Глава 8

Налаживаем взаимодействие между компьютерами: настройка IP-адресации и маршрутизации

В этой главе вы найдете ответы на следующие вопросы:

- ***Что такое IP-адрес, маска подсети, основной шлюз?***
- ***Как работает IP-маршрутизация?***
- ***Как «читать» таблицу маршрутизации?***
- ***Как маршрутизаторы обмениваются таблицами маршрутизации?***
- ***Как назначать IP-адреса компьютерам в сети?***
- ***Как проверить работоспособность протокола IP?***

Итак, мы выбрали набор протоколов TCP/IP и установили его (инсталлировали соответствующее программное обеспечение). Заметим, что в современных операционных системах этот протокол устанавливается по умолчанию; более того, удалить его, например, из Windows XP или Windows Server 2003 обычным способом невозможно (кнопка **Удалить** в свойствах сетевых подключений неактивна).

К сожалению, одной только установки протокола TCP/IP будет недостаточно. Стек не заработает, пока в нашей сети не будет правильным образом настроена *IP-адресация* и *маршрутизация*. (Опять сравним работу сети с работой почты: как сможет почтальон доставить письмо адресату, если дороги и транспорт хотя и работают, но на домах нет номеров, а почтовые отделения не знают, как пересылать письма из одного города в другой?)

Поэтому сейчас мы должны узнать, что такое *IP-адрес* и *маска подсети*, выяснить, как оба этих параметра используются для определения *локальных* или *удаленных IP-сетей*, и на конкретных примерах ознакомиться с тем, как компьютеры и маршрутизаторы *доставляют IP-пакеты* из одной сети в другую.

IP v6

Многие активно развивающиеся в техническом отношении страны (Китай, Япония, Корея и др.) начинают испытывать дефицит IP-адресов, идентифицирующих не только компьютеры, но и другие устройства с функциями доступа в Интернет. Принятый сейчас 32-битовый стандарт обеспечивает количество IP-адресов, равное почти 4,3 млрд., но их большая часть закреплена за США (около 70%), Канадой и европейскими странами, а вот, например, КНР получила их всего 22 млн.

Новая, 128-разрядная версия протокола IP v.6 позволит увеличить количество IP-адресов до огромной величины — $3{,}4 \times 10^{38}$.

Протокол IP v6 — в Windows XP

Для использования протокола IPv6 в Windows XP имеется необходимое программное обеспечение, которое, однако, по умолчанию не активизировано. Чтобы задействовать новый протокол, достаточно в командной строке (меню **Пуск**, **Выполнить**) ввести и запустить на исполнение команду `ipv6 install`.

Получить необходимые справки по работе с протоколом IPv6 можно (после его инсталляции) командой `ipv6 /?`.

Основы IP-адресации

Первым обязательным параметром в свойствах протокола TCP/IP любого компьютера является его IP-адрес.

IP-адрес — это уникальная 32-разрядная последовательность двоичных цифр, с помощью которой компьютер *однозначно идентифицируется* в IP-сети. (Напомним, что на канальном уровне в роли таких же уникальных адресов компьютеров выступают MAC-адреса сетевых адаптеров, невозможность совпадения которых контролируется изготовителями на стадии производства.)

В этой главе будет обсуждаться наиболее распространенная версия 4 протокола IP, или *IPv4*. Однако уже создана следующая версия протокола — *IP версии 6* (*IPv6*), в которой IP-адрес представляется в виде 128-битной последовательности двоичных цифр. Эта версия протокола IP пока еще не получила широкого распространения, хотя и поддерживается многими современными маршрутизаторами и операционными системами (например, Windows XP или Windows Server 2003).

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 битов (на *октеты*), каждый октет переводят в десятичное число и при записи разделяют эти числа точками. В таком виде (это представление называется «десятичные числа с точками», или, по-английски, «*dotted-decimal notation*») IP-адреса занимают гораздо меньше места и намного легче запоминаются (табл. 8.1).

Таблица 8.1

Различные представления IP-адреса

IP-адрес в 32-разрядном виде	11000000 10101000 0000101 11001000			
IP-адрес, разбитый на октеты	11000000	10101000	00000101	11001000
Октеты в десятичном представлении	192	168	5	200
IP-адрес в виде десятичных чисел, разделенных точками	192.168.5.200			

Чтобы быстро осуществлять подобное преобразование в уме (что сетевым администраторам требуется нередко, а калькулятор не всегда под рукой), полезно запомнить следующую таблицу. В ней приведены десятичные значения степеней числа 2 с показателем, равным порядковому номеру бита в октете (напомним — нумерация битов производится справа налево и начинается с нуля):

Порядковый номер бита в октете	7	6	5	4	3	2	1	0
2 в степени, соответствующей номеру бита	128	64	32	16	8	4	2	1

Запомнив такую таблицу, несложно в уме преобразовывать октеты в десятичные числа и обратно.

Десятичное число легко вычисляется как *сумма цифр, соответствующих ненулевым битам в октете*, например:

$$\mathbf{10101101} \rightarrow \mathbf{128 \cdot 1} + 64 \cdot 0 + \mathbf{32 \cdot 1} + 16 \cdot 0 + \mathbf{8 \cdot 1} + \\ + \mathbf{4 \cdot 1} + 2 \cdot 0 + \mathbf{1 \cdot 1} = 173.$$

Несколько сложнее перевести десятичное представление в двоичное, но при некоторой тренировке это также не представляет проблем. Например:

$$201 \rightarrow \mathbf{128 \cdot 1} + \mathbf{64 \cdot 1} + 32 \cdot 0 + 16 \cdot 0 + \mathbf{8 \cdot 1} + 4 \cdot 0 + \\ + 2 \cdot 0 + \mathbf{1 \cdot 1} = \mathbf{11001001}.$$

Однако одного только IP-адреса компьютеру для работы в сети TCP/IP недостаточно. Вторым обязательным параметром, без которого протокол TCP/IP работать не будет, является *маска подсети*.

Маска подсети — это 32-разрядное число, состоящее из идущих вначале единиц, а затем — нулей, например (в десятичном представлении) `255.255.255.0` или `255.255.240.0`.

Маска подсети играет исключительно важную роль в IP-адресации и маршрутизации. Чтобы понять значение этого параметра, вспомним, что сеть ARPANet строилась как набор соединенных друг с другом гетерогенных сетей. Для правильного взаимодействия в такой сложной сети каждый участник должен уметь определять, какие IP-адреса принадлежат его *локальной* сети, а какие — *удаленным* сетям.

Здесь и используется маска подсети, с помощью которой производится *разделение любого IP-адреса* на две части: *идентификатор сети* (*Net ID*) и *идентификатор узла* (*Host ID*). Такое разделение делается очень просто: там, где в маске подсети стоят единицы, находится идентификатор сети, а где стоят нули — идентификатор узла.

Например, в IP-адресе `192.168.5.200` при использовании маски подсети `255.255.255.0` идентификатором сети будет число `192.168.5.0`, а идентификатором узла — число `200`. Стоит нам поменять маску подсети, скажем, на число `255.255.0.0`, как и идентификатор узла, и идентификатор сети изменятся на `192.168.0.0` и `5.200`, соответственно, и от этого, как мы дальше увидим, иначе будет вести себя компьютер при посылке IP-пакетов.

Правила назначения IP-адресов сетей и узлов

Теперь, когда мы знаем, что такое IP-адрес, маска подсети, идентификаторы сети и узла, полезно запомнить **правила, которые следует применять при назначении этих параметров:**

1) идентификатор сети не может содержать только двоичные нули или только единицы. Например, адрес `0.0.0.0` не может являться идентификатором сети;
2) идентификатор узла также не может содержать только двоичные нули или только единицы — такие адреса зарезервированы для специальных целей:
   - все нули в идентификаторе узла означают, что этот адрес является *адресом сети*. Например, `192.168.5.0` является правильным адресом сети при использовании маски `255.255.255.0` и его нельзя использовать для адресации компьютеров,
   - все единицы в идентификаторе узла означают, что этот адрес является *адресом широковещания* для данной сети. Например, `192.168.5.255` является адресом широковещания в сети `192.168.5.0` при использовании маски `255.255.255.0` и его нельзя использовать для адресации компьютеров;
3) идентификатор узла в пределах одной и той же подсети должен быть уникальным;
4) диапазон адресов от `127.0.0.1` до `127.255.255.254` нельзя использовать в качестве IP-адресов компьютеров. Вся сеть `127.0.0.0` по маске `255.0.0.0` зарезервирована под так называемый *«адрес заглушки»* (*loopback*), используемый в IP для обращения компьютера к самому себе.

Это легко проверить: достаточно на любом компьютере с установленным протоколом TCP/IP выполнить команду

```
PING 127.12.34.56
```

и, если протокол TCP/IP работает, вы увидите, как ваш компьютер будет отвечать на собственные запросы.

Классовая и бесклассовая IP-адресация

Первоначальная система IP-адресации в Интернете выглядела следующим образом. Все пространство возможных IP-адресов (а это более четырех миллиардов, точнее 4 294 967 296 адресов) было разбито на пять *классов*, причем принадлежность IP-адреса к определенному классу определялась по нескольким битам первого октета (табл. 8.2). Заметим, что для адресации сетей и узлов использовались только классы A, B и C. Кроме того, для этих сетей были определены *фиксированные маски подсети по умолчанию*, равные, соответственно, `255.0.0.0`, `255.255.0.0` и `255.255.255.0`, которые не только жестко определяли диапазон возможных IP-адресов узлов в таких сетях, но и механизм маршрутизации.

Таблица 8.2

Классы адресов в первоначальной схеме IP-адресации

Класс	Первые биты в октете	Возможные значения первого октета	Возможное число сетей	Возможное число узлов в сети
A	0	1–126	126	16777214
B	10	128–191	16384	65534
C	110	192–223	2097152	254
D	1110	224–239	Используется для многоадресной рассылки (multicast)	
E	1111	240–254	Зарезервирован как экспериментальный	

Чтобы рассчитать максимально возможное количество узлов в любой IP-сети, достаточно знать, сколько битов содержится в идентификаторе узла, или, иначе, сколько нулей имеется в маске подсети. Это число используется в качестве показателя степени двойки, а затем из результата вычитается два зарезервированных адреса (сети и широковещания). Аналогичным способом легко вычислить и возможное количество сетей классов A, B или C, если учесть, что первые биты в октете уже зарезервированы, а в классе A нельзя использовать IP-адреса `0.0.0.0` и `127.0.0.0` для адресации сети.

Распределением IP-адресов в мире занимается частная некоммерческая корпорация под названием ICANN (Internet Corporation for Assigned Names and Numbers), а точнее, работающая под ее патронажем организация IANA (Internet Assigned Numbers Authority).

Для получения нужного диапазона IP-адресов организациям предлагалось заполнить регистрационную форму, в которой следовало указать текущее число компьютеров и планируемый рост компьютерного парка в течение двух лет.

Первоначально данная схема хорошо работала, поскольку количество сетей было небольшим. Однако с развитием Интернета такой подход к распределению IP-адресов стал вызывать проблемы, особенно острые для сетей класса B. Действительно, организациям, в которых число компьютеров не превышало нескольких сотен (скажем, 500), приходилось регистрировать для себя целую сеть класса B. Поэтому количество доступных сетей класса B стало на глазах «таять», но при этом громадные диапазоны IP-адресов (в нашем примере — более 65000) пропадали зря.

Чтобы решить проблему, была разработана *бесклассовая схема IP-адресации* (*Classless InterDomain Routing*, *CIDR*), в которой не только отсутствует привязка IP-адреса к классу сети и маске подсети по умолчанию, но и допускается применение так называемых *масок подсети с переменной длиной* (*Variable Length Subnet Mask*, *VLSM*). Например, если при выделении сети для вышеуказанной организации с 500 компьютерами вместо фиксированной маски `255.255.0.0` использовать маску `255.255.254.0`,

то получившегося диапазона из 512 возможных IP-адресов будет вполне достаточно. Оставшиеся 65 тысяч адресов можно зарезервировать на будущее или раздать другим желающим подключиться к Интернету.

Этот подход позволил гораздо более эффективно выделять организациям нужные им диапазоны IP-адресов, и проблема с нехваткой IP-сетей и адресов стала менее острой.

IP-адреса для локальных сетей

Все используемые в Интернете адреса, как мы уже говорили, должны регистрироваться в IANA, что гарантирует их уникальность в масштабе всей планеты. Такие адреса называют *реальными*, или *публичными* (*public*) *IP-адресами*.

Для локальных сетей, не подключенных к Интернету, регистрация IP-адресов, естественно, не требуется, так что, в принципе, здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к Интернету, RFC 1918 рекомендует применять в локальных сетях только следующие диапазоны так называемых *частных* (*private*) *IP-адресов* (в Интернете эти адреса не существуют и использовать их там нет возможности):

- `10.0.0.0` — `10.255.255.255`;
- `172.16.0.0` — `172.31.255.255`;
- `192.168.0.0` — `192.168.255.255`.

Основы IP-маршрутизации

Как уже говорилось, чтобы правильно взаимодействовать с другими компьютерами и сетями, каждый компьютер определяет, какие IP-адреса принадлежат его локальной сети, а какие — удаленным

сетям. Если выясняется, что IP-адрес компьютера назначения принадлежит локальной сети, пакет посылается непосредственно компьютеру назначения, если же это адрес удаленной сети, то пакет посылается по адресу основного шлюза.

Рассмотрим этот процесс подробнее. Возьмем компьютер со следующими параметрами протокола IP:

- IP-адрес — `192.168.5.200`;
- маска подсети — `255.255.255.0`;
- основной шлюз — `192.168.5.1`.

При запуске протокола IP на компьютере выполняется *операция логического «И» между его собственными IP-адресом и маской подсети*, в результате которой все биты IP-адреса, соответствующие нулевым битам маски подсети, также становятся нулевыми:

- IP-адрес в 32-разрядном виде — `11000000 10101000 00000101 11001000`;
- маска подсети — `11111111 11111111 11111111 00000000`;
- идентификатор сети — `11000000 10101000 00000101 00000000`.

Эта простая операция позволяет компьютеру определить *идентификатор собственной сети* (в нашем примере — `192.168.5.0`).

Теперь предположим, что компьютеру надо отправить IP-пакет по адресу `192.168.5.15`. Чтобы решить, как это нужно сделать, компьютер выполняет *операцию логического «И» с IP-адресом компьютера назначения и собственной маской подсети*. Легко понять, что полученный в результате *идентификатор сети назначения* будет совпадать с идентификатором собственной сети компьютера-отправителя. Так наш компьютер определит, что компьютер назначения находится в одной с ним сети, и выполнит следующие операции:

- с помощью протокола ARP будет определен физический MAC-адрес, соответствующий IP-адресу компьютера назначения;
- с помощью протоколов канального и физического уровня по этому MAC-адресу будет послана нужная информация.

Теперь посмотрим, что изменится, если пакет надо отправить по адресу `192.168.10.20`. Компьютер выполнит аналогичную процедуру определения идентификатора сети назначения. В результате будет получен адрес `192.168.10.0`, не совпадающий с идентификатором сети компьютера-отправителя. Так будет установлено, что компьютер назначения находится в удаленной сети, и алгоритм действий компьютера-отправителя изменится:

- будет определен MAC-адрес не компьютера назначения, а маршрутизатора;
- с помощью протоколов канального и физического уровня по этому MAC-адресу на маршрутизатор будет послана нужная информация.

Несмотря на то, что IP-пакет в этом случае не доставляется непосредственно по назначению, протокол IP на компьютере-отправителе считает свою задачу выполненной (вспомните, что и мы при отправке письма всего лишь бросаем его в почтовый ящик). Дальнейшая судьба IP-пакета зависит от правильной настройки маршрутизаторов, объединяющих сети `192.168.5.0` и `192.168.10.0`.

Кстати, в данном примере легко продемонстрировать, насколько важна правильная настройка маски подсети в параметрах IP-адресации. Пусть мы по ошибке указали для компьютера `192.168.5.200` маску подсети, равную `255.255.0.0`. В этом случае при попытке послать пакет по адресу `192.168.10.20` наш компьютер посчитает, что компьютер назначения находится в его собственной сети (ведь идентификаторы сетей при такой маске совпадают!), и будет пытаться отправить пакет самостоятельно.

В итоге этот пакет не попадет в маршрутизатор и не будет доставлен по назначению.

Чтобы понять, как работают маршрутизаторы, давайте сначала проанализируем *таблицу маршрутов*, которую выстраивает при загрузке протокола IP обычный компьютер, например, с операционной системой Windows XP (рис. 8.1).

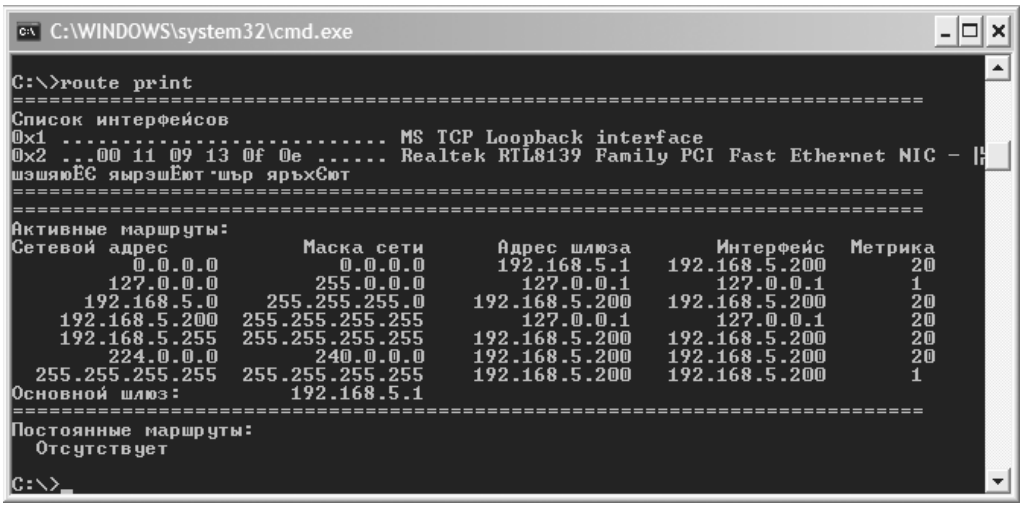


Рис. 8.1. Таблица маршрутов в ОС Windows XP

Как нетрудно видеть, в таблице определено несколько маршрутов с разными параметрами. Читать каждую такую запись в таблице маршрутизации нужно следующим образом:

> *Чтобы доставить пакет в сеть с адресом из поля* ***Сетевой адрес*** *и маской из поля* ***Маска сети****, нужно с интерфейса с IP-адресом из поля* ***Интерфейс*** *послать пакет по IP-адресу из поля* ***Адрес шлюза****, а «стоимость» такой доставки будет равна числу из поля* ***Метрика****.*

Отметим, что параметры **Сетевой адрес** и **Маска сети** вместе задают диапазон всех разрешенных в данной сети IP-адресов. Например, 127.0.0.0 и 255.0.0.0, как мы уже говорили, означают любой IP-адрес от 127.0.0.1 до 127.255.255.254. Вспомним также, что IP-адрес 127.0.0.1 называется «адресом заглушки» — посланные по этому адресу пакеты должны обрабатываться самим компьютером. Кроме того, маска 255.255.255.255 означает сеть из одного IP-адреса, а комбинация 0.0.0.0 — любой неопределенный адрес или маску подсети.

Тогда первая строка в таблице маршрутизации означает в точности то, что делает компьютер при необходимости послать пакет в удаленную, т. е. неизвестную ему из таблицы маршрутизации, сеть — со своего интерфейса пакет посылается на IP-адрес маршрутизатора.

Вторая строка таблицы заставляет компьютер посылать самому себе (и отвечать на них) все пакеты, отправленные по любому IP-адресу из диапазона 127.0.0.1 — 127.255.255.254.

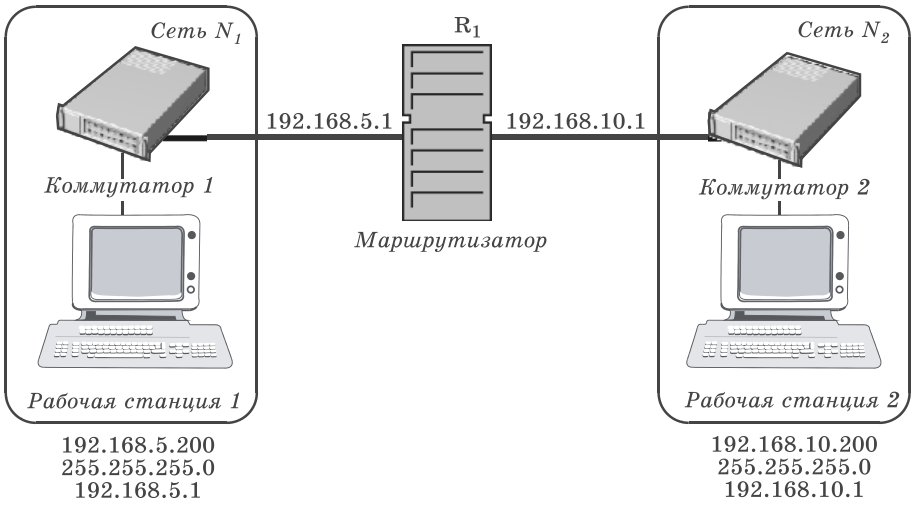
В третьей строке определено, как посылать пакеты компьютерам локальной сети (по адресам из диапазона 192.168.5.1 — 192.168.5.254). Здесь четко видно, что делать это должен сам компьютер — адресом шлюза является его собственный IP-адрес 192.168.5.200.

Аналогично (пятая, шестая и седьмая строки таблицы) нужно поступать и в случае, когда пакеты направляются по адресу рассылки подсети (192.168.5.255), по адресам многоадресной рассылки (224.0.0.0) или по адресу локальной широковещательной рассылки (255.255.255.255).

Четвертая же строка означает, что пакеты, посланные по IP-адресу 192.168.5.200 (обратите внимание на маску!), должны обрабатываться самим компьютером.

Несколько сложнее будет выглядеть таблица маршрутизации компьютера с двумя сетевыми адаптерами, который мы будем использовать в качестве маршрутизатора для объединения двух сегментов небольшой сети (рис. 8.2).

а)



б)

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.5.0    255.255.255.0      192.168.5.1     192.168.5.1      20
      192.168.5.1  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.5.255  255.255.255.255      192.168.5.1     192.168.5.1      20
     192.168.10.0    255.255.255.0      192.168.10.1    192.168.10.1     20
     192.168.10.1  255.255.255.255        127.0.0.1       127.0.0.1      20
   192.168.10.255  255.255.255.255      192.168.10.1    192.168.10.1     20
        224.0.0.0        240.0.0.0      192.168.5.1     192.168.5.1      20
        224.0.0.0        240.0.0.0      192.168.10.1    192.168.10.1     20
  255.255.255.255  255.255.255.255      192.168.5.1     192.168.5.1       1
  255.255.255.255  255.255.255.255      192.168.10.1    192.168.10.1      1
===========================================================================
```

Рис. 8.2. Объединение сети с помощью маршрутизатора (*а*) и таблица маршрутизации компьютера R_1 (*б*)

В этой таблице появилось несколько дополнительных строк, обозначающих маршруты в обе сети — `192.168.5.0` и `192.168.10.0`. Заметим, что все такие маршруты будут выстроены компьютером автоматически.

Чтобы после этого наладить *обмен IP-пакетами между сетями*, нужно выполнить следующие действия:

- включить маршрутизацию на компьютере R_1 — это можно сделать, например, настроив службу маршрутизации и удаленного доступа, входящую в состав операционной системы Windows Server 2003;
- на всех компьютерах в сети N_1 параметр **Основной шлюз** нужно установить равным IP-адресу интерфейса маршрутизатора, подключенного к этой сети, т. е. равным `192.168.5.1`, а на компьютерах в сети N_2 — равным `192.168.10.1`.

Таким образом, маршрутизатор — это программно-аппаратное устройство с несколькими сетевыми интерфейсами, на котором работает *служба маршрутизации*.

Усложним нашу сеть, добавив в нее второй маршрутизатор и сеть N_3 с адресом `192.168.15.0` (рис. 8.3).

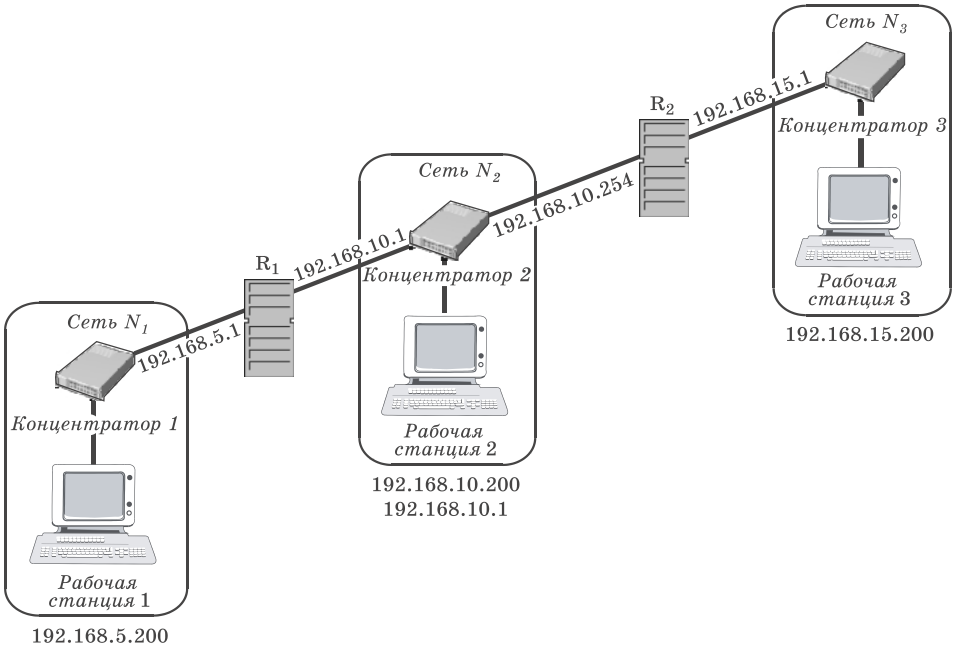


Рис. 8.3. Сеть с двумя маршрутизаторами

В такой сети настройка маршрутизации усложняется. Проблема в том, что, хотя маршрутизатор R_1 «знает», как посылать пакеты в сети N_1 и N_2, маршрута в сеть N_3 у него нет. В свою очередь, у маршрутизатора R_2 отсутствует маршрут в сеть N_1. Значит, обмен IP-пакетами между сетями N_1 и N_3 будет невозможен.

Решить эту проблему в такой небольшой сети довольно просто — надо добавить нужные записи в таблицы маршрутизаторов R_1 и R_2. Для этого на маршрутизаторе R_1 достаточно выполнить команду, предписывающую направлять все пакеты, предназначенные для сети `192.168.15.0`, по адресу `192.168.10.254` (т. е. второму маршрутизатору, который уже сможет доставить эти пакеты по назначению; ключ `P` здесь используется, чтобы сделать этот маршрут постоянным):

```
ROUTE –P ADD 192.168.15.0
      MASK 255.255.255.0 192.168.10.254
```

В качестве IP-адреса маршрутизатора принято выбирать либо первый, либо последний из возможных в данной IP-сети адресов.

Аналогичная команда на маршрутизаторе R_2 должна выглядеть так:

```
ROUTE –P ADD 192.168.5.0
       MASK 255.255.255.0 192.168.10.1
```

После этого взаимодействие в нашей сети будет налажено.

В крупных сетях, содержащих большое количество соединенных друг с другом подсетей, вручную прописывать маршруты доставки пакетов на всех маршрутизаторах довольно утомительно. К тому же такие маршруты являются *статическими*, значит, при каждом изменении конфигурации сети нужно будет проделывать большую работу по перестройке системы IP-маршрутизации.

Чтобы избежать этого, достаточно настроить маршрутизаторы так, чтобы они *обменивались друг*

с другом информацией о маршрутах. Для этого в локальных сетях используют такие протоколы, как *RIP* (*Routing Information Protocol*) и *OSPF* (*Open Shortest Path First*). Протокол RIP проще в настройке, чем OSPF, однако для обмена информацией в нем применяются широковещательные сообщения, заметно нагружающие сеть. Поэтому RIP обычно используют в относительно небольших сетях. Протокол OSPF работает эффективнее, но сложнее настраивается, поэтому его использование рекомендуется для крупных корпоративных сетей.

Назначение IP-адресов и проверка работоспособности TCP/IP

Мы уже видели, насколько важной для взаимодействия компьютеров в сети TCP/IP является правильная настройка протокола IP. Поэтому важно обсудить, какими способами можно настраивать параметры IP на компьютерах и как быстро проверить работоспособность всей системы IP-адресации и маршрутизации.

Самый простой способ настройки параметров протокола IP — назначить их вручную. Достоинством такого метода является то, что сетевые администраторы полностью контролируют все IP-адреса компьютеров в сети, что может быть важно с точки зрения защиты данных или взаимодействия с Интернетом. Однако у этого способа много недостатков. Во-первых, легко ошибиться и ввести неправильные параметры маски или шлюза или, что еще хуже, назначить повторяющийся в сети IP-адрес. Во-вторых, при изменениях параметров IP-адресации в сети (например, при смене IP-адреса маршрутизатора) придется перенастраивать все компьютеры. Но самое неприятное, что при таком способе настройки практически невозможно работать в крупных кор-

поративных сетях с мобильными устройствами типа ноутбуков или КПК, которые часто перемещаются из одного сегмента сети в другой.

Поэтому в организациях чаще применяют специальные серверы, поддерживающие *протокол динамической конфигурации узлов* (*Dynamic Host Configuration Protocol*, *DHCP*), задача которых состоит в обслуживании запросов клиентов на получение IP-адреса и другой информации, необходимой для правильной работы в сети. Именно поэтому компьютеры с операционными системами Windows по умолчанию настроены на автоматическое получение IP-адреса.

Если сервер DHCP недоступен (отсутствует или не работает), то начиная с версии Windows 98 компьютеры самостоятельно назначают себе IP-адрес. При этом используется *механизм автоматической личной IP-адресации* (*Automatic Private IP Addressing*, *APIPA*), для которого корпорацией Microsoft в IANA был зарегистрирован диапазон адресов `169.254.0.0` — `169.254.255.255`.

Наконец, обсудим, какие шаги нужно предпринять *для проверки параметров и работоспособности протокола IP*.

1. **Выполните команду `IPCONFIG /ALL`.**

   Если в выданной на экран информации не содержится никаких параметров, значит, у вас нет активных интерфейсов.

   Если в выданной информации есть диагностическое сообщение «Сеть отключена», значит, у вас проблемы с физическим уровнем — проверьте подключение коннектора в разъеме сетевого адаптера и/или работоспособность коммутатора.

   Если ваши параметры IP-адреса и маски подсети равны `0.0.0.0`, значит, вы используете статический IP-адрес, конфликтующий с другим узлом в сети.

Если ваш IP-адрес находится в диапазоне `169.254.x.x`, значит, DHCP-сервер недоступен и работать вы сможете только с теми компьютерами в сети, которые также самостоятельно назначили себе адрес.

В нормальной ситуации при получении IP-адреса от DHCP-сервера или правильной ручной настройке вы должны увидеть в выданной на экран информации такие параметры, как IP-адрес компьютера, маска подсети, основной шлюз, DNS-сервер и DHCP-сервер (а также, возможно, другие параметры).

2. **Выполните команду `PING 127.0.0.1`.**

   Если ответ не получен, это свидетельствует о неправильной настройке стека протоколов TCP/IP; придется переустановить соответствующую программную поддержку.

   Если ответ получен, значит, стек протоколов TCP/IP работает правильно.

3. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес соседнего компьютера.**

   Так проверяется работоспособность локальной сети.

4. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес основного шлюза.**

   Так проверяется доступность и работоспособность маршрутизатора.

5. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес любого удаленного компьютера.**

   Так проверяется работоспособность всей системы маршрутизации вашей корпоративной сети или соединения с Интернетом.

Во многих современных сетях пакеты протокола ICMP, с помощью которых утилита `PING` тестирует взаимодействие, запрещаются по требованию служб безопасности. ОС Windows XP SP2 с включенным

межсетевым экраном также блокирует ICMP-пакеты. Поэтому, если утилита PING не показывает ответов, не спешите искать причину «сбоя» на своем компьютере, а сначала выясните у сетевого администратора (или в настройках своей ОС Windows XP), разрешено ли в вашей сети использование ICMP.

В заключение приведем набор кратких правил, которые помогут вам не ошибиться при настройке IP-адресации и маршрутизации в сетях TCP/IP:

1) чтобы взаимодействовать в сети TCP/IP, все компьютеры должны иметь IP-адреса;
2) компьютеры, находящиеся в одном физическом сегменте сети (соединенные концентраторами или коммутаторами), должны принадлежать одной IP-сети, но иметь уникальные IP-адреса;
3) для определения идентификаторов локальной сети или удаленных сетей используется маска подсети;
4) чтобы взаимодействовать с удаленными сетями, компьютерам требуется адрес основного шлюза, который должен совпадать с адресом маршрутизатора, соединяющего вашу сеть с другими;
5) маршрутизаторы — это компьютеры с несколькими сетевыми интерфейсами, умеющие передавать IP-пакеты из одной сети в другую в соответствии со своими таблицами маршрутизации;
6) маршрутизатор всегда имеет маршруты во все сети, подключенные к нему непосредственно; маршруты в другие сети нужно настраивать;
7) таблицы маршрутизации можно настраивать вручную либо применять динамические протоколы обмена информацией о маршрутизации.

Вопросы и задания

1. Какие параметры и настройки обязательны для обеспечения работы стека протоколов TCP/IP?
2. Что такое IP-адрес? Какова его структура? Какие возможны способы представления IP-адресов?
3. Чем отличаются версии 4 и 6 протокола IP? Какие преимущества обеспечит версия 6 протокола IP? Почему возникла необходимость в переходе на версию 6 протокола IP?
4. Что такое маска подсети? Для чего она нужна?
5. В чем заключается смысл разделения IP-адреса на идентификаторы сети и узла? Для чего это требуется?
6. Какие IP-адреса и маски являются допустимыми, а какие — нет? Почему?
7. В чем различие между классовой и бесклассовой IP-адресациями? Каковы их преимущества и недостатки?
8. Что такое классы IP-адресов? По каким правилам они определяются?
9. Как назначить IP-адреса в локальной сети (без выхода в Интернет)?
10. Каковы основные принципы маршрутизации пакетов в локальных и удаленных сетях?
11. Что такое таблица маршрутов (таблица маршрутизации)? Объясните смысл каждой из ее колонок.
12. Как «прописать» в таблице маршрутизации отсутствующий в ней новый маршрут?
13. Что такое динамическая конфигурация узлов? Для чего она нужна?
14. В чем заключается технология автоматической личной IP-адресации?
15. Каков типовой алгоритм проверки работоспособности протокола IP?