном некорректном состоянии таблицы маршрутизации, вызванном незавершившимся ее перестроением после некоторого изменения доступности тех или иных каналов передачи данных. В этом случае обрабатываемый IP-пакет выбрасывается и модуль IP завершает работу. Повторную пересылку выброшенного пакета обеспечат протокольные модули более высокого уровня, работающие на компьютере — отправителе пакета.

Если значение `ID` идентификатора интерфейса, указанного в соответствующем поле выбранной строки таблицы, отличается от идентификатора интерфейса, принявшего обрабатываемый IP-пакет, то этот пакет следует отправить в интерфейс ID путем

обращения к его драйверу. Но при этом дополнительно требуется указать IP-адрес сетевого устройства, подключенного в сегмент интерфейса ID, которому следует адресовать передаваемый драйверу IP-пакет. Если в строке таблицы маршрутизации задана прямая адресация (значение признака косвенной адресации равно 0), то в качестве такого IP-адреса передается IP-адрес получателя из IP-пакета; в противном случае — IP-адрес шлюза из строки таблицы маршрутизации. Работа модуля IP по маршрутизации принятого пакета завершается обращением к драйверу выбранного сетевого интерфейса с передачей рассмотренных параметров.

3.2.4. Об агрегации строк таблицы маршрутизации

Поскольку при маршрутизации модулем IP каждого пакета последовательно просматриваются все строки таблицы маршрутизации (до сопоставления IP-адреса получателя с указанным в строке IP-адресом подсети), желательно по возможности сократить число строк таблицы для ускорения поиска, а следовательно, для уменьшения среднего времени, затрачиваемого модулем IP на маршрутизацию одного пакета, и повышения производительности маршрутизатора.

Основной способ уменьшения количества строк таблицы маршрутизации — агрегация идентичных (с точки зрения данного маршрутизатора) маршрутов (проходящих через один и тот же шлюз) и замена совокупности строк, описывающих такие маршруты одной агрегированной строкой. Приведем простые рекомендации по выявлению в таблице маршрутизации идентичных маршрутов и их агрегации. Пусть в таблице маршрутизации имеется N строк (где $N = 2^n$) с маской $/L_m$ и удовлетворяются следующие условия: в этих строках совпадают, во-первых, номера подсетей, вычисленные с использованием маски $/(L_m - n)$, во-вторых, IP-адрес шлюза и идентификатор интерфейса. Тогда эти N строк можно заменить одной агрегированной строкой с указанием в качестве IP-адреса подсети первых $L_m - n$ бит адреса любой из агрегируемых строк и с добавлением в конце этого адреса необходимого количества нулей.

В качестве маски этой подсети необходимо установить значение $L_m - n$. Эта маска будет короче масок всех агрегируемых сетей. Значениями полей IP-адреса шлюза и идентификатора интерфейса агрегированной записи станут совпадающие значения соответствующих полей агрегируемых строк.

Дополнительно отметим, что агрегацию строк таблицы маршрутизации можно выполнять в случае, когда одна или несколько (небольшое по сравнению с N число строк) из упомянутых N строк не удовлетворяют рассмотренному условию агрегации. В этой ситуации рекомендуется создать агрегированную строку, но разместить ее в таблице маршрутизации после строк исключения. В случае, когда адрес получателя IP-пакета будет принадлежать одной из подсетей, являющихся

исключениями из правила маршрутизации, определяемого агрегированной строкой, требуемая строка будет найдена модулем IP раньше агрегированной строки — и модуль IP прекратит дальнейший поиск.

Агрегирование подсетей выполняется каждым маршрутизатором полностью независимо от других маршрутизаторов. Поэтому в разных маршрутизаторах подсетям с одним и тем же адресом могут назначаться различные маски, задающие размер начинающегося с этого адреса блока агрегированных сетей. Так, например, таблица маршрутизации пограничного маршрутизатора сети ЮФУ содержит всего несколько агрегированных строк с масками от /24 (одна сеть класса C) до /21 (восемь сетей класса C). В маршрутизаторе сети RUNNet, к которому подключен упомянутый маршрутизатор сети ЮФУ, все подсети, соответствующие упомянутым строкам таблицы маршрутизатора ЮФУ, агрегируются в состав строки с маской /19 (32 сети класса C). При этом адрес подсети с маской /21 маршрутизатора ЮФУ совпадает с адресом второй половины (точнее, третьей четверти) подсети с маской /19 маршрутизатора RUNNet.

3.3. Протокол ARP

Когда модуль IP обращается к драйверу сетевого интерфейса для передачи IP-пакета в подключенный к этому интерфейсу сегмент сети, он передает драйверу в виде параметров указанный IP-пакет и IP-адрес получателя этого пакета в соответствующем сегменте. Этот адрес может быть адресом промежуточного шлюза и отличаться от конечного адреса получателя рассматриваемого IP-пакета. Но в любом случае к рассматриваемому сегменту подключен либо конечный получатель пакета, либо промежуточный шлюз (и драйверу предается IP-адрес сетевого устройства, заведомо находящегося в обслуживаемом этим драйвером сегменте). Для отправки по указанному IP-адресу полученный IP-пакет должен быть инкапсулирован в кадр соответствующей среды передачи с указанием в заголовке этого кадра MAC-адреса его получателя. Возникает задача преобразования IP-адреса сетевого устройства в его MAC-адрес.

Эта задача решается драйвером сетевого интерфейса средствами протокола ARP (Address Resolution Protocol — протокол преобразования адресов) путем обращения к модулю ARP своего интерфейса (каждый интерфейс имеет свой ARP-модуль), передавая ему в качестве параметра IP-адрес и получая в ответ соответствующий MAC-адрес. Модуль ARP решает эту задачу с использованием своей ARP-таблицы, каждая строка которой содержит два поля: IP-адрес и соответствующий ему MAC-адрес. После начальной активации интерфейса эта таблица пуста и заполняется в процессе обработки обращений драйвера к модулю ARP.

Модуль ARP обрабатывает обращение драйвера следующим образом. Вначале он выполняет поиск строки, в которой значение поля IP-адреса совпадает со значением