Сети TCP/IP. Адресация в стеке протоколов TCP/IP

Важную часть технологии TCP/IP **составляют задачи адресации**, к числу которых относятся следующие:

- **Согласованное использование адресов различного типа**. Эта задача включает отображение адресов разных типов друг на друга, например сетевого IP-адреса на локальный, доменного имени — на IP-адрес.
- **Обеспечение уникальности адресов**.
- **Конфигурирование сетевых интерфейсов и сетевых приложений.**

Ключевым словом, которое характеризует принятый в TCP/IP подход к решению этих проблем, является **масштабируемость.** Процедуры, предлагаемые TCP/IP для назначения, отображения и конфигурирования адресов, одинаково хорошо работают в сетях разного масштаба. Наиболее популярными масштабируемыми средствами поддержки адресации в сетях TCP/IP являются: технология бесклассовой междоменной маршрутизации, система доменных имен, протокол

Структура стека протоколов TCP/IP

Сегодня стек TCP/IP широко используется как в глобальных, так и в локальных сетях. Этот стек имеет иерархическую структуру, в которой определено четыре уровня (рис. 14.1)

Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

Рис. 14.1. Иерархическая структура стека TCP/IP

Прикладной уровень стека TCP/IP соответствует трем верхним уровням модели OSI: прикладному, представления и сеансовому. Он объединяет сервисы, предоставляемые системой пользовательским приложениям. К ним относятся такие распространенные протоколы, как **протокол передачи файлов** (File Transfer Protocol, FTP), **протокол эмуляции терминала telnet**, **простой протокол передачи почты** (Simple Mail Transfer Protocol, SMTP), **протокол передачи гипертекста** (Hypertext Transfer Protocol, HTTP) и многие другие. Протоколы прикладного уровня развертываются на хостах.

Транспортный уровень стека TCP/IP может предоставлять вышележащему уровню два типа сервиса:

- **гарантированную доставку обеспечивает протокол управления передачей** (Transmission Control Protocol, TCP);
- **доставку по возможности, или с максимальными усилиями, обеспечивает протокол пользовательских дейтаграмм** (User Datagram Protocol, UDP).

UDP является простейшим дейтаграммным протоколом, который **используется тогда, когда задача надежного обмена данными либо вообще не ставится, либо решается средствами более высокого уровня** — прикладным уровнем или пользовательскими приложениями.

В функции протоколов TCP и UDP входит также исполнение роли **связующего звена** между прилегающими к транспортному уровню прикладным и сетевым уровнями.

Программные модули, реализующие протоколы TCP и UDP, подобно модулям протоколов прикладного уровня

Сетевой уровень, называемый также уровнем интернета, является стержнем всей архитектуры TCP/IP. **Он обеспечивает перемещение пакетов в пределах составной сети, образованной объединением нескольких подсетей.**

Основным протоколом сетевого уровня является межсетевой протокол (Internet Protocol, IP). В его задачу входит продвижение пакета между сетями — от одного маршрутизатора к другому до тех пор, пока пакет не попадет в сеть назначения. В отличие от протоколов прикладного и транспортного уровней протокол IP развертывается не только на хостах, но и на всех маршрутизаторах (шлюзах). **Протокол IP — это дейтаграммный протокол, работающий без установления соединений**

К сетевому уровню TCP/IP часто относят протоколы, выполняющие вспомогательные функции по отношению к IP - **протоколы маршрутизации RIP и OSPF,** предназначенные для изучения топологии сети, определения маршрутов и составления таблиц маршрутизации. По этой же причине к сетевому уровню могут быть отнесены **протокол межсетевых управляющих сообщений** (Internet Control Message Protocol, ICMP), предназначенный для передачи маршрутизатором источнику сведений об ошибках, возникших при передаче пакета.

Идеологическим отличием архитектуры стека TCP/IP от многоуровневой архитектуры других стеков является интерпретация функций самого нижнего уровня — уровня сетевых интерфейсов.

Нижний уровень стека TCP/IP **отвечает только за организацию взаимодействия с подсетями разных технологий**, входящими в составную сеть. TCP/IP рассматривает любую подсеть, входящую в составную сеть, как средство транспортировки пакетов между двумя соседними маршрутизаторами.

Задачу организации интерфейса между технологией TCP/IP и любой другой технологией промежуточной сети упрощенно можно свести к двум задачам:

- **упаковка (инкапсуляция) IP-пакета в единицу передаваемых данных промежуточной сети;**
- **преобразование сетевых адресов в адреса технологии данной промежуточной сети.**

Такой гибкий подход упрощает решение проблемы расширения набора поддерживаемых технологий. При появлении новой популярной технологии она быстро включается в стек TCP/IP путем разработки соответствующего стандарта, определяющего метод инкапсуляции IP-пакетов в ее кадры.

Каждый коммуникационный протокол оперирует некоторой единицей передаваемых данных. Названия этих единиц иногда закрепляются стандартом, а чаще просто определяются традицией.

Рис. 14.2. Названия протокольных единиц данных в TCP/IP

- **Потоком данных, информационным потоком, или просто потоком, называют данные, поступающие от приложений на вход протоколов транспортного уровня — TCP и UDP.** Протокол TCP «нарезает» из потока данных сегменты.
- **Единицу данных протокола UDP часто называют дейтаграммой. Дейтаграмма — это общее название для единиц данных, которыми оперируют протоколы без установления соединений**. К таким протоколам относится и протокол IP, поэтому его единицу данных иногда тоже называют дейтаграммой, хотя достаточно часто используется и другой термин — пакет.
- В стеке TCP/IP **единицы данных любых технологий**, в которые упаковываются IP-пакеты для их последующей передачи через сети составной сети, **принято называть также**

Типы адресов стека TCP/IP

Для идентификации сетевых интерфейсов используются три типа адресов:

- **локальные (аппаратные) адреса;**
- **сетевые адреса (IP-адреса);**
- **символьные (доменные) имена.**

Локальные адреса

В большинстве технологий LAN (Ethernet, FDDI, Token Ring) для однозначной адресации интерфейсов используются MAC-адреса. Роль, которую играют эти адреса в TCP/IP, не зависит от того, какая именно технология используется в подсети, поэтому все они имеют общее название — **локальные (аппаратные) адреса.**

Сетевые IP-адреса

Реализацией глобальной системы адресации является уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей. **Пара, состоящая из номера сети и номера узла, отвечает поставленным условиям и может являться сетевым адресом, или в терминологии TCP/ IP — IP-адресом.**

Маршрутизатор по определению входит сразу в несколько сетей, следовательно, каждый его интерфейс должен иметь собственный IP-адрес. Конечный узел, имеющий несколько сетевых интерфейсов, также может входить в несколько IP-сетей, а значит, иметь несколько IP-адресов — по числу сетевых связей. Таким образом, **IP-адрес идентифицирует не отдельный узел сети, а одно сетевое соединение, или один**

Каждый раз, когда пакет направляется адресату через составную сеть, в его заголовке указывается IP-адрес узла назначения. По номеру сети назначения каждый очередной маршрутизатор находит IP-адрес следующего маршрутизатора. Между IP-адресом и локальным адресом узла нет никакой функциональной зависимости, поэтому единственный способ установления соответствия — ведение таблицы. **Эту задачу решает протокол разрешения адресов ARP (рис. 14.3).**

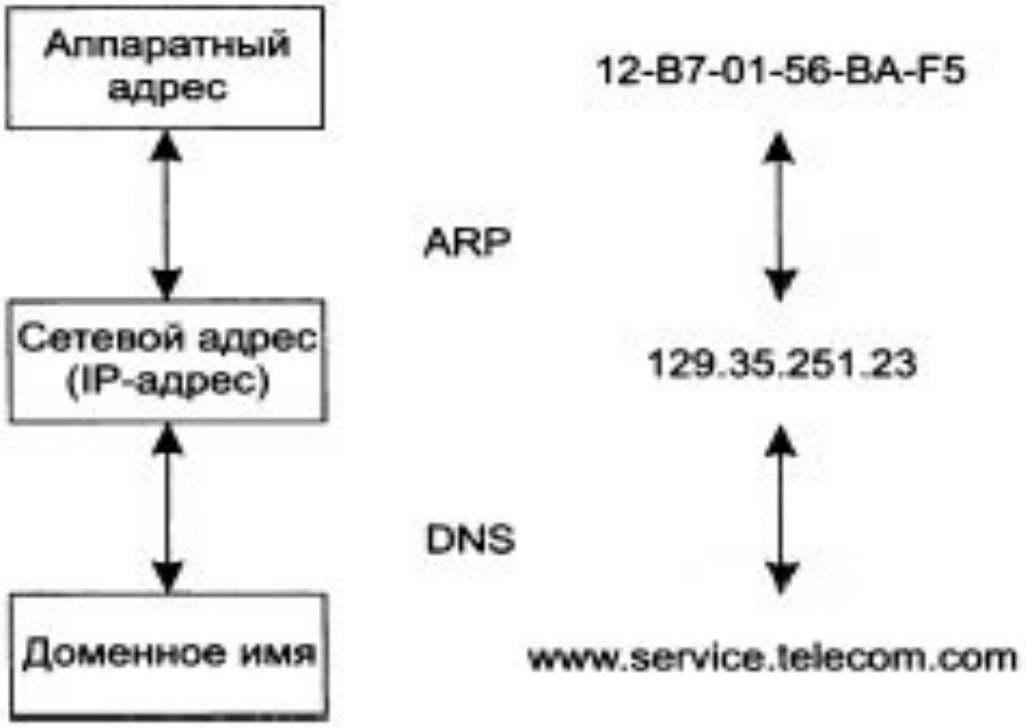

Рис. 14.3. Преобразование адресов

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса.

Символьные идентификаторы сетевых интерфейсов в пределах составной сети строятся по иерархическому принципу. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала — простое имя хоста, затем — имя группы хостов, потом — имя более крупной группы (домена), и так — до имени домена самого высокого уровня. **Символьные имена называют также доменными именами.**

В сетях TCP/IP используется специальная сетевая служба, называемая системой доменных имен (Domain Name System, DNS), которая автоматически устанавливает соответствие между доменными именами и IP-адресами на основании создаваемых администраторами сети таблиц соответствия. **По этой причине доменные имена называют также**

Формат IP-адреса

В заголовке IP-пакета предусмотрены поля для хранения IP-адреса отправителя и IP- адреса получателя. Каждое из этих полей имеет фиксированную длину 4 байта (32 бита).

Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например:

128.10.2.30

Этот же адрес может быть представлен в двоичном формате:

10000000 00001010 00000010 00011110

Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Вместе с тем при передаче пакета по сети часто возникает необходимость разделить адрес на эти две части. Можно предложить несколько

Простейший из них состоит в использовании фиксированной границы. **При этом все 32-битное поле адреса заранее делится на две части не обязательно равной, но фиксированной длины**, в одной из которых всегда будет размещаться номер сети, в другой — номер узла. Поскольку поле, которое отводится для хранения номера узла, имеет фиксированную длину, все сети будут иметь одинаковое максимальное число узлов. Такой жесткий подход не позволяет дифференцированно удовлетворять потребности отдельных предприятий и организаций.

Второй подход основан на применении **маски, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла.** При таком подходе адресное пространство можно использовать для создания множества сетей разного размера.

Маска — это число, применяемое в паре с IP-адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Граница между последовательностями единиц и нулей в маске соответствует

Третий способ основан на **классах адресов**. Этот способ представляет собой компромисс по отношению к двум предыдущим: **размеры сетей хотя и не могут быть произвольными, как при использовании масок, но и не должны быть одинаковыми, как при установлении фиксированных границ.** Вводится пять классов адресов: A, B, C, D, E. Три из них — A, B и C — предназначены для адресации сетей, а два — D и E — имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером

Классы IP-адресов

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса (рис. 14.4).

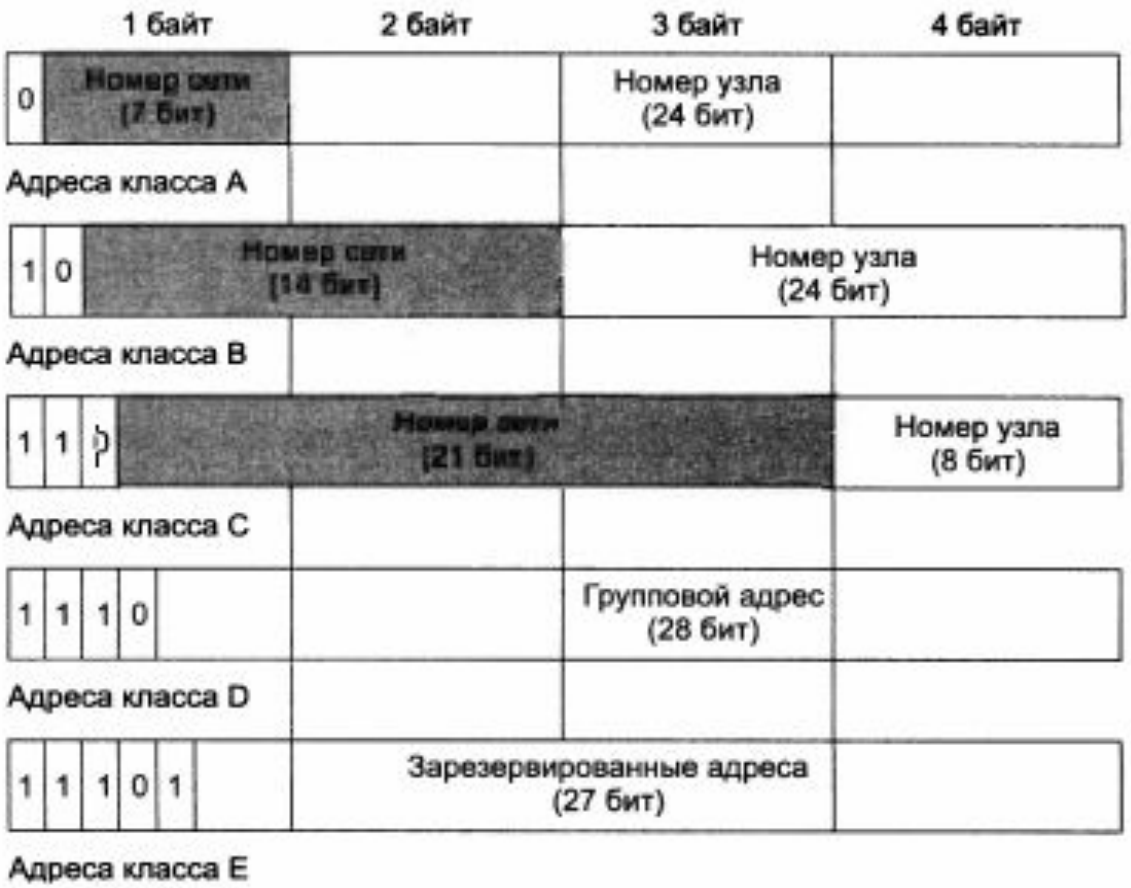

Рис. 14.4. Классы IP-адресов

- Сетей класса A сравнительно немного, зато количество узлов в них очень большое, оно может достигать 2^24, что равно 16 777 216 узлов. Сетей класса B больше, чем сетей класса A, но их размеры меньше, максимальное количество узлов в сетях класса B составляет 2^16 (65 536). Сетей класса C больше всего, но они характеризуются самым маленьким максимально возможным количеством узлов, всего – 2^8 (256).
- В то время как **адреса классов A, B и C используются для идентификации отдельных сетевых интерфейсов**, то есть являются индивидуальными адресами, **групповые адреса класса D идентифицируют группу сетевых интерфейсов**, которые в общем случае могут принадлежать разным сетям. Интерфейс, входящий в группу, получает наряду с обычным индивидуальным IP-адресом еще один групповой адрес.
- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к **классу**

Особые IP-адреса

В TCP/IP существуют ограничения при назначении IP-адресов, а именно номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц. Отсюда следует, что максимальное количество узлов, каждого класса, должно быть уменьшено на 2.

Введя эти ограничения, разработчики технологии TCP/IP получили возможность расширить функциональность системы адресации следующим образом:

- Если IP-адрес состоит только из двоичных нулей, то он называется **неопределенным адресом** и обозначает адрес того узла, который сгенерировал этот пакет.
- Если в поле номера сети стоят только нули, то по умолчанию считается, что **узел назначения принадлежит той же самой** сети, что и узел, который отправил пакет.
- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такой адрес называется **ограниченным широковещательным (limited broadcast**).
- Если в поле адреса назначения в разрядах, соответствующих номеру узла, стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети, номер которой указан в адресе назначения. Такой тип адреса называется **широковещательным (broadcast)**.

Особый смысл имеет IP-адрес, первый октет которого равен 127. **Этот адрес является внутренним адресом стека протоколов компьютера (или маршрутизатора).** Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127. Когда программа посылает данные по IP-адресу 127.x.x.x, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера как только что принятые. Маршрут перемещения данных образует «петлю», поэтому этот адрес называется **адресом обратной петли** (loopback).

Использование масок при IP-адресации

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой.

Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде IP-адрес 129.64.134.5 равен:

10000001.01000000.10000110.00000101

В то время как маска 255.255.128.0 выглядит так:

11111111.11111111.10000000.00000000

Если игнорировать маску и интерпретировать адрес 129.64.134.5 на основе классов, то номером сети является 129.64.0.0, а номером узла — 0.0.134.5 (поскольку адрес относится к классу B).

Если же использовать маску, то 17 последовательных двоичных единиц в маске «наложенные» на IP-адрес 129.64.134.5, делят его на две части:

- **номер сети: 10000001.01000000.1;**
- **номер узла: 0000110.00000101.**

Наложение маски можно интерпретировать как выполнение логической операции И (AND). Так, в предыдущем примере номер сети из адреса 129.64.134.5 является результатом выполнения логической операции AND с маской 255.255.128.0:

10000001 01000000 10000110 00000101 AND

11111111 11111111 10000000 00000000

Для записи масок используются и другие форматы. Например, удобно интерпретировать значение маски, записанной в шестнадцатеричном коде: FF.FF.00.00 — маска для адресов класса B. Еще чаще встречается запись с префиксом 185.23.44.206/26 — данная запись говорит о том, что маска для этого адреса содержит 26 единиц.

Таблица 14.2. Маски для стандартных классов сетей

Класс адресов	Десятичная форма	Двоичная форма	Шестнадцатеричная форма	Префикс
A	255.0.0.0	11111111. 00000000. 00000000. 00000000	FF.00.00.00	/8
B	255.255.0.0	11111111. 11111111. 00000000. 00000000	FF.FF.00.00	/16
C	255.255.255.0	11111111. 11111111. 11111111. 00000000	FF.FF.FF.00	/24

Маски могут использоваться для самых разных целей. С их помощью администратор может разбить одну выделенную ему поставщиком услуг сеть определенного класса на несколько других, не требуя от него дополнительных номеров сетей, — эта **операция называется разделением на подсети (subnetting).** На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых «префиксов» с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов — **такая операция называется**

Порядок назначения IP-адресов

По определению схема IP-адресации должна обеспечивать уникальность нумерации сетей, а также уникальность нумерации узлов в пределах каждой из сетей. Следовательно, процедуры назначения номеров как сетям, так и узлам сетей должны быть централизованными.

Назначение адресов автономной сети

В небольшой автономной IP-сети условие уникальности номеров сетей и узлов может быть выполнено «вручную» сетевым администратором.

Однако при таком подходе исключена возможность в будущем подсоединить данную сеть к Интернету. Чтобы избежать коллизий, в стандартах Интернета **определено несколько диапазонов частных адресов, рекомендуемых для автономного использования**:

- в классе A — сеть 10.0.0.0;
- в классе B — диапазон из 16 сетей (172.16.0.0-172.31.0.0);
- в классе C — диапазон из 255 сетей (192.168.0.0-192.168.255.0).

Рассмотрим пример, когда две сети необходимо соединить глобальной связью. В таких случаях в качестве линии связи используют два маршрутизатора, соединенных по двухточечной схеме (рис. 14.5). Для вырожденной сети, образованной линией связи, связывающей порты двух смежных маршрутизаторов, приходится выделять отдельный номер сети, хотя в этой сети всего два узла. Принципиальным решением является переход на новую версию протокола IP — протокол IPv6, в котором резко расширяется адресное пространство.

Рис. 14.5. Нерациональное использование пространства IP-адресов

Адресация и технология CIDR

Технология бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR) основана на использовании масок для более гибкого распределения адресов и более эффективной маршрутизации. **Она допускает произвольное разделение IP-адреса на поля для нумерации сети и узлов.** При такой системе адресации клиенту может быть выдан пул адресов, более точно соответствующий его запросу, чем это происходит при адресации, основанной на классах адресов.

Пусть, например, как показано на рис. 14.6, провайдер располагает адресами в диапазоне

0-193.23.255.255, или в двоичной записи:

1100 0001.00010100.0000 0000.0000 0000-1100 0001.00010111.1111 1111.1111 1111.

Здесь префикс провайдера имеет длину 14 разрядов — 1100 0001.0001 01, что можно записать в виде 193.20.0.0/14. Префикс обычно интерпретируется как номер подсети.

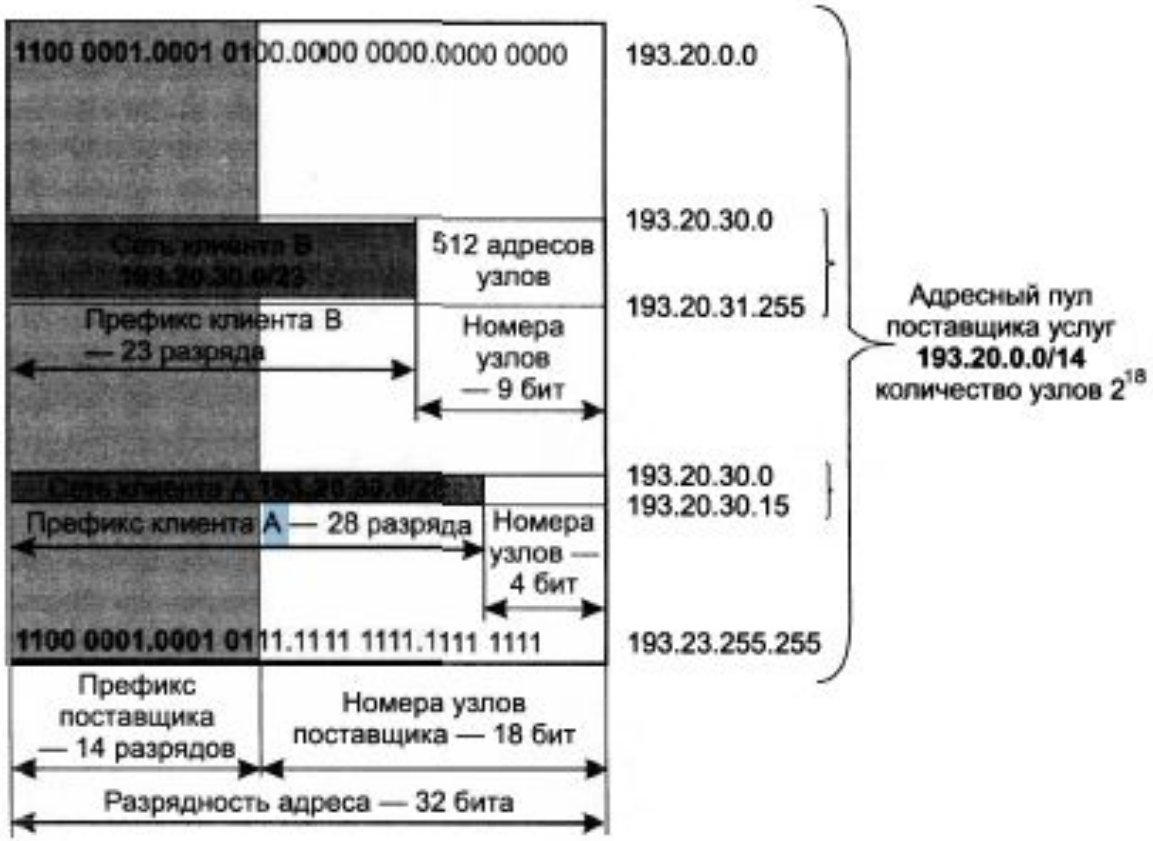

Рис. 14.6. Схема распределения адресного пространства в соответствии с CIDR

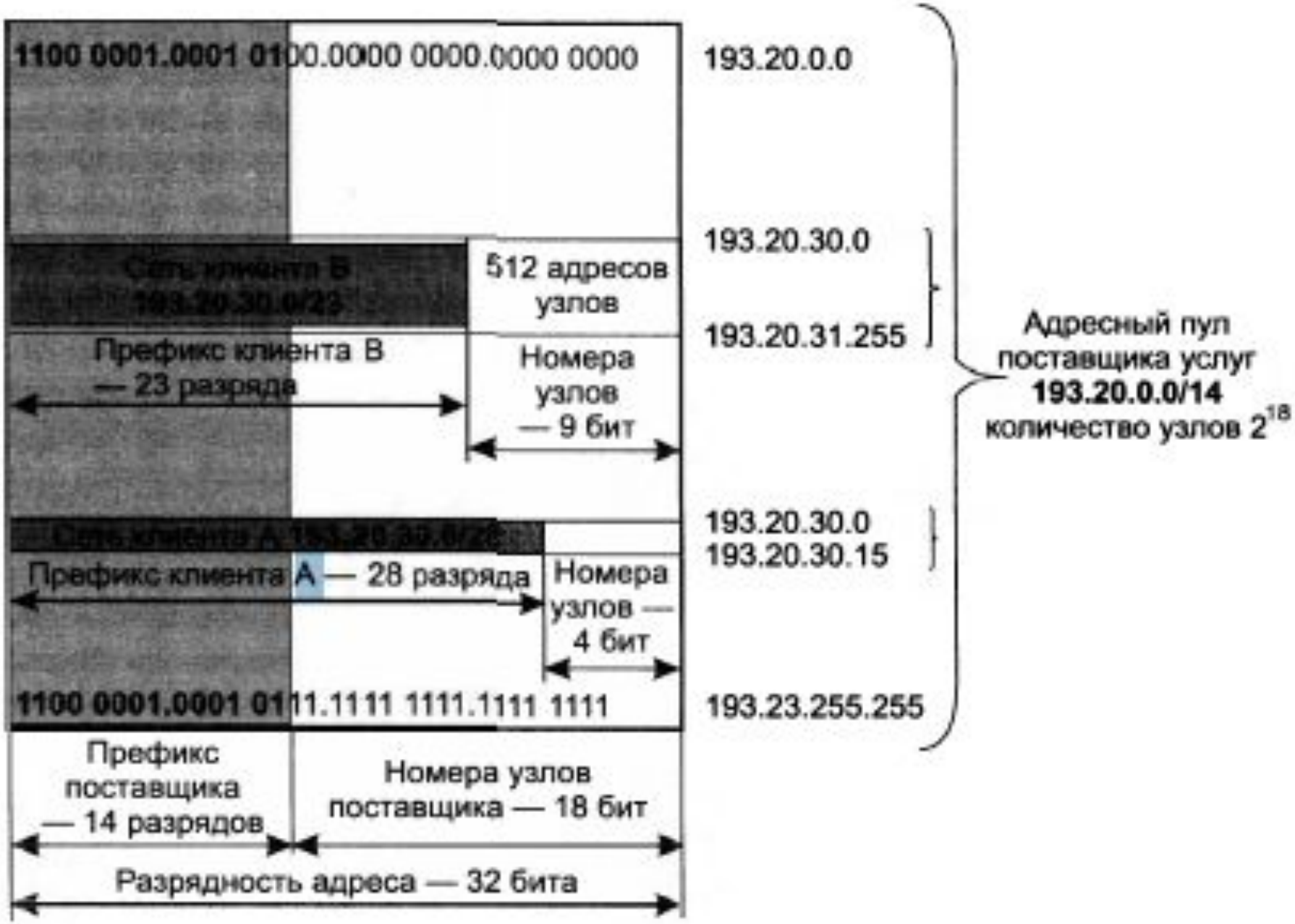

Рис. 14.6. Схема распределения адресного пространства в соответствии с CIDR

Для обобщенного представления пула адресов IP/n справедливы следующие утверждения:

- значением префикса (номера сети) являются n старших двоичных разрядов IP адреса;
- поле для адресации узлов состоит из (32-n) младших двоичных разрядов IP-адреса;
- первый по порядку адрес должен состоять только из нулей;
- Q количество адресов в пуле равно 2^(32-n)

Отображение IP-адресов на локальные адреса

На каждом маршрутизаторе протокол IP определяет, какому следующему маршрутизатору в этой сети надо направить пакет. В результате решения этой задачи протоколу IP становится известен IP-адрес интерфейса следующего маршрутизатора. Чтобы локальная технология сети смогла доставить пакет следующему маршрутизатору, необходимо:

- **упаковать пакет в кадр соответствующего для данной сети формата (например, Ethernet);**
- **снабдить данный кадр локальным адресом следующего маршрутизатора.**

Решением этих задач занимается уровень

Протокол разрешения адресов (ARP)

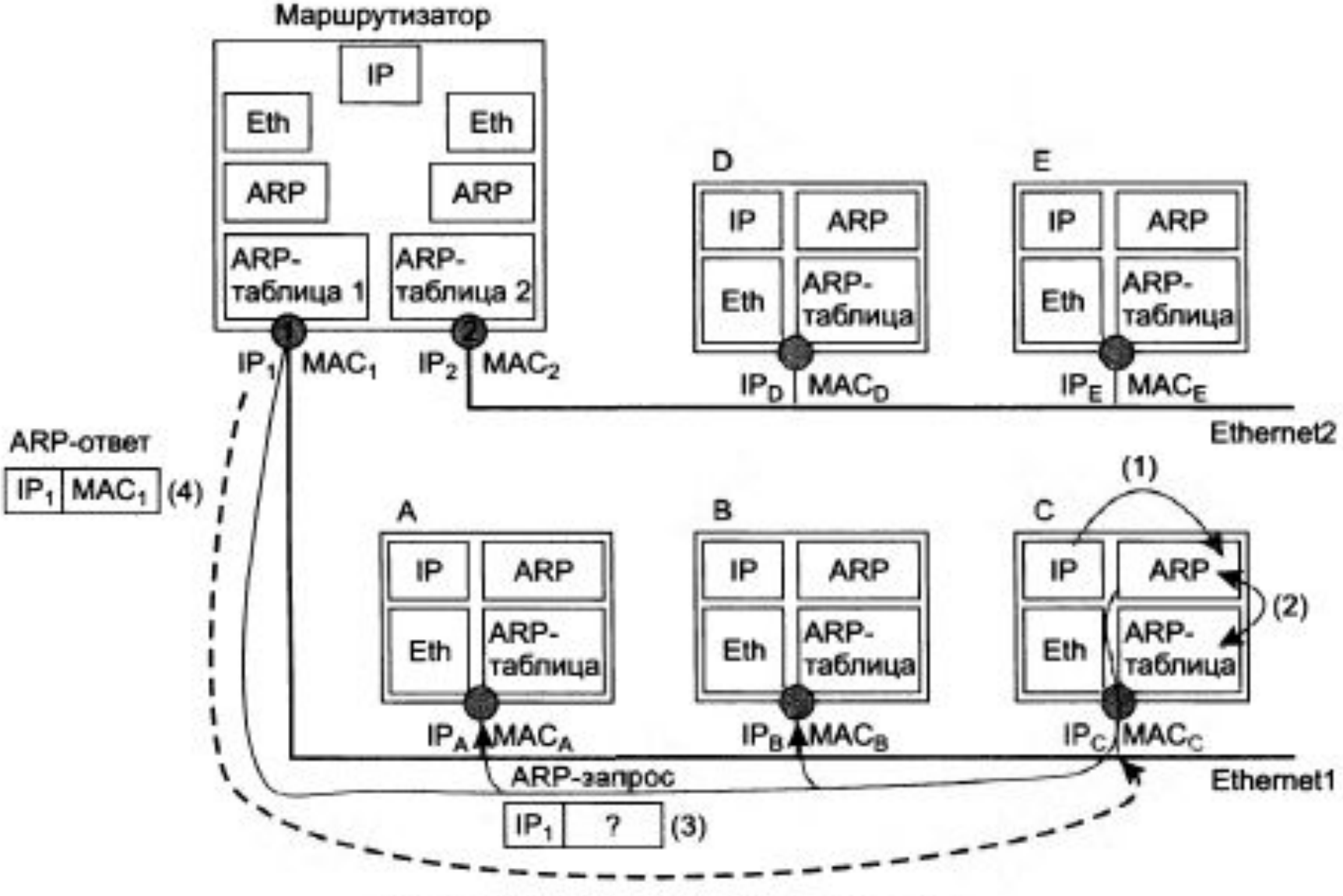

Рис. 14.7. Схема работы протокола ARP

1. На первом шаге происходит передача от протокола IP протоколу ARP примерно такого сообщения: «Какой MAC-адрес имеет интерфейс с адресом IP_1?»
2. Работа протокола ARP начинается с просмотра собственной ARP-таблицы. Предположим, что среди содержащихся в ней записей отсутствует запрашиваемый IP-адрес.
3. В этом случае протокол ARP формирует ARP-запрос, вкладывает его в кадр протокола Ethernet и широковещательно рассылает.
4. Все интерфейсы сети Ethernet 1 получают ARP-запрос и направляют его «своему» протоколу ARP. ARP сравнивает указанный в запросе адрес IP_1 с IP-адресом собственного интерфейса.
5. Протокол ARP, который констатировал совпадение, формирует ARP-ответ. В ARP-ответе маршрутизатор указывает локальный адрес MAC1 соответствующий адресу IP_1 своего интерфейса, и отправляет его запрашивающему узлу.

В результате обмена ARP-сообщениями модуль IP, пославший запрос с интерфейса, имеющего адрес **194.85.135.75**, определил, что IP-адресу **194.85.135.65** соответствует MAC-адрес **00E0F77F1920**. Этот адрес затем помещается в заголовок кадра Ethernet, ожидавшего отправления IP-пакета.

Чтобы уменьшить число ARP-обращений в сети, найденное соответствие между IP-адресом и MAC-адресом сохраняется в ARP-таблице соответствующего интерфейса, в данном случае — это запись:

194.85.135.65 - 00E0F77F1920

В ARP-таблицах существуют два типа записей: динамические и статические. Статические записи создаются вручную с помощью утилиты arp и не имеют срока устаревания. **Динамические записи** должны периодически обновляться. Если запись не обновлялась в течение определенного времени, то она исключается из таблицы. Таким образом, в ARP-таблице

Таблица 14.5. Пример ARP-таблицы

IP-адрес	MAC-адрес	Тип записи
194.85.135.65	00E0F77F1920	Динамический
194.85.135.75	008048EB7E60	Динамический
194.85.60.21	008048EB7567	Статический

Таблица 14.3. Пример ARP-запроса

Поле	Значение
Тип сети	1 (0x1)
Тип протокола	2048 (0x800)
Длина локального адреса	6 (0x6)
Длина сетевого адреса	4 (0x4)
Операция	1 (0x1)
Локальный адрес отправителя	008048EB7E60
Сетевой адрес отправителя	194.85.135.75
Локальный (искомый) адрес получателя	000000000000
Сетевой адрес получателя	194.85.135.65

Таблица 14.4. Пример ARP-ответа

Поле	Значение
Тип сети	1 (0x1)
Тип протокола	2048 (0x800)
Длина локального адреса	6 (0x6)
Длина сетевого адреса	4 (0x4)
Операция	2 (0x1)
Локальный адрес отправителя	00E0F77F1920
Сетевой адрес отправителя	194.85.135.65
Локальный (искомый) адрес получателя	008048EB7E60
Сетевой адрес получателя	194.85.135.75

Другой способ разрешения адресов используется в глобальных сетях, в которых не поддерживается широковещательная рассылка. Здесь администратору сети чаще всего приходится вручную формировать и помещать на какой-либо сервер ARP-таблицы.

- При включении каждый узел и маршрутизатор регистрируют свой адрес в выделенном маршрутизаторе. Всякий раз, когда возникает необходимость определения по IP-адресу локального адреса, модуль ARP обращается к выделенному маршрутизатору с запросом и автоматически получает ответ без участия администратора. **Работающий таким образом маршрутизатор называют ARP-сервером.**
- В некоторых случаях возникает обратная задача — нахождение IP-адреса по известному локальному адресу. **Тогда в действие вступает реверсивный протокол разрешения адресов (Reverse Address Resolution Protocol, RARP).**

Система DNS

Пространство DNS-имен

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей.

Дерево имен начинается с **корня**, обозначаемого здесь точкой. Затем следуют **старшая символьная часть имени**, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует **конечному узлу сети**. В отличие от имен файлов, при записи которых сначала указывается самая старшая составляющая, затем составляющая более низкого уровня и т. д., **запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей**. Составные части доменного имени отделяются друг от друга точкой.

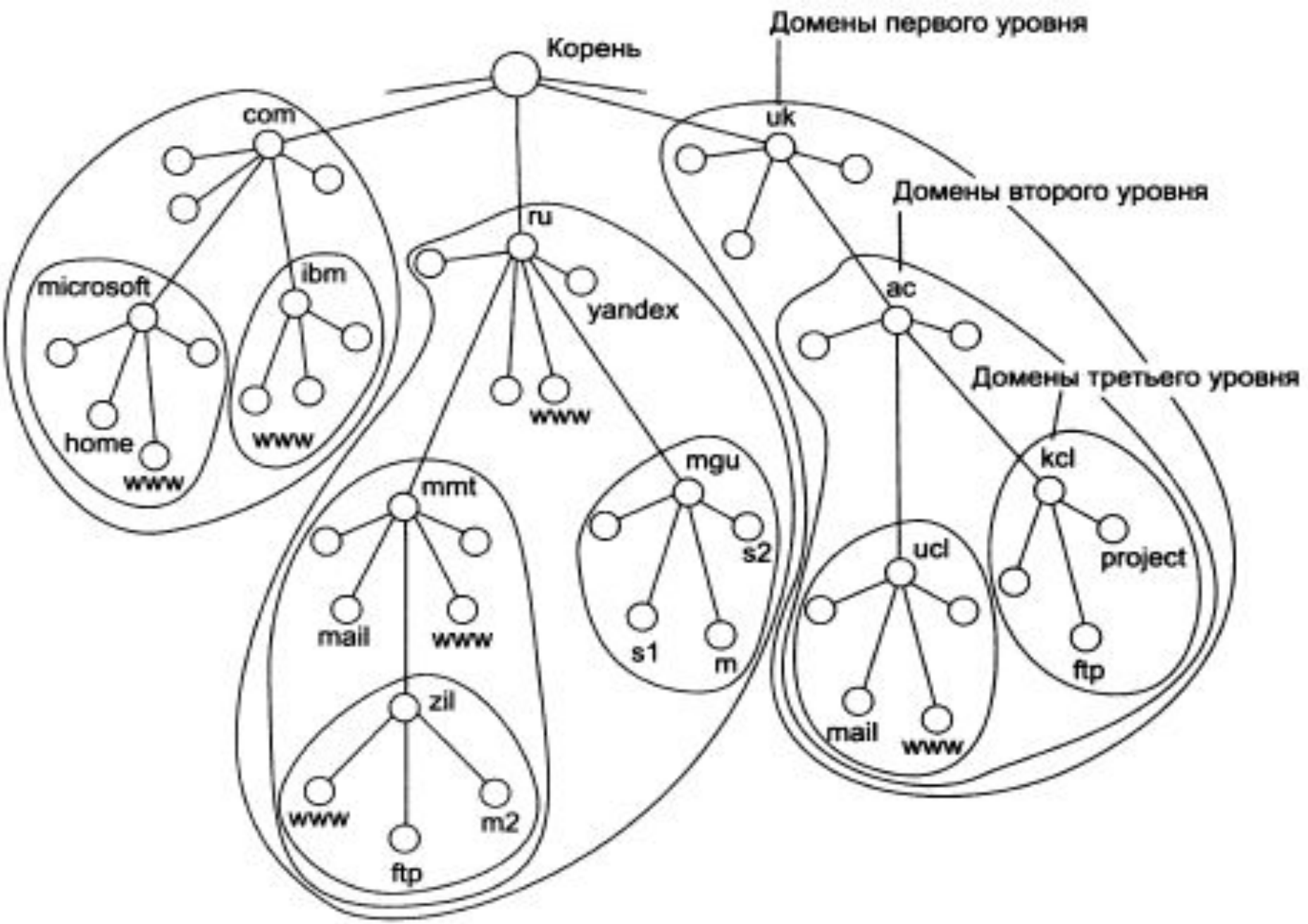

Рис. 14.10. Пространство доменных имен

Домены первого уровня

Разделение административной ответственности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии. **Совокупность имен, у которых несколько старших составных частей совпадают, образует домен имен (domain).**

Иерархическая организация службы DNS

Служба DNS имеет иерархическую структуру. Иерархию образуют DNS-серверы, которые поддерживают распределенную базу отображений, а **DNS-клиенты обращаются к серверам с запросами об отображении доменного имени на IP-адрес.**

Запросы к DNS-серверам и их ответы обслуживаются протоколом DNS, что позволяет клиенту делать запросы относительно некоторого доменного имени, либо задавая тип записи, либо запрашивая все типы, относящиеся к данному имени.

При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Вершину иерархии серверов DNS составляют **корневые серверы**, они хранят файлы отображений DNS-серверов следующего уровня, называемого верхним (top level DNS).

Разделение пространства имен между серверами

Пространство доменных имен «разрезают» между DNS-серверами обычно так, чтобы сервер хранил записи только в пределах одного уровня, а для имен своих поддоменов хранил только ссылки на DNS-серверы, отвечающие за эти поддомены.

Часть пространства доменных имен, для которых DNS-сервер имеет полную информацию об их отображениях на основе соответствующего текстового файла, называется **зоной DNS**, а сам текстовый файл — **файлом зоны**. Когда DNS-сервер дает ответ о записи, входящей в зону, за которую он отвечает, такой ответ называется **полномочным (authoritative) ответом DNS**.

Файл зоны состоит из текстовых записей нескольких типов, таких как:

- A — отображает имя на IPv4-адрес;
- AAAA — отображает имя на IPv6-адрес;
- NS — определяет имя DNS-сервера для некоторого домена;
- MS — определяет имя почтового сервера для некоторого домена.

Рекурсивная и нерекурсивная процедуры

Существуют две основные схемы разрешения DNS-имен. В первом варианте работу попоиску IP-адреса координирует DNS-клиент:

- **DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени.**
- **DNS-сервер отвечает клиенту, указывая адрес следующего DNS-сервера**, обслуживающего домен верхнего уровня, заданный в следующей старшей части запрошенного имени.
- **DNS-клиент делает запрос следующего DNS-сервера**, который отсылает его к DNS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится отображение запрошенного имени на IP-адрес. Этот сервер дает окончательный ответ клиенту.

Такая процедура разрешения имени называется **нерекурсивной** — в этом случае клиент сам итеративно выполняет последовательность запросов к разным серверам имен.

Во втором варианте реализуется **рекурсивная процедура:**

- **DNS-клиент запрашивает локальный DNS-сервер,** то есть тот сервер, обслуживающий поддомен, которому принадлежит имя клиента.

Далее возможны два варианта действий:

- **если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту;**
- **если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д.**, а получив ответ, передает его клиенту, который все это время ждет его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему серверу, именно поэтому схема называется **рекурсивной**, или косвенной.

DNS-серверы стараются не поддерживать

Корневые серверы

Корневые серверы — наиболее уязвимое звено службы DNS, так как разрешение всех запросов, ответы на которые не находятся в кэше или файле зоны какого-либо DNS-сервера нижнего уровня, начинаются с обращения к одному из корневых серверов.

Использование произвольной рассылки

Пусть имеется некоторая группа DNS-серверов, предоставляющих клиентам идентичные услуги. В соответствии с технологией произвольной рассылки всем серверам группы должен быть присвоен один и тот же IP-адрес, который в данной ситуации интерпретируется как адрес произвольной рассылки. При отправке запроса к серверам группы клиент выбирает в соответствии с правилами предпочтения один из маршрутов (серверов). В случае службы DNS клиент обычно выбирает ближайший сервер.

Использование в службе DNS техники произвольной рассылки сулит несколько потенциальных преимуществ:

- **повышение производительности за счет распараллеливания нагрузки на серверы (баланс нагрузки);**
- **повышение надежности за счет «горячего» резервирования серверов**, когда любой сервер может выполнить запрос клиента;
- **защита от DDoS/DoS-атак.**


Карта
Спутник
Гибрид
Letter: K
Operator: RIPE NCC
IPv4: 193.0.14.129
ASN: 25152
Location: Novosibirsk, RU
Type: Local
Legend
Multiple instances
Single instance
Google

Использование произвольной рассылки

В DNS-службе техника произвольной рассылки используется для рационализации взаимодействия клиента и серверов.

Пусть имеется некоторая группа DNS-серверов, предоставляющих клиентам идентичные услуги. В соответствии с технологией произвольной рассылки **всем серверам группы должен быть присвоен один IP-адрес,** который интерпретируется как **адрес произвольной рассылки**. Кроме того, должны быть найдены маршруты от DNS-клиента до каждого из серверов группы. **При отправке запроса к серверам группы клиент выбирает в соответствии с некоторыми правилами предпочтения один из маршрутов.** В случае службы DNS клиент обычно выбирает ближайший сервер.

Использование техники произвольной рассылки сулит обеспечивает:

- **повышение производительности за счет распараллеливания нагрузки на серверы (баланс нагрузки);**
- **повышение надежности за счет «горячего» резервирования серверов, когда любой сервер может выполнить запрос клиента;**
- **защиту от DDoS/DoS-атак**

Обратная зона

Служба DNS предназначена не только для нахождения IP-адреса по имени хоста, но и для решения обратной задачи — нахождения DNS-имени по известному IP-адресу.

Обратная запись не всегда существует даже для тех адресов, для которых есть прямые записи. Обратная задача решается в Интернете путем организации так называемых **обратных зон.**

Обратная зона — это система таблиц, которая хранит соответствие между IP-адресами и DNS-имена хостов некоторой сети.

Первый этап преобразования заключается в том, что **составляющие IP-адреса интерпретируются как составляющие DNS-имени**.

Далее, учитывая, что при записи IP-адреса старшая часть является самой левой частью адреса, а при записи DNS-имени — самой правой, то **составляющие в преобразованном адресе указываются в обратном порядке**.

Для хранения отображений всех адресов, начинающихся, например, с числа 192, заводится зона 192 со своими серверами имен. Для записей о серверах, поддерживающих старшие в иерархии обратные зоны, создана специальная зона in-addr.arpa:

106.31.192.in-addr.arpa.

Протокол DHCP

Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, гарантируя от дублирования адресов за счет централизованного управления их распределением.

Режимы DHCP

Протокол DHCP работает в соответствии с моделью клиент-сервер. **Во время старта системы компьютер, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфигурационные параметры.**

При этом DHCP-сервер может работать в разных режимах, включая:

- **ручное назначение статических адресов;**
- **автоматическое назначение статических адресов**

- **В ручном режиме администратор помимо пула доступных адресов снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов**. DHCP-сервер, пользуясь этой информацией, всегда выдаст определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес.
- **В режиме автоматического назначения статических адресов DHCP-сервер самостоятельно**, без вмешательства администратора, произвольным образом **выбирает** клиенту **IP-адрес из пула наличных IP-адресов**. Адрес дается клиенту из пула в постоянное пользование, то есть между идентифицирующей информацией клиента и его IP-адресом существует постоянное соответствие.
- **При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды.** Это дает

Алгоритм динамического назначения адресов

Администратор управляет процессом конфигурирования сети, определяя два основных конфигурационных параметра DHCP-сервера: **пул адресов, доступных распределению, и срок аренды**. Срок аренды диктует, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его у DHCP-сервера. Срок аренды зависит от режима работы пользователей сети.

DHCP-поиск

DHCP-сервер должен находиться в одной подсети с клиентами, учитывая, что клиенты посылают ему широковещательные запросы (рис. 14.12). Для снижения риска выхода сети из строя из-за отказа DHCP-сервера в сети иногда ставят резервный DHCP-сервер (такой вариант соот

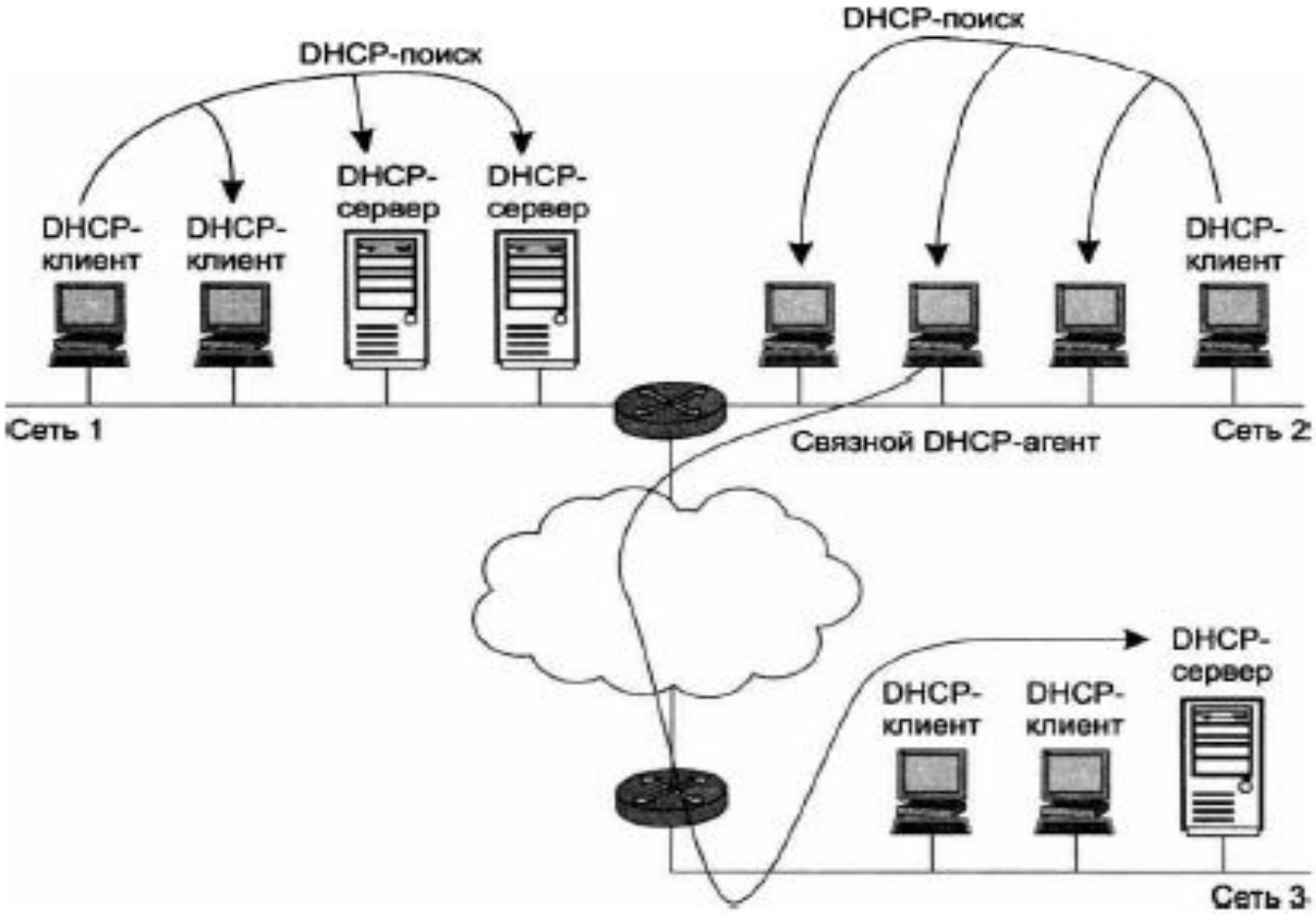

Рис. 14.12. Схемы взаимного расположения DHCP-серверов и DHCP-клиентов

Вот как выглядит упрощенная схема обмена:

- Когда компьютер включают, установленный на нем **DHCP-клиент посылает ограниченное широковещательное сообщение DHCP-поиска**.
- Находящиеся в сети DHCP-серверы получают это сообщение. Если в сети DHCP-серверы отсутствуют, то с**ообщение DHCP-поиска получает связной DHCP-агент**.
- **Все DHCP-серверы**, получившие сообщение DHCP-поиска, **посылают DHCP-клиенту**, обратившемуся с запросом, **свои DHCP-предложения**.
- **DHCP-клиент собирает конфигурационные DHCP-предложения от всех DHCP-серверов.** В нём содержатся идентификационная информация о DHCP-сервере, предложение которого принято, а также значения принятых конфигурационных параметров.
- **Все DHCP-серверы получают DHCP-запрос, и только один выбранный DHCP-сервер посылает положительную DHCP-квитанцию, а остальные серверы аннулируют свои предложения.**
- **DHCP-клиент получает положительную DHCP-квитанцию и переходит в рабочее состояние.**

В сети, где адреса назначаются динамически, нельзя быть уверенным в адресе, который в данный момент имеет тот или иной узел. И такое непостоянство IP-адресов влечет за собой некоторые проблемы:

- Во-первых, **возникают сложности при преобразовании символьного доменного имени в IP- адрес**.
- Во-вторых, **трудно осуществлять удаленное управление и автоматический мониторинг интерфейса** (например, сбор статистики), если в качестве его идентификатора выступает динамически изменяемый IP-адрес.
- Наконец, для обеспечения безопасности сети многие **сетевые устройства могут блокировать (фильтровать) пакеты,** определенные поля которых имеют некоторые заранее заданные значения.

Спасибо за внимание!