Протокол межсетевого взаимодействия. IP-пакет

Протокол IP относится к протоколам без установления соединений. Если во время продвижения пакета происходит какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки - протокол IP реализует политику доставки «по возможности».

- **Поле номера версии** занимает 4 бита и идентифицирует версию протокола IP.
- **Значение длины заголовка** IP-пакета также занимает 4 бита и измеряется в 32-битных словах. Наибольшая длина заголовка составляет 60 байт.
- **Поле типа сервиса (Type of Service, ToS) — байт дифференцированного обслуживания, или DS-байт.** Данное поле служит **хранению пр ивания па**

Рис. 15.1. Структура заголовка IP-пакета

- Следующие три бита поля ToS **определяют критерий выбора маршрута**. Если бит D (Delay) установлен в 1, то маршрут должен выбираться для минимизации задержки доставки данного пакета, установленный бит T— для максимизации пропускной способности, а бит R— для максимизации надежности доставки.
- **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.
- **Идентификатор пакета** занимает 2 байта и используется для распознавания пакетов, образовавшихся путем деления на части (фрагментации) исходного пакета.

- **Флаги** занимают 3 бита и содержат признаки, связанные с фрагментацией. Установленный в 1 бит DF запрещает маршрутизатору фрагментировать данный пакет, а установленный в 1 бит MF 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.
- **Поле времени жизни (Time To Live, TTL)** занимает один байт и используется для задания предельного срока, в течение которого пакет может перемещаться по сети. Если значение поля времени жизни становится нулевым до того, как пакет достигает получателя, пакет уничтожается.

- **Поле протокола верхнего уровня** занимает один байт и содержит идентификатор, указывающий, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета.
- **Контрольная сумма** заголовка занимает 2 байта и рассчитывается только по заголовку. Контрольная сумма проверяется и повторно рассчитывается на каждом маршрутизаторе и конечном узле как дополнение к сумме всех 16-битных слов заголовка. Если контрольная сумма неверна, то пакет отбрасывается, как только обнаруживается ошибка.
- **Поля IP-адресов** источника и приемника имеют одинаковую длину — 32 бита.
- **Поле параметров** используется только при

- IP: Version = 4 (0x4)
- IP: Header Length = 20 (0x14)
- IP: Service Type = 0 (0x0)
- IP: Precedence = Routine
- IP: ...0 = Normal Delay
- IP: 0... = Normal Throughput
- IP: 0.. = Normal Reliability
- IP: Total Length = 54 (0x36)
- IP: Identification = 31746 (0x7C02) IP: Flags Summary = 2 (0x2)
- IP: 0 = Last fragment in datagram
- IP: 1. = Cannot fragment datagram
- IP: Fragment Offset = 0 (0x0) bytes IP: Time to Live = 128 (0x80) IP: Protocol = TCP - Transmission Control
- IP: Checksum = 0xEB86
- IP: Source Address = 194.85.135.75
- IP: Destination Address = 194.85.135.66
- IP: Data: Number of data bytes remaining = 34 (0x0022)

Схема IP-маршрутизации

На каждом маршрутизаторе и конечных узлах функционируют протоколы IP.
К нескольким интерфейсам (портам) маршрутизаторов присоединяются сети.
Каждый **интерфейс маршрутизатора можно рассматривать как отдельный узел сети**: он имеет сетевой адрес и локальный адрес в той подсети, которая к нему подключена. Таким образом, **маршрутизатор можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть**. Как единое устройство **маршрутизатор не имеет выделенного адреса**, ни сетевого, ни

Таблица маршрутизации маршрутизатора 4

Номер сети	Следующий маршрутизатор	Входной интерфейс	Число хопов
N1	IP_{12}	IP_{41}	1
N2	—	IP_{41}	0
N3	IP_{12}	IP_{41}	1
N4	IP_{21}	IP_{41}	1
N5	—	IP_{42}	0
N6	IP_{21}	IP_{41}	2
IP_B	IP_{21}	IP_{41}	2
По умолчанию	IP_{51}	IP_{42}	—

Таблица маршрутизации узла B

Номер сети	Следующий маршрутизатор	Входной интерфейс	Число хопов
N1	IP_{13}	IP_B	1
N2	IP_{13}	IP_B	1
N3	—	IP_B	0
N4	IP_{31}	IP_B	1
N5	IP_{13}	IP_B	2
N6	IP_{31}	IP_B	2
По умолчанию	IP_{31}	IP_B	—

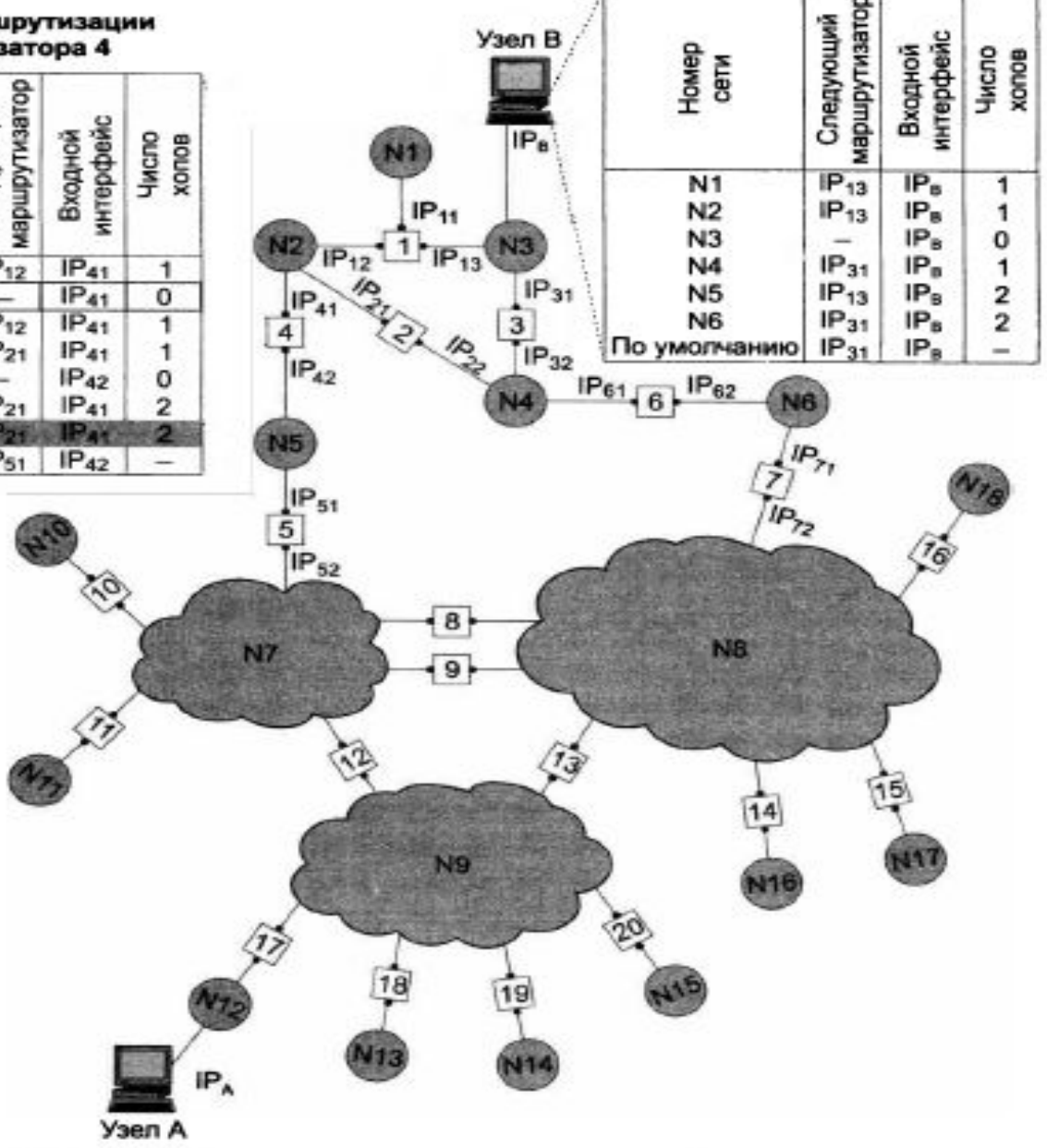


Рис. 15.2. Принципы маршрутизации в составной сети

При наличии у маршрутизатора **блока управления** этот блок имеет собственные локальный и сетевой адреса, по которым к нему обращается центральная станция управления. В технической документации такого рода адреса называются **адресами обратной петли (looopback address), или адресами виртуальных интерфейсов (virtual interface address).**В сложных составных сетях существуют несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами.

Упрощенная таблица маршрутизации

Первый столбец таблицы содержит **адреса назначения пакетов**.

В каждой строке таблицы следом за адресом назначения указывается сетевой адрес следующего маршрутизатора, на который надо направить пакет, чтобы тот передвигался по направлению к заданному адресу по рациональному маршруту.

Перед тем как передать пакет следующему маршрутизатору, текущий маршрутизатор должен определить, на какой из нескольких собственных портов (IP41 или IP42) он должен поместить данный пакет. Для этого служит третий столбец таб
вы

Таблица 15.1. Таблица маршрутизации маршрутизатора 4

Адрес назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
N1	IP_{12} (R1)	IP41	1
N2	–	IP41	0 (подсоединена)
N3	IP_{12} (R1)	IP41	1
N4	IP_{21} (R2)	IP41	1
N5	–	IP42	0 (подсоединена)
N6	IP_{21} (R2)	IP21	2
IP_8	IP_{21} (R2)	IP41	2
Маршрут по умолчанию	IP_{51} (R5)	IP42	–

Когда пакет поступает на маршрутизатор, модуль IP извлекает из его заголовка номер сети назначения и последовательно сравнивает его с номерами сетей из каждой строки таблицы. **Строка с совпавшим номером сети показывает ближайший маршрутизатор, на который следует направить пакет**.

Чаще всего в качестве адреса назначения в таблице указывается не весь IP-адрес, а только номер сети назначения. Однако в некоторых случаях в таблицу маршрутизации помещают для данного узла отдельную строку, содержащую его полный IP-адрес и соответствующую маршрутную информацию.

В случае крупной сети объем таблиц маршрутизации может оказаться очень большим, что повлияет на время ее просмотра, потребует много места для хранения и т.п. Поэтому на практике широко известен **прием уменьшения количества записей в таблице маршрутизации, основанный на введении маршрута по умолчанию (default route),** учитывающего особенности топологии сети. **Маршрутизатор, через который пролегает путь ко всем сетям называется маршрутизатором по умолчанию (default router).** Для всех пакетов, адресованных в сети N7-N18, маршрутизатор предлагает продолжить путь через один и тот же порт IP51 маршрутизатора 5, который в данном случае и является маршрутизатором по умолчанию.

Таблицы маршрутизации конечных узлов

Задачу маршрутизации решают не только промежуточные узлы (маршрутизаторы), но и конечные узлы — компьютеры.

Структуры таблиц маршрутизации конечных узлов и транзитных маршрутизаторов аналогичны. Таблица маршрутизации конечного узла B, принадлежащего сети N3, могла бы выглядеть так, как табл. 15.2.

Таблица 15.2. Таблица маршрутизации конечного узла B

Номер сети назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
N1	IP_{13} (R1)	IP_B	1
N2	IP_{13} (R1)	IP_B	1
N3	–	IP_B	0
N4	IP_{31} (R3)	IP_B	1
N5	IP_{13} (R1)	IP_B	2
N6	IP_{31} (R3)	IP_B	2
Маршрут по умолчанию	IP_{31} (R3)	IP_B	–

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.

Рассмотрим таблицу маршрутизации другого конечного узла составной сети — узла А (табл. 15.3). Все пакеты, направляемые из узла А, либо не выходят за пределы сети N12, либо непременно проходят через порт 1 маршрутизатора 17. Этот маршрутизатор и определен в таблице

Таблица 15.3. Таблица маршрутизации конечного узла А

Номер сети назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
N12	–	IPA	0
Маршрут по умолчанию	$IP_{17.1}$ (R17)	IPA	–

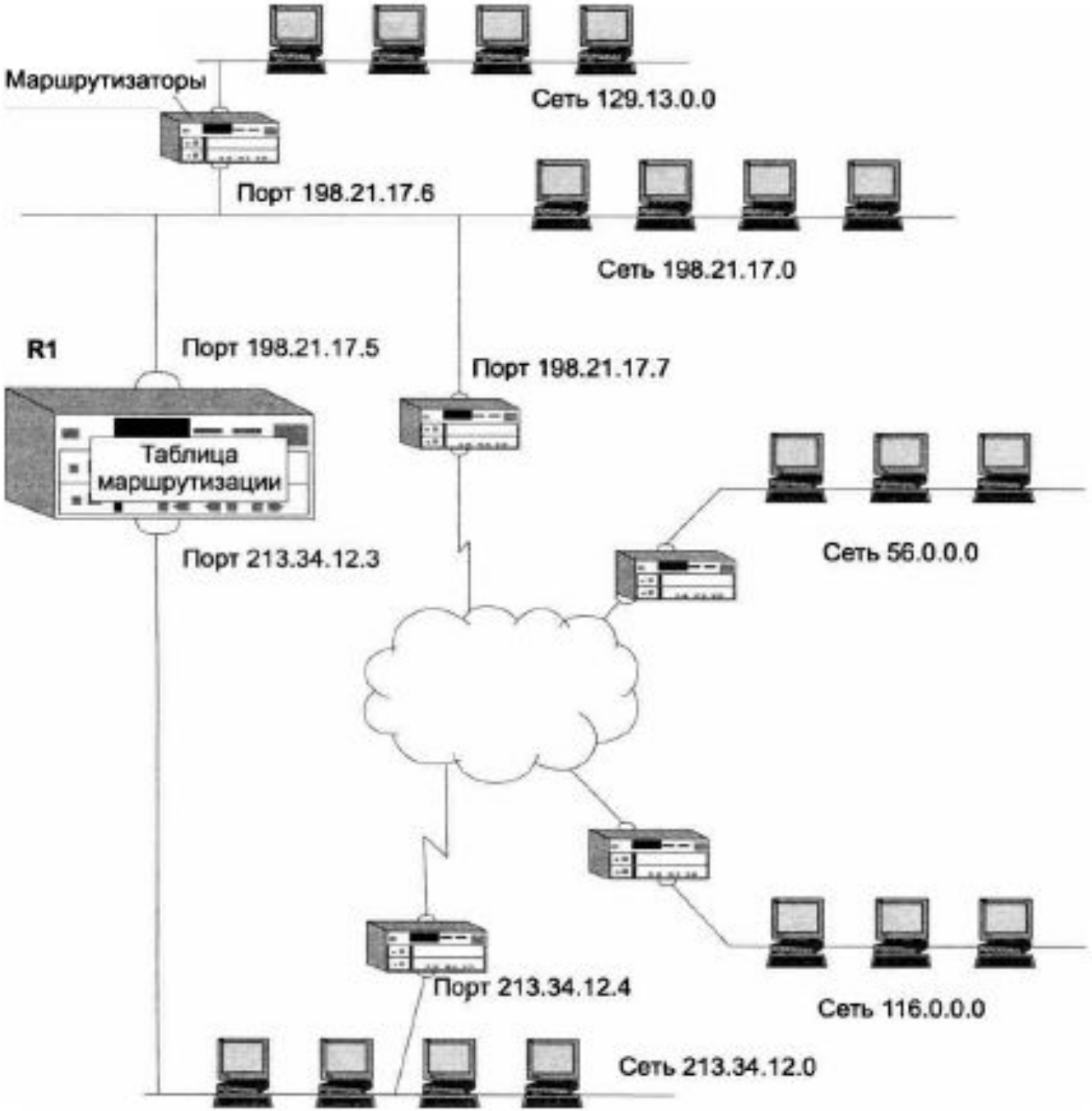


Рис. 15.3. Пример маршрутизируемой сети

Начнем с «придуманного» предельно упрощенного варианта таблицы маршрутизации (табл. 15.4). 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 ма

Таблица 15.4. Упрощенная таблица маршрутизации маршрутизатора R1

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.

Таблица 15.5. Таблица программного маршрутизатора ОС Windows

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

Если на месте маршрутизатора R1 установить один из популярных *аппаратных* маршрутизаторов, то его таблица маршрутизации для этой же сети может выглядеть совсем иначе (табл. 15.6).

Если на месте маршрутизатора R1 установить один из популярных аппаратных маршрутизаторов, то его таблица маршрутизации для этой же сети может выглядеть совсем иначе (табл. 15.6).

Таблица 15.6. Таблица маршрутизации аппаратного маршрутизатора

Адрес назначения	Маска	Шлюз	Метрика	Статус	TTL	Источник
198.21.17.0	255.255.255.0	198.21.17.5	0	Up	–	Подключена
213.34.12.0	255.255.255.0	213.34.12.3	0	Up	–	Подключена
56.0.0.0	255.0.0.0	213.34.12.4	14	Up	–	Статическая
116.0.0.0	255.0.0.0	213.34.12.4	12	Up	–	Статическая
129.13.0.0	255.255.0.0	198.21.17.6	1	Up	160	RIP

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

- Первым из них являются **адреса сети назначения.**
- Вторым обязательным полем таблицы маршрутизации является **адрес следующего маршрутизатора**.
- Третий ключевой параметр — **адрес порта**, на который нужно направить пакет, в некоторых таблицах указывается прямо, а в некоторых — косвенно.

Стандартным решением сегодня является **использование поля маски** в каждой записи таблицы, как это сделано в таблицах маршрутизатора ОС Windows и аппаратного маршрутизатора (столбцы «Маска»).

Метрика 0 для аппаратного маршрутизатора или 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

Источники и типы записей в таблице маршрутизации

Практически для всех маршрутизаторов существуют три основных источника записей в таблице.

Одним из источников записей в таблице маршрутизации является **программное обеспечение стека TCP/IP, которое при инициализации маршрутизатора автоматически заносит в таблицу несколько записей**, в результате чего создается так называемая **минимальная таблица маршрутизации**.

Еще одним источником записей в таблице является **администратор, непосредственно формирующий записи с помощью некоторой системной утилиты, например программы route**, доступной в операционных системах Unix и Windows. Заданные вручную записи всегда являются статическими, то есть они не имеют срока жизни.

И наконец, третьим источником записей могут быть **протоколы маршрутизации, такие как RIP или OSPF.** Эти записи всегда являются ди
ср

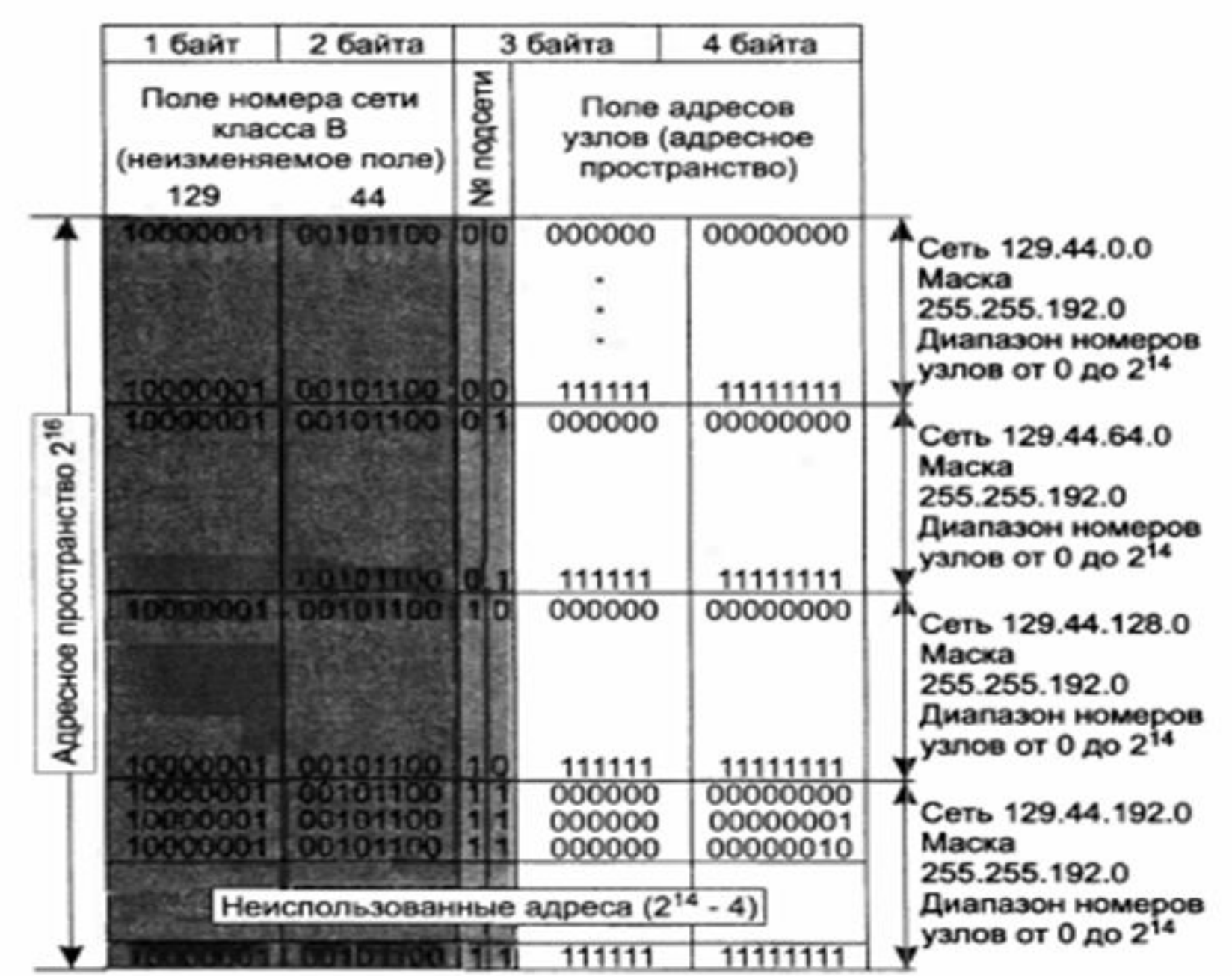
Таблица 15.6. Таблица маршрутизации аппаратного маршрутизатора

Адрес назначения	Маска	Шлюз	Метрика	Статус	TTL	Источник
198.21.17.0	255.255.255.0	198.21.17.5	0	Up	–	Подключена
213.34.12.0	255.255.255.0	213.34.12.3	0	Up	–	Подключена
56.0.0.0	255.0.0.0	213.34.12.4	14	Up	–	Статическая
116.0.0.0	255.0.0.0	213.34.12.4	12	Up	–	Статическая
129.13.0.0	255.255.0.0	198.21.17.6	1	Up	160	RIP

Маршрутизация с использованием масок

Алгоритм маршрутизации усложняется, когда в систему адресации узлов вносятся дополнительные элементы — **маски**. Часто администраторы сетей испытывают неудобства, поскольку количества номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом. В такой ситуации возможны два пути. Первый из них связан с **получением** от какого-либо центрального органа **дополнительных номеров сетей**. Второй способ **связан с использованием технологии масок**, которая позволяет разделить одну имеющуюся сеть на несколько.

На рис. 15.11 показано разделение всего адресного диапазона на четыре равные части — каждая по 2^14 адресов.



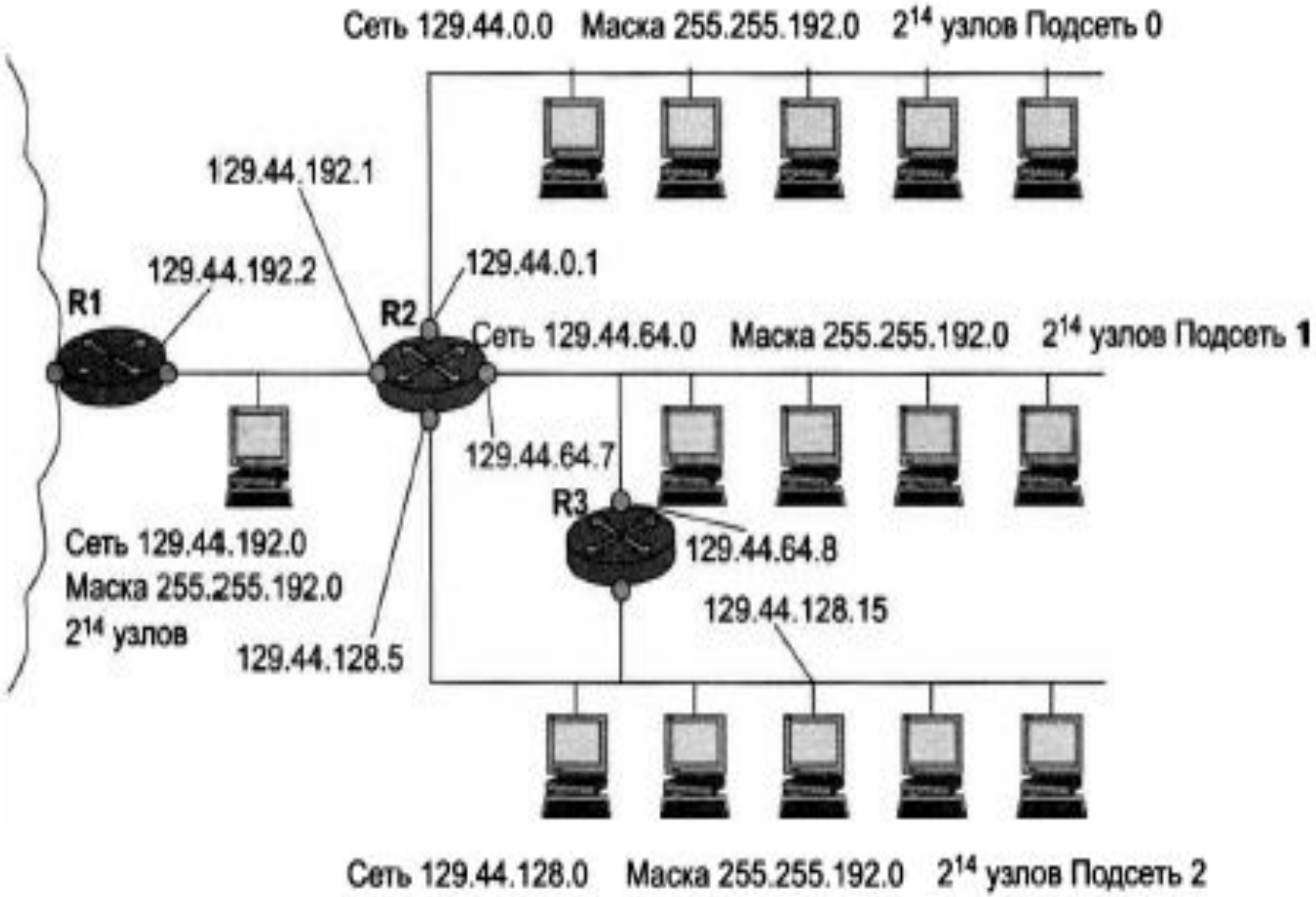


Рис. 15.12. Маршрутизация с использованием масок одинаковой длины

Пример сети, построенной путем деления на четыре сети равного размера, показан на рис. 15.12. Весь трафик во внутреннюю сеть 129.44.0.0, направляемый из внешней сети, поступает через маршрутизатор R1. В целях структуризации информационных потоков во внутренней сети установлен дополнительный маршрутизатор R2. Каждая из новых сетей 129.44.0.0/18, 129.44.64.0/18, 129.44.128.0/18 и 129.44.192.0/18 подключена к соответственно сконфигурированным портам внутреннего маршрутизатора R2.

Поступающий в сеть общий трафик разделяется локальным маршрутизатором R2 между четырьмя сетями.

Первые четыре записи в таблице соответствуют внутренним подсетям, непосредственно подключенным к портам маршрутизатора R2.

Запись 0.0.0.0 с маской 0.0.0.0 соответствует маршруту по умолчанию.

Последняя запись определяет специфический маршрут к узлу 129.44.128.15.

Таблица 15.8. Таблица маршрутизатора R2 в сети с масками одинаковой длины

Адрес назначения	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.192.0	129.44.0.1	129.44.0.1	Подключена
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–
129.44.128.15	255.255.255.255	129.44.64.8	129.44.64.7	–

Использование масок переменной длины

Во многих случаях более эффективным является разбиение сети на подсети разного размера.

На рис.15.13 половина из имеющихся адресов (215) отведена для создания *сети 1, имеющей адрес 129.44.0.0 и маску 255.255.128.0.* Далее в пространстве адресов был «вырезан» небольшой фрагмент для создания вспомогательной сети 3, предназначенной для связывания внутреннего маршрутизатора R2 с внешним маршрутизатором R1. Для нумерации узлов в такой вырожденной сети достаточно отвести

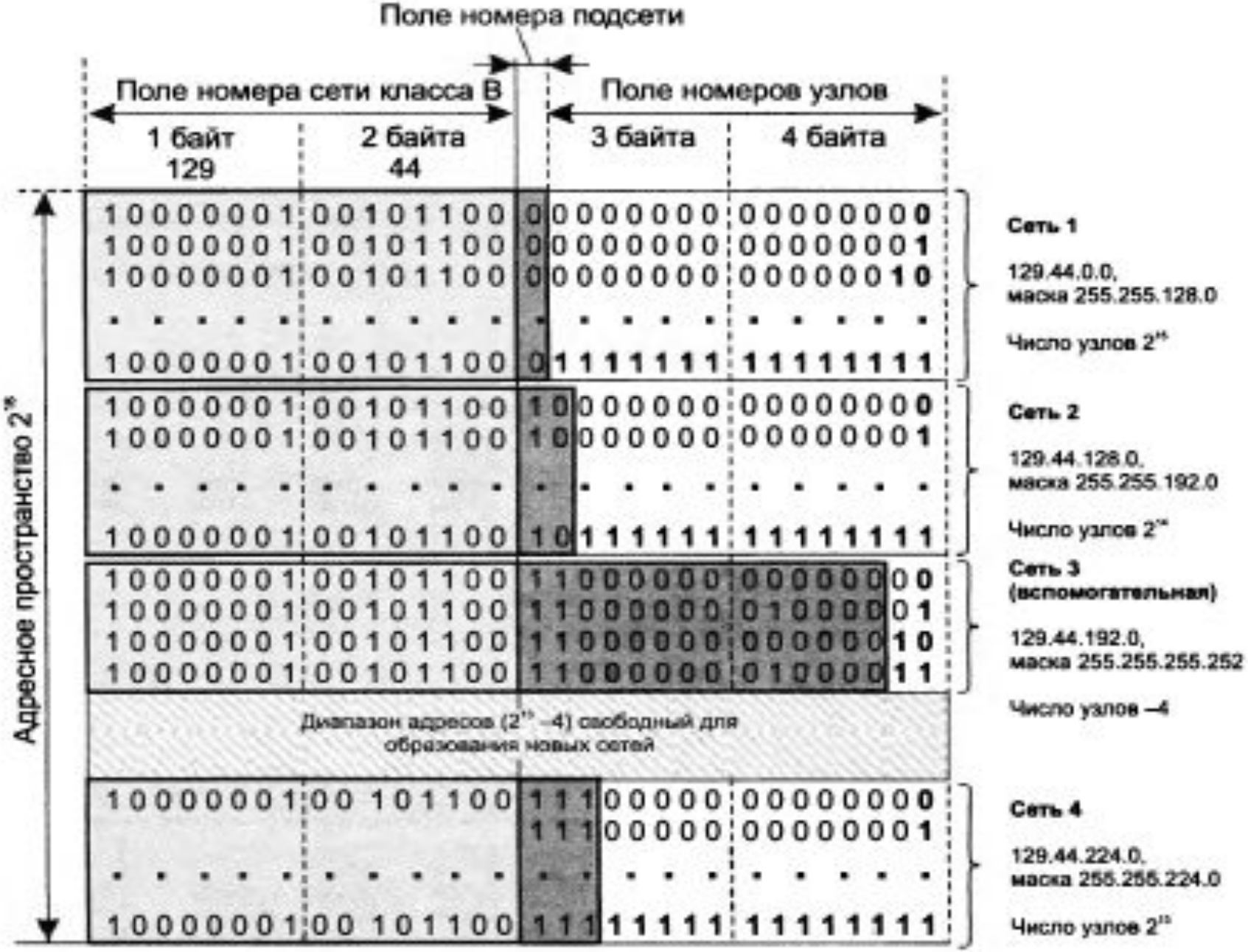


Рис. 15.13. Разделение адресного пространства 129.44.0.0 сети класса B на сети разного размера путем использования масок переменной длины

Оставшееся адресное пространство администратор может нарезать на разное количество сетей разного объема в зависимости от своих потребностей. Из оставшегося пула адресов администратор, например, может образовать еще одну достаточно большую сеть с числом узлов — на рисунке это сеть 4.

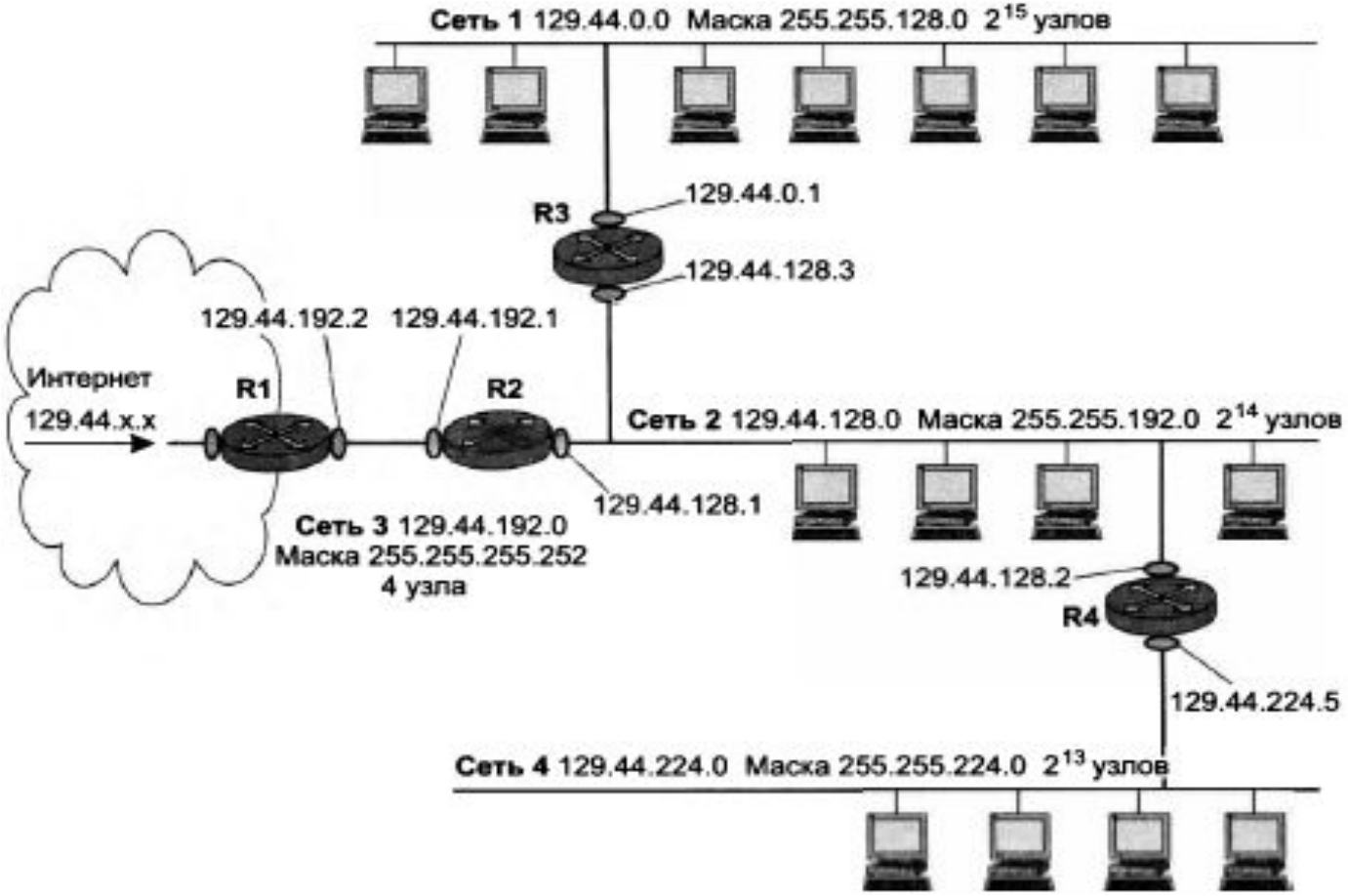


Рис. 15.14. Структуризация сети масками переменной длины

Таблица 15.9. Таблица маршрутизатора R2 в сети с масками переменной длины

Адрес назначения	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.128.0	129.44.128.3	129.44.128.1	1
129.44.128.0	255.255.192.0	129.44.128.1	129.44.128.1	Подключена
129.44.192.0	255.255.255.248	129.44.192.1	129.44.192.1	Подключена
129.44.224.0	255.255.224.0	129.44.128.2	129.44.128.1	1
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	–

Таблица 15.10. Фрагмент таблицы маршрутизатора R1

Адрес назначения	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.0.0	129.44.192.1	129.44.191.2	2
129.44.192.0	255.255.255.192	129.44.192.2	129.44.192.2	Подключена

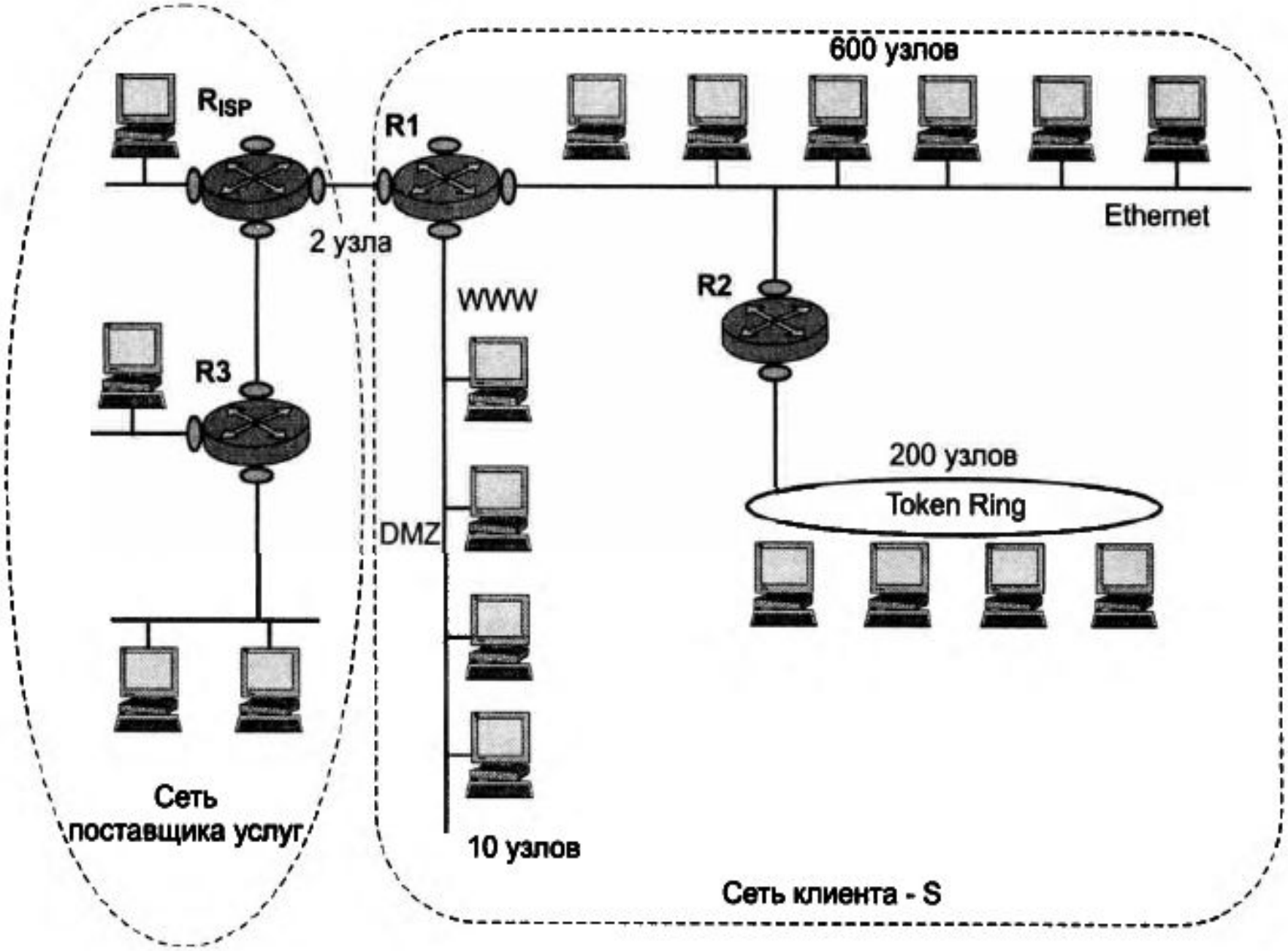


Рис. 15.15. Сети поставщика услуг и клиента

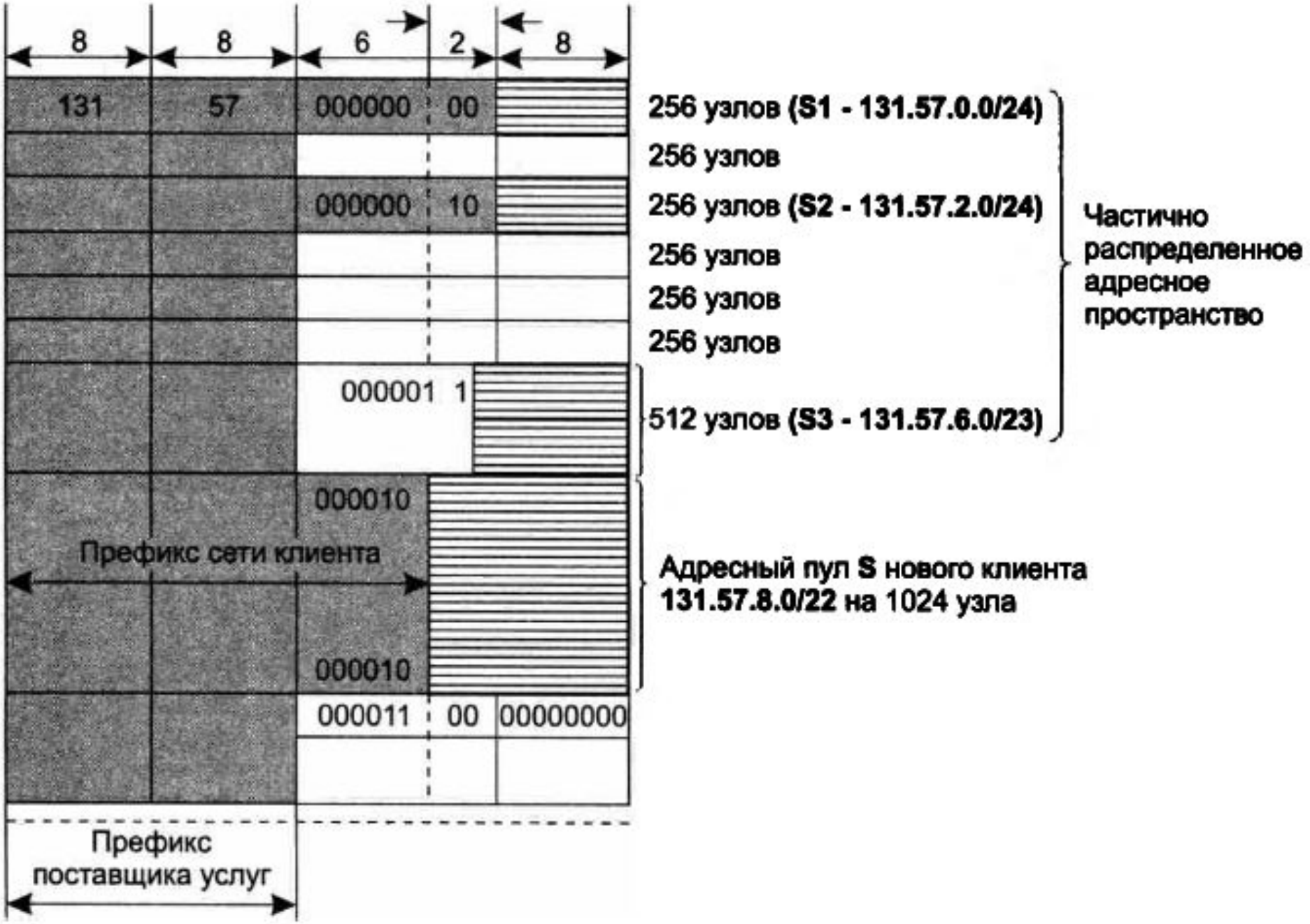


Рис. 15.16. Адресное пространство поставщика услуг

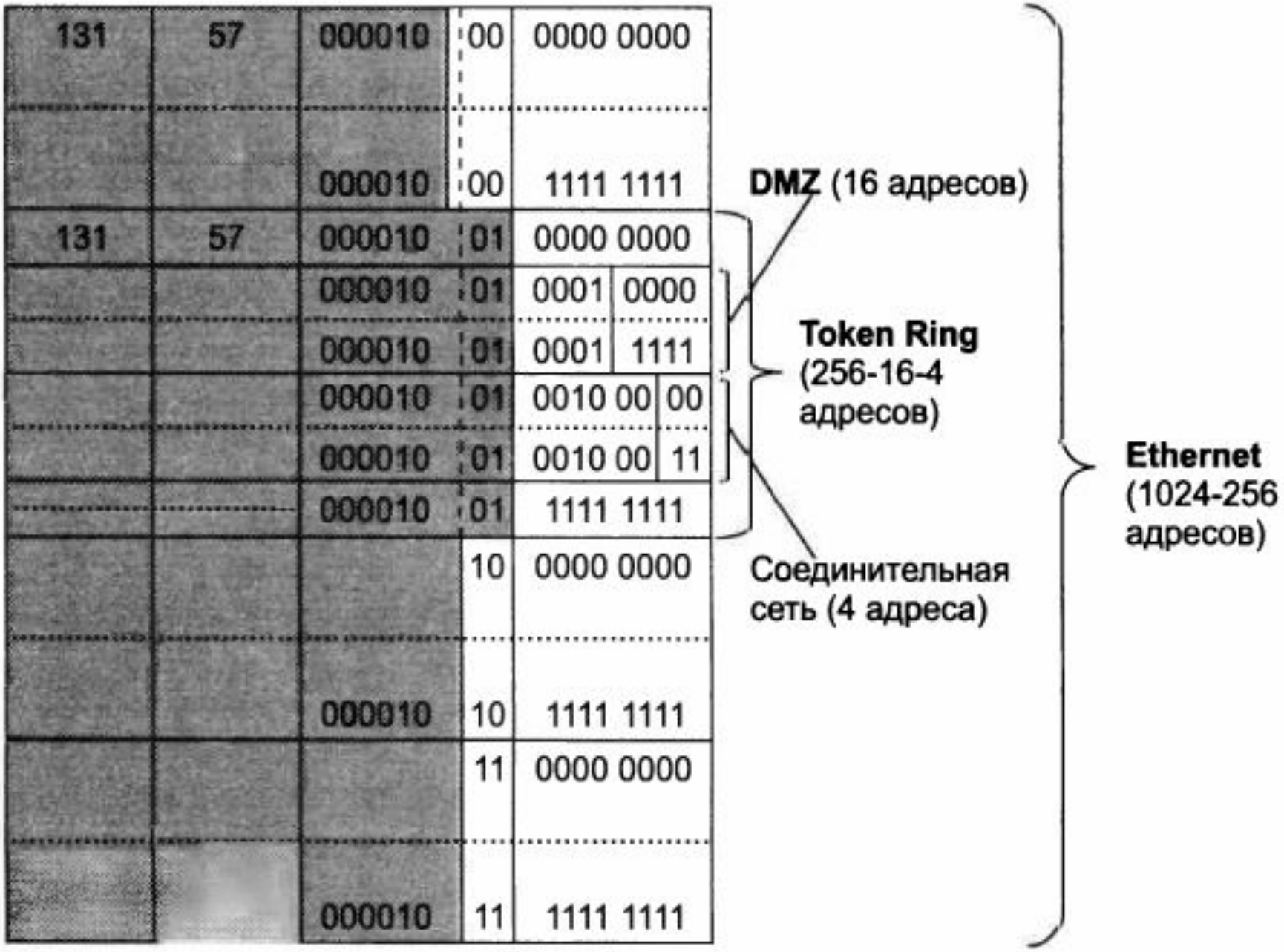


Рис. 15.17. Планирование адресного пространства для сетей клиента

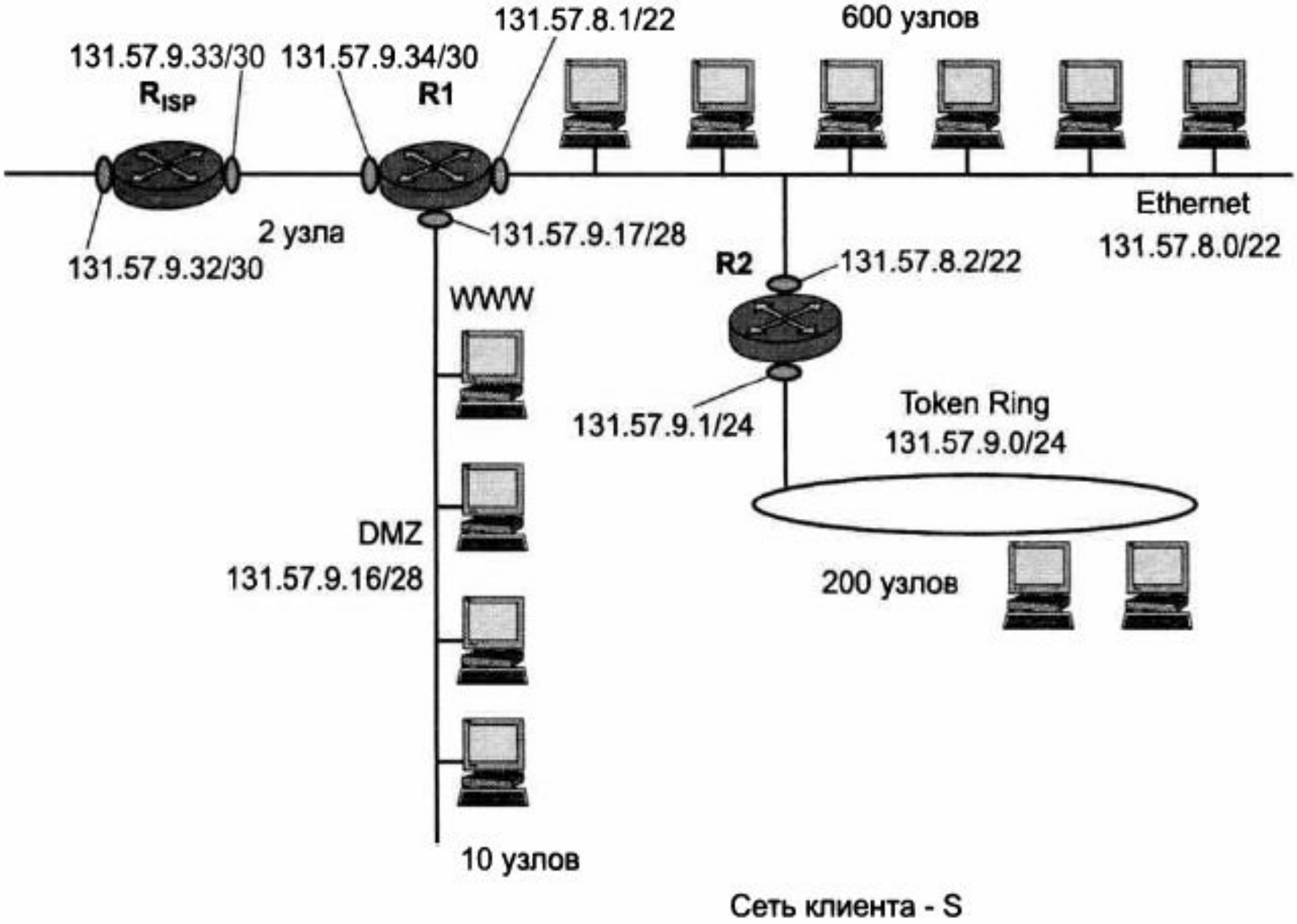


Рис. 15.18. Сконфигурированная сеть клиента

CIDR и маршрутизация

На решение этой проблемы сбоев магистральных маршрутизаторов из-за перегрузок и несовершенства протоколов маршрутизации направлена **технология бесклассовой междоменной маршрутизации CIDR.**

Суть заключается в следующем. Каждому поставщику услуг Интернета **назначается непрерывный диапазон IP-адресов**. При таком подходе все адреса каждого поставщика услуг имеют **общую старшую часть** — префикс, поэтому маршрутизация на магистралях Интернета может осуществляться на основе префиксов. Вместо множества записей по числу сетей в таблицу маршрутизации достаточно

Таблица 15.12. Таблица маршрутизатора RISP поставщика услуг

Адрес назначения	Маска	Следующий маршрутизатор	Номер выходного интерфейса	Расстояние
131.57.0.0 (S1)	255.255.255.0	R3	1	Подключена
131.57.2.0 (S2)	255.255.255.0	R3	3	1
131.57.4.0 (S3)	255.255.254.0	R1	3	1
131.57.8.0 (S)	**255.255.252.0**	**R1**	**2**	**Подключена**
Маршрут по умолчанию	0.0.0.0	$R_{external}$	4	—

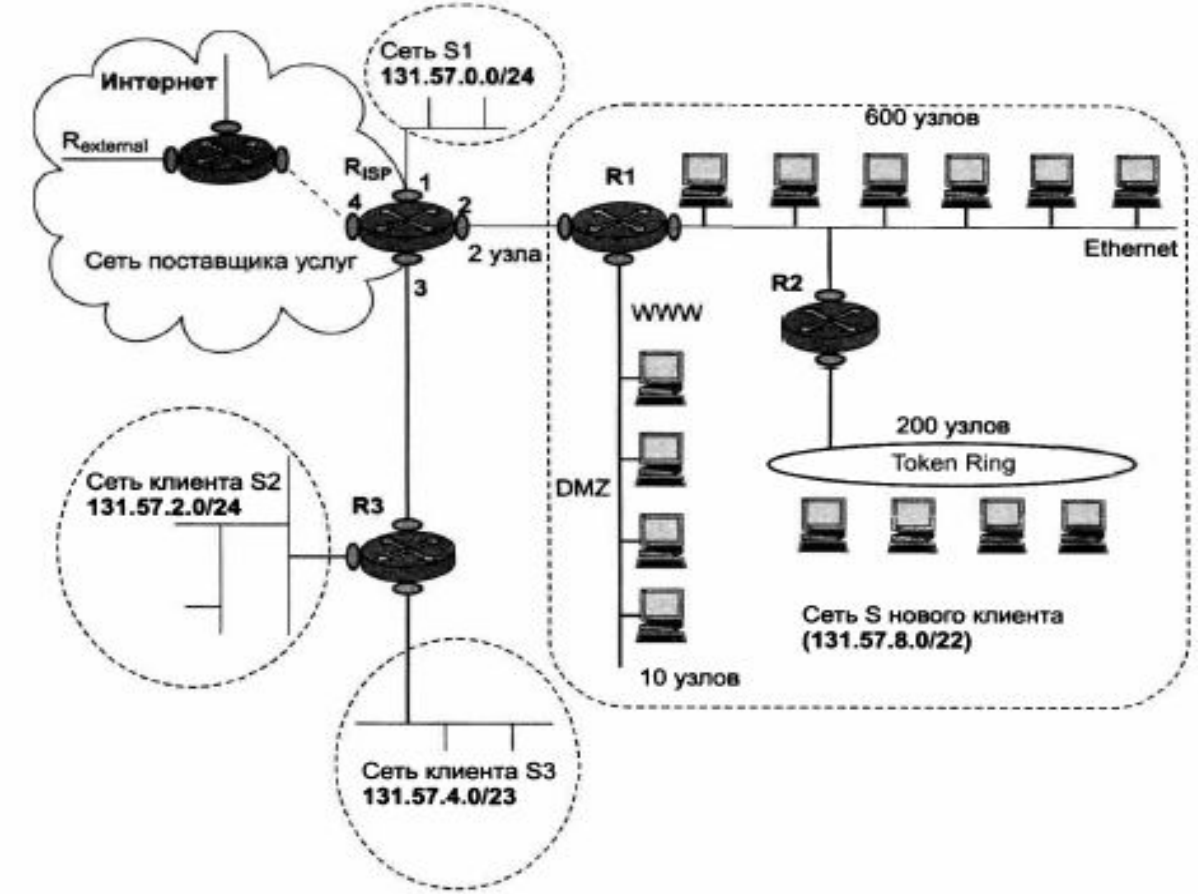


Рис. 15.19. Объединение подсетей

Итак, внедрение технологии CIDR позволяет решить две основные задачи.

- **Более экономное расходование адресного пространства.**
- **Уменьшение числа записей в таблицах маршрутизации за счет объединения маршрутов** — одна запись в таблице маршрутизации может представлять большое количество сетей.

Необходимым условием эффективного использования технологии CIDR является локализация адресов, то есть назначение адресов, имеющих совпадающие префиксы, сетям, располагающимся территориально по соседству.

Фрагментация IP-пакетов

Важной особенностью протокола IP является его **способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров (Maximum Transmission Unit, MTU).**

Фрагментация сообщений может происходить в узле-отправителе и динамически в маршрутизаторах.

- В первом случае деление **фрагментация** сообщения **происходит при передаче данных между протоколами одного и того же стека** внутри компьютера. Протоколы TCP анализируют тип технологии нижнего уровня, определяют ее MTU и делят сообщения на такие части, которые умещаются в кадры канального уровня того же стека протоколов.
- На маршрутизаторе, когда пакет необходимо передать из сети с большим значением MTU в сеть с меньшим значением MTU, становятся востребованными способности протокола IP выполнять фрагментацию.

Параметры фрагментации

Каждый из фрагментов должен быть снабжен полноценным заголовком IP.

- **Идентификатор пакета** используется для распознавания пакетов, образовавшихся путем деления на части (фрагментации) исходного пакета.
- **Поле времени жизни (**Time To Live, TTL) занимает один байт и определяет **предельный срок, в течение которого пакет может перемещаться по сети**. Время жизни пакета измеряется в секундах и задается источником (отправителем).
- **Поле смещения фрагмента** предоставляет получателю информацию о положении фрагмента относительно начала поля данных исходного нефрагментированного пакета.
- Установленный в единицу однобитный **флаг MF** (More Fragments — больше фрагментов) говорит о том, что **данный пакет является промежуточным (не последним) фрагментом.**
- **Флаг DF** (Do not Fragment — не фрагментировать), установленный в единицу, **запрещает маршрутизатору**

Механизм фрагментации

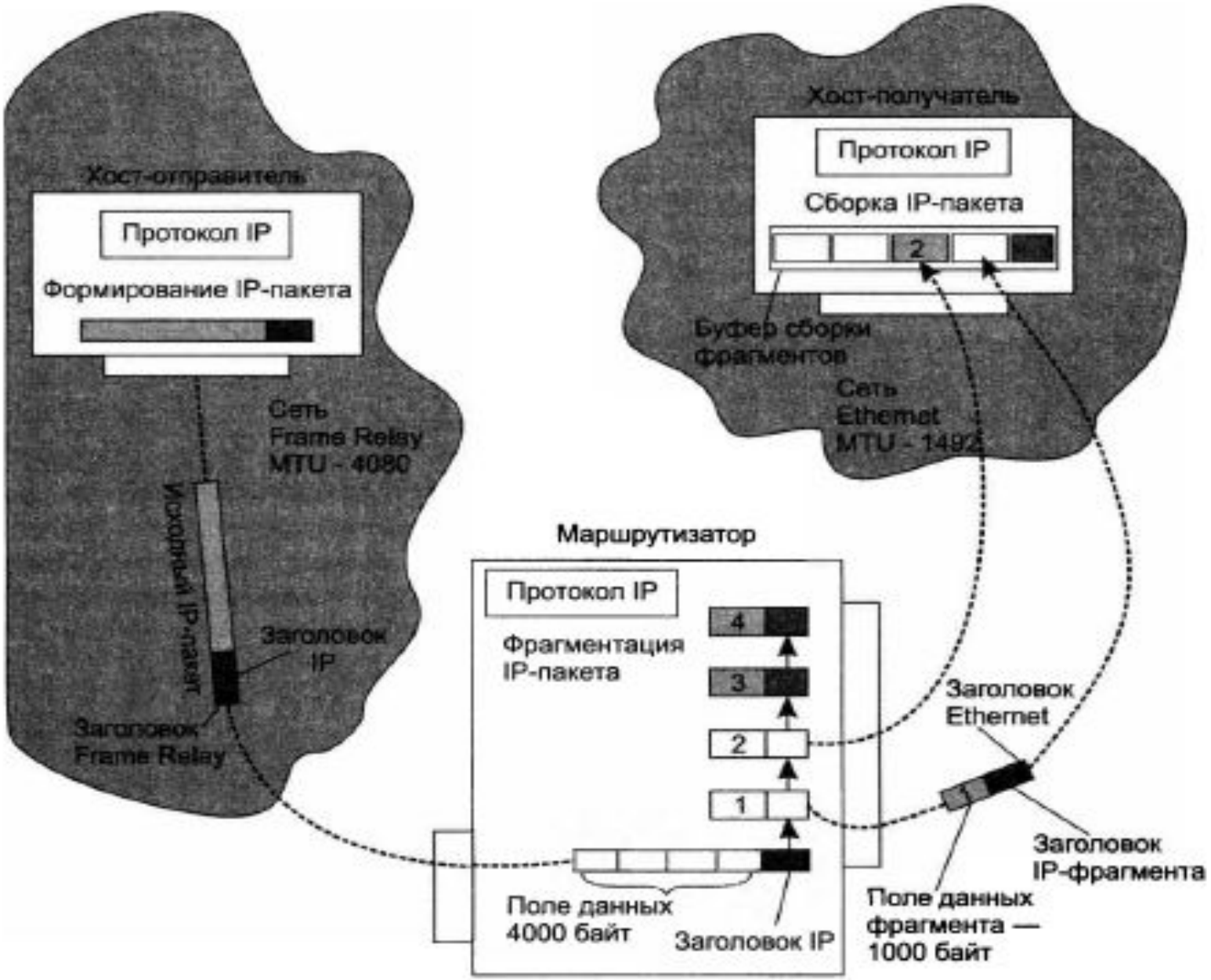


Рис. 15.20. Фрагментация в составной сети

Протокол ICMP

Протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP) является вспомогательным протоколом, использующимся для диагностики и мониторинга сети.

Свойство «необязательности» протокола IP, доставляющего данные «по возможности», компенсируется протоколами более высоких уровней стека TCP/IP.

Задача ICMP — быть **средством оповещения отправителя о «несчастных случаях», произошедших с его пакетами.** Для передачи по сети ICMP-сообщение инкапсулируется в поле данных IP-пакета. IP-адрес узла-источника определяется из заголовка пакета, вызвавшего инцидент.

Заголовок ICMP-сообщения состоит из 8 байт:

- **тип (1 байт)** — числовой идентификатор типа сообщения;
- **код (1 байт)** — числовой идентификатор, более тонко дифференцирующий тип ошибки;
- **контрольная сумма (2 байта)** — подсчитывается для всего ICMP-сообщения. **Содержимое оставшихся четырех байтов в заголовке и поле данных зав**

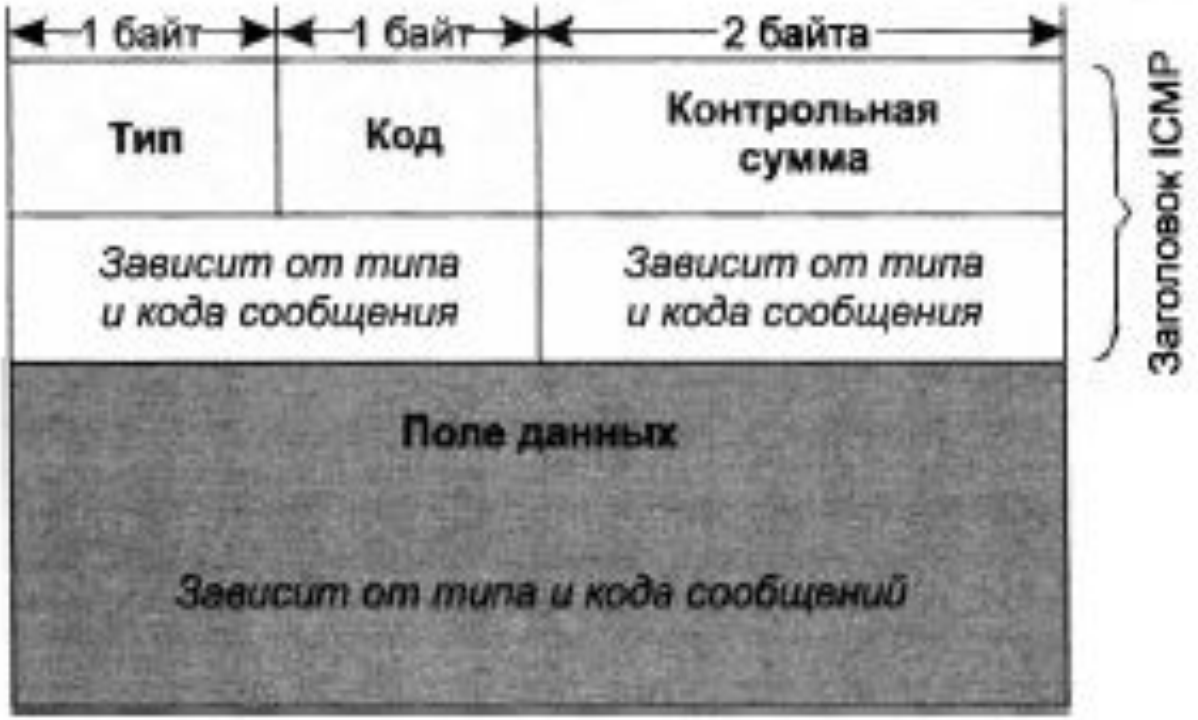


Рис. 15.21. Формат ICMP-сообщения

Эти сообщения можно разделить на две группы (помеченные на рисунке условными символами):

- **сообщения об ошибках,**
- **сообщения запрос-ответ.**

Сообщения типа запрос-ответ связаны в пары: эхо-запрос — эхо-ответ, запрос маски — ответ маски, запрос времени — ответ времени.

Сообщения об ошибках, конкретизируются уточняющим кодом.

Таблица типов ICMP-сообщений

Значение в поле «Тип»	Тип сообщения
0	Эхо-ответ
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправление маршрута
8	Эхо-запрос
11	Истечение времени диаграммы
12	Проблема с параметрами пакета
13	Запрос отметки времени
14	Ответ отметки времени
17	Запрос маски
18	Ответ маски

Таблица кодов причин ошибок 3

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
5	Ошибка в маршруте источника
6	Сеть назначения неизвестна
7	Узел назначения неизвестен
8	Узел-источник изолирован
9	Административный запрет
	. . . . .

? сообщение-запрос

(i) сообщение-ответ

√ сообщение-ошибка

Рис. 15.22. Типы и коды ICMP-сообщений

Утилита traceroute

Когда маршрутизатор не может передать или доставить IP-пакет, он отсылает узлу, отправившему этот пакет, сообщение о недостижимости узла назначения. В поле типа помещается значение 3, а в поле кода — значение из диапазона 0-15, уточняющее причину, по которой пакет не был доставлен.

Помимо причины ошибки, указанной в заголовке, дополнительная диагностическая информация передается в поле данных ICMP-сообщения. Именно туда помещает
IP-пакета, котор

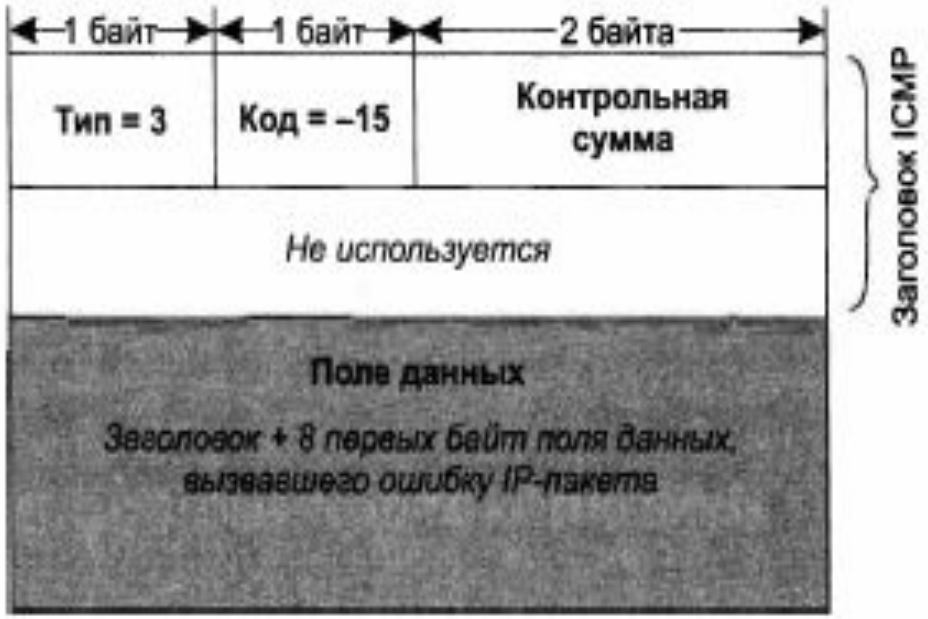


Рис. 15.23. Формат ICMP-сообщения об ошибке недостижимости узла назначения

ICMP-сообщения об ошибках лежат в основе работы популярной утилиты **traceroute** для Unix, имеющей в Windows название **tracert**. **Эта утилита позволяет проследить маршрут до удаленного хоста, определить среднее время оборота (RTT), IP-адрес и доменное имя каждого промежуточного маршрутизатора.**

Утилита traceroute осуществляет трассировку маршрута, посылая серию обычных IP-пакетов в конечную точку изучаемого маршрута.

Идея метода состоит в следующем. **Значение времени жизни (TTL) первого отправляемого пакета устанавливается равным 1**. Когда протокол IP первого маршрутизатора принимает этот пакет, то он в соответствии со своим алгоритмом **уменьшает значение TTL на 1 и получает 0.** Маршрутизатор **отбрасывает пакет с нулевым временем жизни** и возвращает узлу-источнику ICMP-сообщение об ошибке истечения времени дейтаграммы вместе с заголовком IP и первыми 8 байтами потерянного пакета.

Получив ICMP-сообщение о причине недоставки пакета, **утилита traceroute запоминает адрес первого маршрутизатора**.

Затем **traceroute посылает следующий IP-пакет, но теперь со значением TTL, равным 2**. Этот пакет благополучно проходит первый маршрутизатор, **но «умирает» на втором**, о чем немедленно отправляется аналогичное сообщение об ошибке истечения времени дейтаграммы. Утилита traceroute

Далее приведена копия экранной формы, выведенной утилитой tracert (Windows) при трассировке хоста ds.internic.net [198.49.45.29]:

```
1 311 ms 290 ms 261 ms 144.206.192.100
2 281 ms 300 ms 271 ms 194.85.73.5
3 2023 ms 290 ms 311 ms moscow-m9-2-S5.relcom.eu.net [193.124.254.37]
4 290 ms 261 ms 280 ms MSK-M9-13.Relcom.EU.net [193.125.15.13]
5 270 ms 281 ms 290 ms MSK.RAIL-1-ATM0-155Mb.Relcom.EU.net [193.124.254.82]
6 300 ms 311 ms 290 ms SPB-RASCOM-1-E3-1-34Mb.Relcom.EU.net [193.124.254.78]
7 311 ms 300 ms 300 ms Hssi11-0.GW1.STK2.ALTER.NET [146.188.33.125]
8 311 ms 330 ms 291 ms 421.ATM6-0-0.CR2.STK2.Alter.Net [146.188.5.73]
9 360 ms 331 ms 330 ms 219.Hssi4-0.CR2.LND1.Alter.Net [146.188.2.213]
10 351 ms 330 ms 331 ms 412.Atm5-0.BR1.LND1.Alter.net [146.188.3.205]
11 420 ms 461 ms 420 ms 167.ATM8-0-0.CR1.ATL1.Alter.Net [137.39.69.182]12 461 ms 441
```

Последовательность строк соответствует последовательности маршрутизаторов, образующих маршрут к заданному узлу. Первое число в строке — число хопов до соответствующего маршрутизатора. Если ответ от какого-либо маршрутизатора не приходит за заданное время, то вместо времени на экране печатается звездочка (*).

Далее идут IP-адрес и доменное имя (если оно имеется) маршрутизатора.

Утилита ping

Эхо-запрос и эхо-ответ, в совокупности называемые эхо-протоколом, представляют собой очень простое средство мониторинга сети. Компьютер или маршрутизатор посылает по составной сети ICMP-сообщение эхо-запроса, указывая в нем IP-адрес узла, достижимость которого нужно проверить. Узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса. Так как эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, то их успешная доставка означает нормальное функционирование всей транспортной системы состав

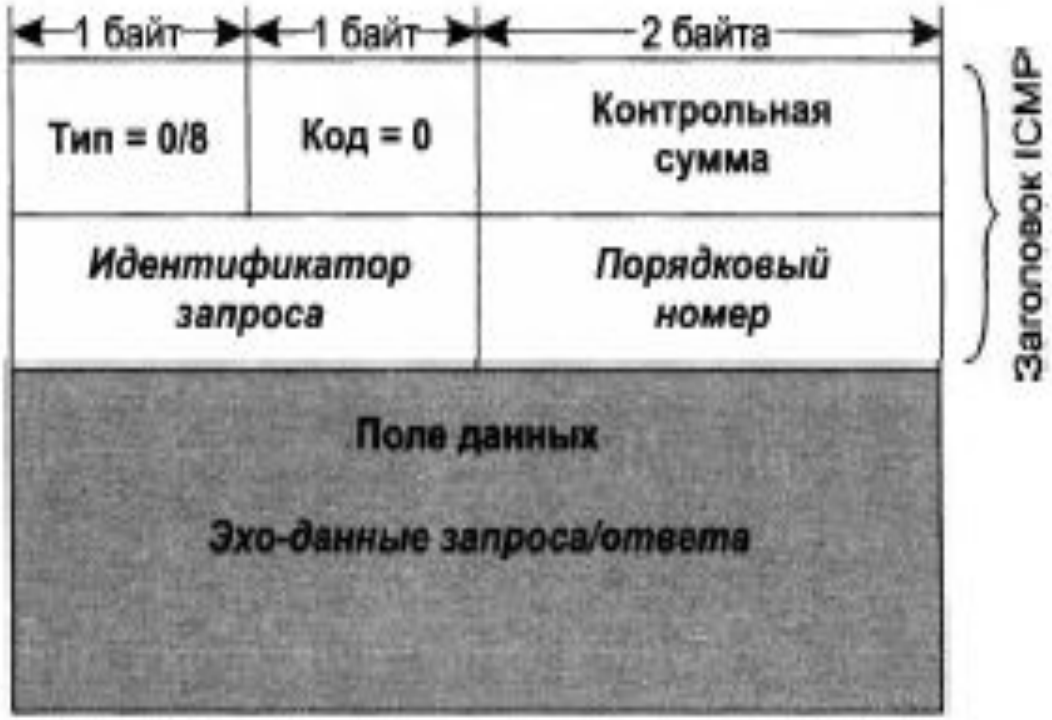


Рис. 15.24. Формат ICMP-сообщений типа эхо-запрос и эхо-ответ

Система адресации протокола IPv6

Новая (шестая) версия протокола IP (IPv6) внесла существенные изменения в систему адресации. **Прежде всего это коснулось увеличения разрядности адреса: вместо 4 байт IP-адреса в версии IPv4 в новой версии под адрес отведено 16 байт.** Это дает возможность пронумеровать огромное количество узлов:

340 282 366 920 938 463 463 374 607 431 762 211 456.

Главной целью изменения системы адресации было не механическое увеличение адресного пространства, а повышение эффективности работы стека

В новой версии IPv6 предусмотрено три основных типа адресов:

- **Индивидуальный адрес** (unicast) является уникальным идентификатором отдельного интерфейса конечного узла или маршрутизатора. Назначение этого типа адреса совпадает с назначением уникальных адресов в версии IPv4.
- **Групповой адрес** (multicast) аналогичен по назначению групповому адресу IPv4 — он идентифицирует группу интерфейсов, относящихся, как правило, к разным узлам. Пакет с таким адресом доставляется всем интерфейсам, имеющим такой адрес.
- **Адрес произвольной рассылки** (anycast) — это новый тип IP-адреса, определяющий группу интерфейсов. **Адрес произвольной рассылки может быть назначен только интерфейсам маршрутизаторам**. Адреса такого типа ориентированы на маршрутизацию от источника, когда маршрут прохождения пакета определяется узлом-отправителем путем указания IP-адресов всех промежуточных маршрутизаторов.

Индивидуальные адреса делятся на несколько подтипов, основным среди которых является **глобальный агрегируемый уникальный адрес.** В отличие от уникальных адресов узлов версии IPv4, которые состоят из двух полей — **номеров сети и узла**, — глобальные агрегируемые уникальные адреса IPv6 имеют более сложную структуру, включающую шесть полей (рис. 15.25).

- **Префикс формата** (Format Prefix, FP) для этого типа адресов имеет размер 3 бита и значение **001**.
- **Поле TLA (**Top-Level Aggregation) предназначено для идентификации сетей самых крупных поставщиков услуг. Конкретное значение этого поля представляет собой общую часть адресов, которыми располагает

3	13	8	24	16	64
FP	TLA		NLA	SLA	Идентификатор интерфейса

Рис. 15.25. Структура глобального агрегируемого уникального адреса в пакете IPv6

- **Поле NLA** (Next-Level Aggregation) предназначено для нумерации сетей средних и мелких поставщиков услуг.
- **Поле SLA** (Site-Level Aggregation) предназначено для адресации подсетей отдельного абонента, например подсетей одной корпоративной сети.
- **Идентификатор интерфейса** является аналогом номера узла в IPv4. Отличием версии IPv6 является то, что в общем случае **идентификатор интерфейса просто совпадает с его локальным (аппаратным) адресом,** а не представляет собой произвольно назначенный администратором

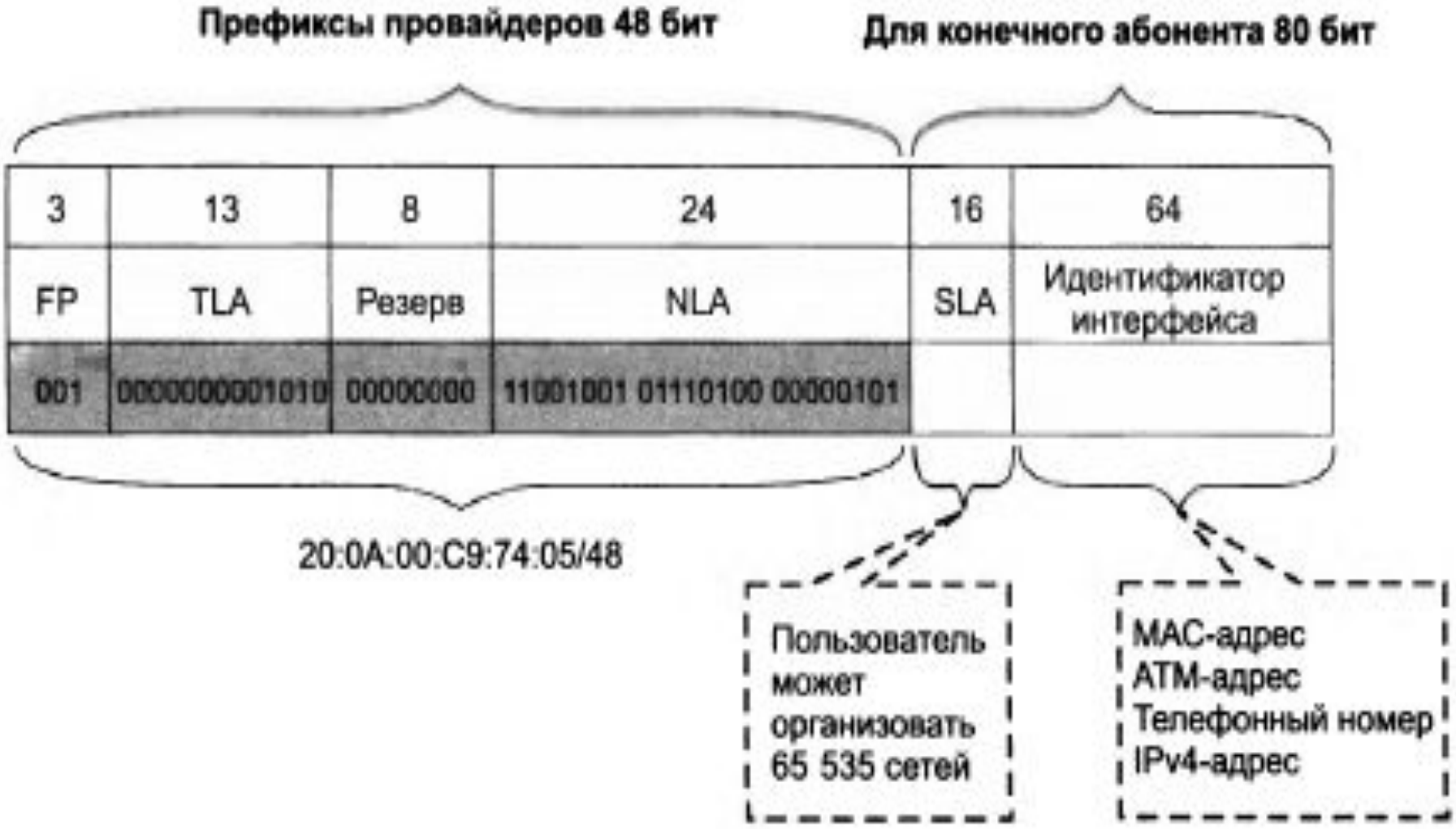


Рис. 15.26. Пример глобального агрегируемого адреса

Снижение нагрузки на маршрутизаторы

Для уменьшение объема служебной информации, передаваемой с каждым пакетом, в новом протоколе IP были введены понятия основного и дополнительных заголовков. **Основной заголовок присутствует всегда**, а необязательные **дополнительные заголовки могут содержать**, например, **информацию о фрагментации** исходного пакета, **полный маршрут следования пакета** при маршрутизации от источника, **информацию, необходимую для защиты передаваемых данных.**

Поле следующего заголовка соответствует по назначению полю протокола в версии IPv4 и содержит данные, определяющие тип заголовка, который следует за текущим. Каждый следующий дополнительный заголовок также

В предложениях по поводу протокола IPv6 фигурируют пока следующие типы дополнительных заголовков:

- **заголовок маршрутизации** — указание полного маршрута при маршрутизации от источника;
- **заголовок фрагментации** — информация, относящаяся к фрагментации IP-пакета;
- **заголовок аутентификации** — информация, необходимая для аутентификации конечных узлов и обеспечения целостности содержимого IP пакетов;
- **заголовок системы безопасности** — информация, необходимая для обеспечения конфиденциальности передаваемых данных путем шифрования и дешифрирования;
- **специальные параметры** — параметры, необходимые для последовательной обработки пакетов на каждом маршрутизаторе;
- **параметры получателя** —

Рис. 15.28. Структура пакета IPv6

Для того чтобы повысить производительность маршрутизаторов, в IPv6 предпринят ряд мер по освобождению маршрутизаторов от некоторых вспомогательных функций.

- **Перенесение функций фрагментации с маршрутизаторов на конечные узлы.** Конечные узлы в версии IPv6 обязаны найти минимальное значение MTU вдоль всего пути, соединяющего исходный узел с узлом назначения.
- **Агрегирование адресов** ведет к уменьшению размера адресных таблиц маршрутизаторов, а значит, к сокращению времени просмотра и обновления таблиц.
- **Широкое использование маршрутизации от источника.** При маршрутизации от источника узел-источник задает полный маршрут прохождения пакета через сети.

Переход на версию IPv6

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.

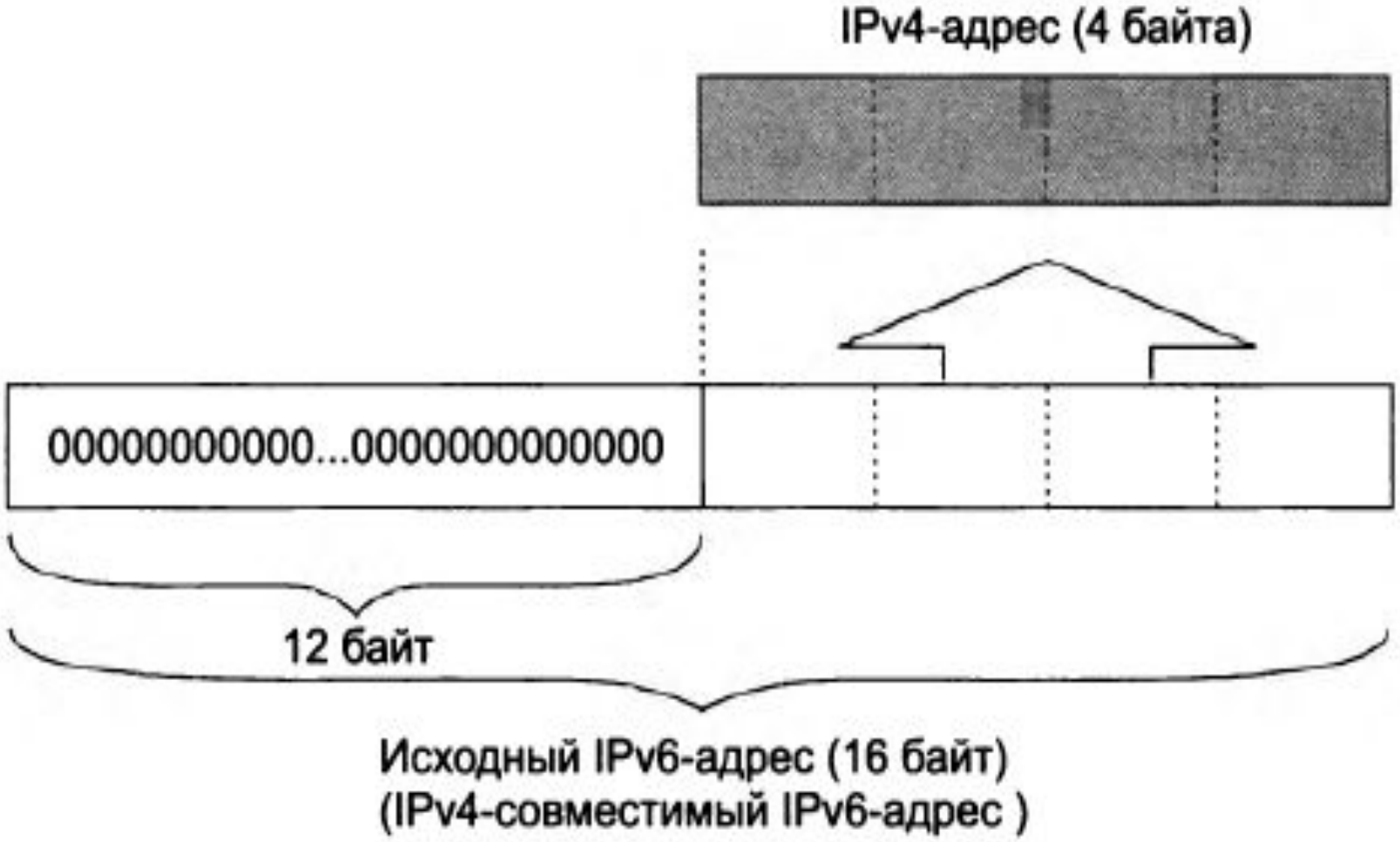


Рис. 15.29. Преобразование IPv6 в IPv4

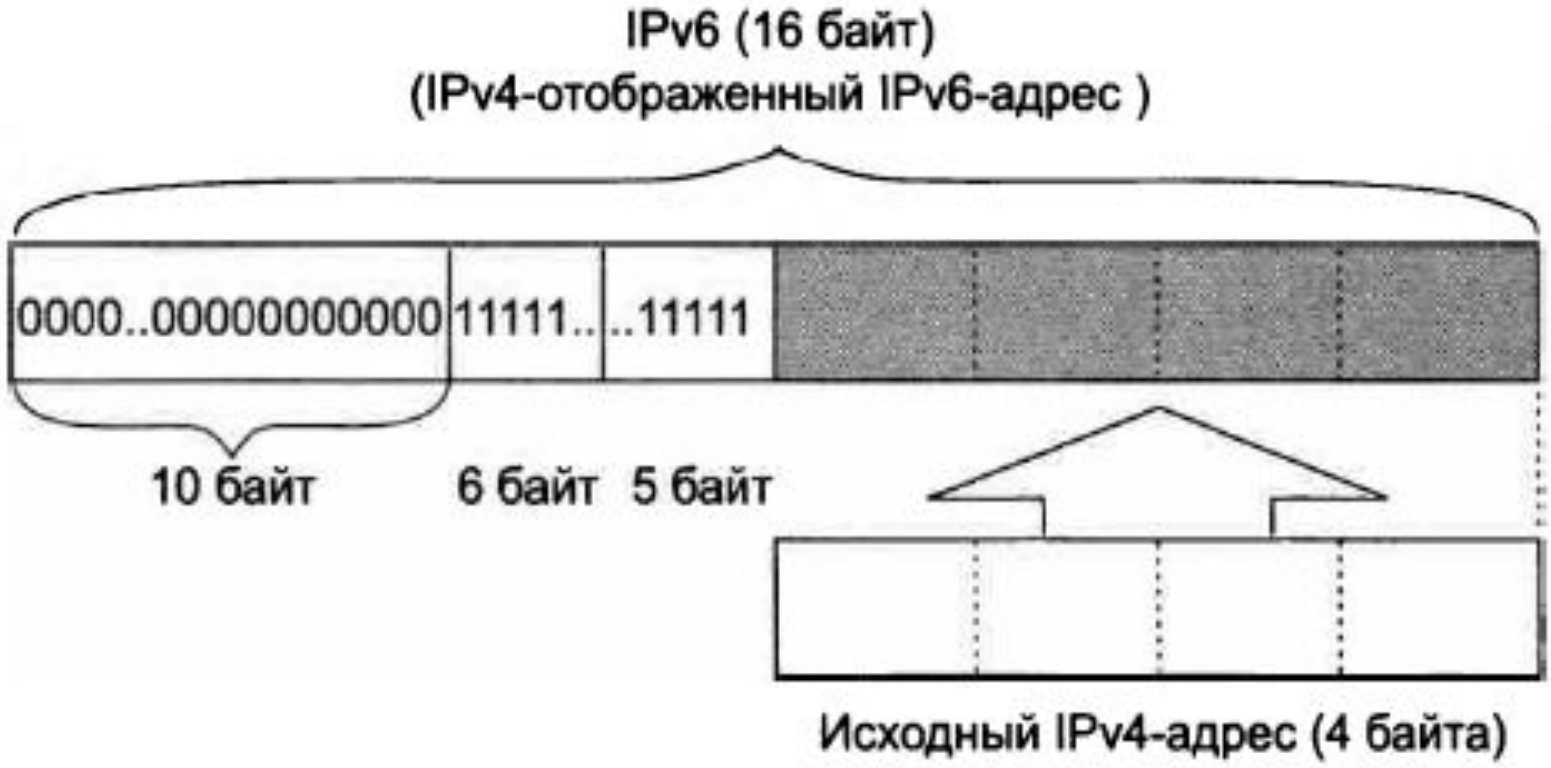


Рис. 15.30. Преобразование IPv4 в IPv6

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 (рис.

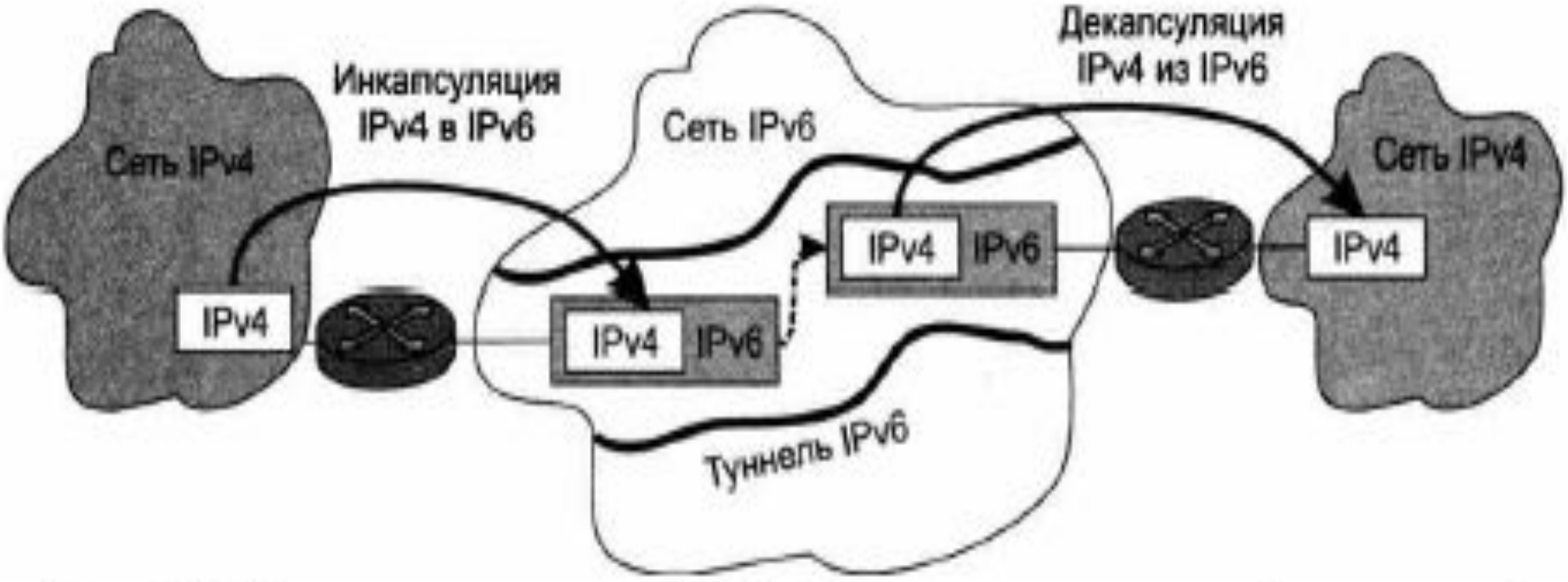


Рис. 15.31. Согласование технологий IPv4 и IPv6 путем туннелирования (инкапсуляции)

Спасибо за внимание!