Министерство образования и науки Российской Федерации
ФГАОУ ВПО «Российский государственный
профессионально-педагогический университет»

Н. В. Ломовцева, Л. В. Волкова

IP-АДРЕСАЦИЯ

Учебное пособие

2-е издание, пересмотренное и дополненное

Допущено Научно-методическим советом по информации, вычислительной технике и компьютерным технологиям Учебно-методического объединения по профессионально-педагогическому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 050501.06 – Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии)

Екатеринбург
РГППУ
2012

УДК 004.72:004.451(075.8)
ББК 3937.2я73-1
Л75

Ломовцева Н. В.

Л75 IP-адресация: учебное пособие / Н. В. Ломовцева, Л. В. Волкова. 2-е изд., пересмотр. и доп. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2012. 60 с.

ISBN 978-5-8050-0454-5

Во 2-м издании пособия (1-е издание вышло в 2008 г.) рассматриваются компоненты IP-адреса, классы IP-адресов и основы IP-адресации, ключевые концепции построения сетей на базе объединения подсетей.

Предназначено студентам профессионально-педагогических и педагогических вузов, а также учителям информатики и преподавателям профессиональных учебных заведений. Может быть использовано при преподавании дисциплин «Компьютерные коммуникации и сети» и «Вычислительные системы, сети и телекоммуникации», а также на курсах повышения квалификации преподавателей.

УДК 004.72:004.451(075.8)
ББК 3937.2я73-1

Рецензенты: кандидат физико-математических наук, профессор В. Н. Ларионов (ГОУ ВПО «Уральский государственный университет им. А. М. Горького»); кандидат технических наук, доцент А. А. Карпов (ФГАОУ ВПО «Российский государственный профессионально-педагогический университет»)

ISBN 978-5-8050-0454-5

Предисловие

Учебное пособие предназначено студентам профессионально-педагогических и педагогических вузов, а также учителям информатики и преподавателям профессиональных учебных заведений. Материал, включенный в пособие, может быть использован при преподавании дисциплин «Компьютерные коммуникации и сети» (специальность 050501 Профессиональное обучение (информатика, вычислительная техника и компьютерные технологии)), «Вычислительные системы, сети и телекоммуникации» (специальность 080801 Прикладная информатика (по областям)), а также в целях повышения квалификации преподавателей.

Данное учебное пособие является частью программно-методического комплекса «Корпоративные сети», включающего:

- учебное пособие «IP-адресация»;
- компьютерный тренажер по теме «IP-адресация».

В пособии рассмотрены основы IP-адресации, ведущие концепции построения сетей посредством объединения подсетей. Предложенные в пособии упражнения нацелены на формирование у обучающихся навыков определения корректности IP-адресов, присваивания IP-адреса узлам и выявления проблем, связанных с IP-адресацией.

При работе с данным пособием необходимо соблюдать следующие правила:

- вести краткий конспект – это поможет ускорить усвоение материала;
- задания, отмеченные значком ✍, выполнять письменно в тетради (впоследствии тетрадь сдается преподавателю);
- отвечать устно на вопросы для самоконтроля;
- для повторения пройденного материала использовать резюме;
- итоговую практическую работу выполнять самостоятельно. Если обучающийся справится со всеми заданиями итоговой практической работы без помощи преподавателя, это будет означать, что материал усвоен им на достаточном уровне.

Предлагаемое учебное пособие содержит таблицы преобразования масок подсетей для сетей классов A, B и C, заданные с использованием одного октета (приложение).

Раздел 1. IP-АДРЕСАЦИЯ И ПОДСЕТИ

Глава 1. Адресация в TCP/IP-сетях

Стек протоколов TCP/IP предназначен для соединения отдельных подсетей, построенных по разным технологиям канального и физического уровней (Ethernet, Token Ring, FDDI, ATM, X.25 и т. д.), в единую сеть. Каждая из технологий нижнего уровня предполагает свою схему адресации. Поэтому на межсетевом уровне требуется единый способ адресации, позволяющий уникально идентифицировать каждый узел, входящий в составную сеть. Таким способом в TCP/IP-сетях является IP-адресация. Узел составной сети, имеющий IP-адрес, называется *хост* (host).

Хороший пример, иллюстрирующий составную сеть, – международная почтовая система адресации. Информация сетевого уровня – это индекс страны, добавленный к адресу письма, написанному на одном из тысяч языков земного шара, например, на китайском. И даже если это письмо должно пройти через множество стран, почтовые работники которых не знают китайского, понятный им индекс страны-адресата подскажет, через какие промежуточные страны лучше передать письмо, чтобы оно кратчайшим путем попало в Китай. А уже там работники местных почтовых отделений смогут прочитать точный адрес, указывающий город, улицу, дом и человека, и доставить письмо адресату, так как адрес написан на языке и в форме, принятой в данной стране.

Рассмотрим типы адресов стека TCP/IP. В стеке TCP/IP используются три типа адресов:

- локальные (другое название – аппаратные);
- IP-адреса (сетевые адреса);
- символьные доменные имена.

Локальный адрес – это адрес, присвоенный узлу в соответствии с технологией подсети, входящей в составную сеть. Если подсетью является локальная сеть Ethernet, Token Ring или FDDI, то локальный адрес – это MAC-адрес (MAC address – Media Access Control address). MAC-адреса назначаются сетевым адаптерам и портам маршрутизаторов производителями оборудования и являются уникальными, так как распределяются централизованно. MAC-адрес имеет размер 6 байт и записывается в шестнадцатеричном виде, например, 00–08–A0–12–5F–72.

IP-адреса (IP address) представляют собой основной тип адресов, на основании которых сетевой уровень передает сообщения, называемые *IP-пакетами*. Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов – по числу сетевых адаптеров. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. Подробнее IP-адреса будут рассмотрены далее.

Символьные доменные имена (domain name) служат для удобства представления IP-адресов. Человеку сложно запоминать числовые IP-адреса, поэтому была разработана специальная служба – DNS (Domain Name System), устанавливающая соответствие между IP-адресами и символьными доменными именами, например, www.rambler.ru.

Вопросы и задания для самоконтроля

1. Что такое хост?
2. Приведите пример составной сети.
3. Каким устройствам назначается MAC-адрес?
4. Какой размер имеет MAC-адрес?
5. Перечислите виды и примеры адресов, используемых в стеке TCP/IP.

Глава 2. IP-адрес

Основные понятия и определения

IP-адрес определяет местонахождение узла в сети подобно тому, как адрес дома указывает его расположение в городе. Как и обычный адрес, IP-адрес должен быть *уникальным* и иметь единый формат. Каждый IP-адрес имеет длину 32 бита и состоит из четырех 8-битных полей, называемых *октетами* (octets), которые отделяются друг от друга точками. Каждый октет представляет десятичное число в диапазоне от 0 до 255 (**192.168.10.25**, **145.189.33.0** и т. п.). Такой формат представления IP-адресов носит особое название – *десятично-точечный* (dotted decimal).

Запись IP-адреса в виде четырех десятичных чисел, разделенных точками, наиболее удобна для восприятия, тем не менее на практике используется еще один формат – *двоичный* (binary), например:

11000001 1000100 000001010 00001101.

Десятично-точечный и двоичный форматы представления IP-адресов равноправны между собой и взаимозаменяемы [1, с. 368].

Преобразование IP-адреса из двоичного формата в десятичный. Рассмотрим правила преобразования двоичного формата представления IP-адреса в десятично-точечный (и наоборот).

В двоичном формате каждый бит в октете сопоставлен с определенным десятичным числом (рис. 1).

Рис. 1. Преобразование IP-адреса из двоичного формата в десятичный

Если возникает необходимость, каждый октет в IP-адресе может быть преобразован в десятичное число. В табл. 1 показано, как биты одного октета преобразуются в десятичное число.

Таблица 1

Преобразование бит одного октета в десятичное число

Двоичная запись	Значения бит	Десятичное число
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

Пример 1

Перевести IP-адрес из двоичного формата представления

11000001 01000100 000001010 00000001

в десятично-точечный.

Решение

Этап 1. По правилам перевода из двоичной системы счисления в десятичную переводим каждый октет (8-битное поле IP-адреса) в десятичное число:

11000001 (=128+64+1) → 193
01000100 (=64+4) → 68
000001010 (=2+8) → 10
00000001 (=1) → 1

Этап 2. Записываем IP-адрес в десятично-точечном формате.

Десятично-точечный формат представления IP-адреса – **193.68.10.1**.

Этап 3. Получаем IP-адрес:

$$\mathbf{11000001.01000100.000001010.00000001_2 - 193.68.10.1_{10}.}$$

Пример 2

Перевести IP-адрес из десятично-точечного формата представления **232.160.21.3** в двоичный.

Решение

Этап 1. По правилам перевода из десятичной системы счисления в двоичную переводим каждый октет в двоичное число:

232 → 11101000
160 → 10100000
21 → 00010101
3 → 00000011

Этап 2. Записываем IP-адрес в двоичном формате.

Двоичный формат представления IP-адреса –

11101000 10100000 00010101 00000011.

Этап 3. Получаем IP-адрес:

$$\mathbf{232.160.21.3_{10} - 11101000\ 10100000\ 00010101\ 00000011_2.}$$

Идентификаторы сетей и узлов. В любом из IP-адресов выделяют две части – *идентификатор сети* и *идентификатор узла*. Первый определяет физическую сеть. Он одинаков для всех узлов в одной объединенной сети и уникален для каждой из сетей, включенных в нее.

Идентификатор узла соответствует конкретному сетевому интерфейсу, расположенному на рабочей станции, серверу, маршрутизатору или другому TCP/IP-узлу в данной сети. Он должен иметь уникальное значение в данной сети. Каждый узел TCP/IP однозначно определяется по своему логическому IP-адресу. Такой адрес необходим всем сетевым компонентам, взаимодействующим по TCP/IP (см. об этом далее).

Любой IP-адрес содержит идентификатор сети и узла. Например, **193.68.10.1**$_{10}$, где адрес сети – **193.68.10.0,** адрес узла – **0.0.0.1** (рис. 2) (о правилах определения адреса сети и узла см. далее).

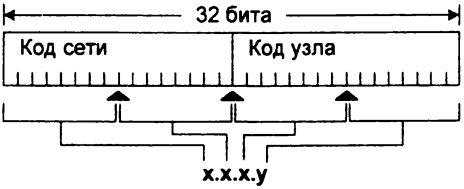


Рис. 2. Пример IP-адреса (193.68.10.1)

Практические задания

1. Переведите следующие двоичные числа в десятичные (см. табл. 1):

1) 10010100;
2) 11010101;
3) 10000001;
4) 00100110;
5) 11000110;
6) 00111101;
7) 11110001;
8) 11000000;
9) 11100000;
10) 11100011;
11) 10101111;
12) 11111000;
13) 11000110;
14) 10001001.

2. Переведите следующие десятичные числа в двоичные:

1) 23;
2) 196;
3) 68;
4) 165;
5) 10;
6) 35;
7) 127;
8) 200;
9) 152;
10) 187;
11) 46;
12) 94;
13) 115;
14) 44.

3. Определите, корректно ли записаны IP-адреса:

1) 110.256.255.50;
2) 143.5.41.255;
3) 192.68.255.254;
4) 109.128.2.2;
5) 18.168.10.0;
6) 130.224.100.2;
7) 198.198.198.1;
8) 195.64.2.1;
9) 200.192.192.1;
10) 190.0.0.0;
11) 144.60.127.258;
12) 18.151.10.2;
13) 230.14.67.90;
14) 268.172.64.0.

4. Запишите IP-адрес, представленный в десятично-точечном формате:

1) 01110110.00001011.00100100.11011001;
2) 01000000.00011001.11010100.11111100;
3) 11111100.11011010.11101001.11011010;
4) 01100101.11110000.01010001.11001110;
5) 00111111.00001001.01111000.11010001;
6) 10000000.11100110.10011110.00101011;
7) 10011010.01010010.11001111.11110111;
8) 10010110.01001111.00000110.00111110;
9) 00001101.11000010.10000000.11011001;
10) 10100011.00100011.10001101.11000111;
11) 00011010.01000000.10100100.01101000;
12) 01010000.01101011.10101011.10100111;
13) 11110001.00101000.10101011.01101001;
14) 01000100.00001000.01000000.10100100.

Резюме

Каждый узел TCP/IP идентифицируется по логическому IP-адресу, а уникальный IP-адрес необходим каждому узлу и сетевому компоненту, использующему TCP/IP. IP-адреса базируются на протоколе IP (Internet Protocol) и являются уникальными 32-битными логическими адресами, которые относятся к уровню 3 (сетевому) эталонной модели OSI. IP-адрес содержит адрес самого устройства, а также адрес сети, в которой это устройство находится. Поскольку IP-адреса имеют иерархическую структуру (как телефонные номера или почтовые индексы), их удобнее использовать в качестве адресов компьютеров, чем MAC-адреса, которые являются плоскими адресами (как номера карточек социального страхования). IP-адреса представляют собой 32-битные значения, которые записываются в виде четырех октетов (групп по 8 бит) и содержат двоичные числа, состоящие из нулей и единиц. В десятичной форме представления с разделением точками каждый байт 4-байтового IP-адреса записывается в виде десятичного числа.

Вопросы и задания для самоконтроля

1. Для чего необходим IP-адрес сети?
2. В каком виде записывается IP-адрес?
3. Какую длину имеет IP-адрес?
4. Что определяют в IP-адресе идентификатор сети и идентификатор узла?
5. Какое десятичное число является эквивалентом двоичного числа 11111111?

Глава 3. Классы IP-адресов

Основные понятия и определения

Каждый класс IP-адресов указывает, какая часть адреса отводится под идентификатор сети, а какая – под идентификатор узла. Класс адреса уточняет, какие биты относятся к идентификатору сети, а какие – к идентификатору узла. Также он фиксирует максимально возможное количество узлов в сети.

Интернет-адреса распределяются организацией InerNIC, которая администрирует Интернет. Эти IP-адреса распределены по классам. Существует пять классов IP-адресов: A, B, C, D, E. Принадлежность IP-адреса к тому или иному классу определяется значением первого октета, так, 32-разрядные IP-адреса могут быть присвоены в общей совокупности 3 720 314 628 узлам. В табл. 2 показано соответствие значений первого октета и классов адресов.

Таблица 2

Соответствие значений первого октета и классов адресов

Класс IP-адреса	A	B	C	D	E
Диапазон первого октета	1–126	128–191	192–223	224–239	240–255

IP-адреса первых трех классов предназначены для адресации отдельных узлов и отдельных сетей и состоят из двух частей – *номера сети* и *номера узла.* Такая схема аналогична схеме почтовых индексов – первые три цифры кодируют регион, а остальные – почтовое отделение внутри региона.

Преимущества двухуровневой схемы очевидны: она позволяет, во-первых, адресовать отдельные сети внутри составной сети целиком, что необходимо для обеспечения маршрутизации, а во-вторых – присваивать узлам номера внутри одной сети независимо от других сетей. Естественно, что компьютеры, входящие в одну и ту же сеть, должны иметь IP-адреса с одинаковым номером сети.

Наиболее распространены адреса классов A, B и C – их назначают хостам. Адреса классов D и E существуют, но обычно не используются конечными пользователями, так как не могут быть назначены хостам: они зарезервированы для служебного использования и групповой рассылки.

Если два компьютера имеют IP-адреса с разными номерами сетей (даже если они принадлежат одной физической сети), то они не могут общаться друг с другом напрямую – для их взаимодействия необходим маршрутизатор.

IP-адреса разных классов отличаются разрядностью номеров сети и узла, что определяет их возможный диапазон значений. Рассмотрим, как определяются поля в IP-адресах разных классов.

Класс А. Адреса класса А назначаются узлам очень большой сети. *Старший бит* в адресах этого класса всегда равен **0**. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Это позволяет иметь 126 сетей с числом узлов до 17 млн в каждой. Таким образом, IP-адреса для класса А находятся в диапазоне от **1** до **126**. Например, **2.35.50.200** (рис. 3).

Рис. 3. Пример IP-адреса класса А

Класс В. Адреса класса В назначаются узлам в больших и средних по размеру сетях. В *двух старших битах* IP-адреса класса В записывается *двоичное значение* **10**. Следующие 14 бит содержат идентификатор сети (два первых октета). Оставшиеся 16 бит (два октета) представляют идентификатор узла. Это позволяет иметь 16 384 сетей класса В, в каждой из которых около 65 тыс. узлов. Таким образом, IP-адреса для класса В находятся в диапазоне от **128** до **191.** Например, **132.58.157.200** (рис. 4).

Рис. 4. Пример IP-адреса класса В

Класс С. Адреса класса С применяются в небольших сетях. *Три старших бита* IP-адреса этого класса содержат *двоичное значение* **110**. Следующие 21 бит составляют идентификатор сети (первые три октета). Оставшиеся восемь бит (последний октет) отводятся под идентификатор

узла. Всего возможно около 2 млн сетей класса С, содержащих до 254 узлов. Таким образом, IP-адреса класса С находятся в диапазоне от **192** до **223**. Например, **192.158.20.01** (рис. 5).

Рис. 5. Пример IP-адреса класса С

Сводные данные для IP-адресов классов А, В, С приведены в табл. 3.

Таблица 3

Сводная таблица классов IP-адресов

Класс	Количество сетей	Количество узлов в сети	Диапазон значений идентификаторов сети
A	126	16 777 214	**1–126**
B	16 384	65 534	**128–191**
C	2 097 152	254	**192–223**

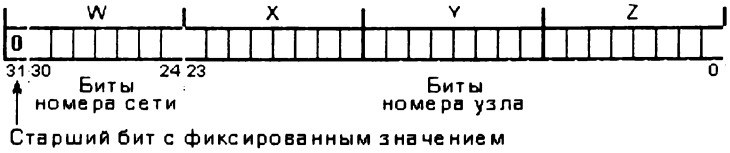
Примечание. В качестве идентификатора сети не может использоваться значение **127**. Оно зарезервировано для широковещательного сигнала, самотестирования.

Класс D. Группа получателей может содержать один, несколько или ни одного узла. *Четыре старших бита* в IP-адресе класса D всегда равны **1110**. Таким образом, IP-адреса класса D находятся в диапазоне от **224** до **239**. Оставшиеся биты обозначают конкретную группу получателей и не разделяются на части. Пакеты с такими адресами рассылаются избранной группе узлов в сети. Их получателями могут быть только специальным образом зарегистрированные узлы. Microsoft поддерживает адреса класса D, применяемые приложениями для групповой рассылки сообщений, включая WINS и Microsoft NetShow™.

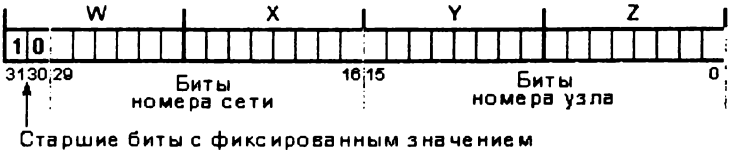
Класс E. Класс E – экспериментальный. Он зарезервирован для использования в будущем и в настоящее время не применяется. *Четыре старших бита* адресов класса E равны **1111**. Таким образом, IP-адреса класса E находятся в диапазоне от **240** до **255** [4, с. 369].

Используя двоичную форму записи IP-адреса, легко определить схемы классов IP-адресов (рис. 6).

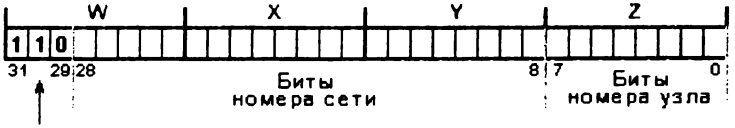
Класс A



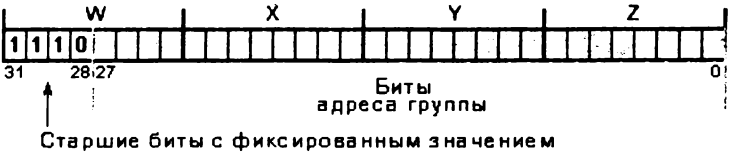
Класс B



Класс C



Класс D



Класс E

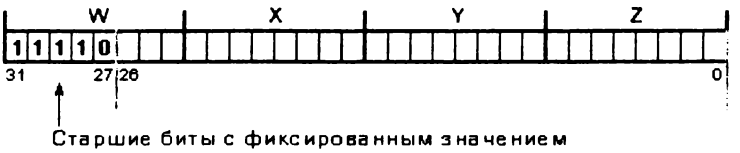


Рис. 6. Двоичные схемы IP-адресов классов A, B, C, D и E

✍Практические задания

1. Укажите классы следующих IP-адресов:

1) 190.30.0.0;
2) 225.4.3.0;
3) 99.168.10.0;
4) 18.1514.20.0;
5) 254.0.0.0;
6) 192.168.10.4;
7) 128.10.2.30;
8) 3.5.58.0;
9) 11.0.0.10;
10) 221.100.5.0;
11) 128.10.2.30;
12) 131.20.15.5;
13) 250.124.15.5;
14) 124.5.5.0.

2. Определите, какая часть IP-адреса относится к адресу сети, а какая – к адресу хоста:

1) 144.35.39.39;
2) 95.210.50.2;
3) 20.135.210.10;
4) 131.45.224.115;
5) 1.234.17.58;
6) 28.244.168.10;
7) 22.192.35.1;
8) 100.250.182.240;
9) 24.182.45.73;
10) 173.128.46.158;
11) 210.58.93.0;
12) 5.20.113.10;
13) 243.254.10.25;
14) 235.12.5.8.

Резюме

Всего существуют пять классов IP-адресов. Microsoft поддерживает назначение узлам адресов классов A, B и C. Каждый класс соответствует сетям определенного размера.

Вопросы и задания для самоконтроля

1. В сетях каких классов IP-адресов имеется до 254 узлов?

2. В сетях каких классов IP-адресов имеется более 65000 узлов?

3. К какому классу относят сеть, если адрес начинается с 0, номер сети занимает 1 байт и остальные 3 байта интерпретируются как номер узла в сети?

4. Сколько бит отводится под номер сети и под номер узла для сети класса C?

Глава 4. Назначение IP-адресов

Основные понятия и определения

Поскольку каждый узел сети Интернет должен обладать уникальным IP-адресом, то, безусловно, важной является задача координации назначения адресов отдельным сетям и узлам. Такую координирующую роль вы-

полняет Интернет-корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers – ICANN).

Естественно, что ICANN не решает задач выделения IP-адресов конечным пользователям и организациям, а занимается распределением диапазонов адресов между крупными организациями – поставщиками услуг по доступу к Интернету (Internet Service Provider), которые, в свою очередь, могут взаимодействовать как с более мелкими поставщиками, так и с конечными пользователями. Так, например, функции по распределению IP-адресов в Европе ICANN делегировал Координационному центру RIPE (The RIPE Network Coordination Centre – RIPE NCC; RIPE – Reseaux IP Europeens). В свою очередь, этот центр делегирует часть своих функций региональным организациям. В частности, российских пользователей обслуживает Региональный сетевой информационный центр «RU-CENTER».

В настоящее время не существует строгих правил назначения IP-адресов, но следует учитывать некоторые тонкости, чтобы выбирать корректные идентификаторы узлов и сетей.

Правила назначения IP-адресов:

1. Идентификатор сети не может быть равным **127**. Это значение зарезервировано для широковещательного сигнала самотестирования.

2. Все биты идентификатора сети или узла не могут быть одновременно установлены в **1**. Такой идентификатор применяется для широковещательных сообщений.

3. Все биты идентификатора сети или узла не могут быть одновременно установлены в **0**, так как в этом случае идентификатор охватывает всю локальную сеть.

4. Каждый идентификатор узла должен быть уникальным для соответствующего идентификатора сети.

Назначение идентификаторов сетей. Уникальный идентификатор необходим каждой сети и каждому внешнему соединению. Если ваша сеть подключена к Интернету, вам надо получить идентификатор сети от *Информационного центра Интернета* (Internet Network Information Center – InterNIC).

Идентификатор сети обозначает узлы TCP/IP, подключенные к одной физической сети. Поэтому чтобы взаимодействовать друг с другом, все узлы одной физической сети должны иметь одинаковый идентификатор сети.

Если несколько сетей соединены через маршрутизаторы, уникальный идентификатор сети необходим для каждой из них. Такая ситуация отражена на рис. 7.

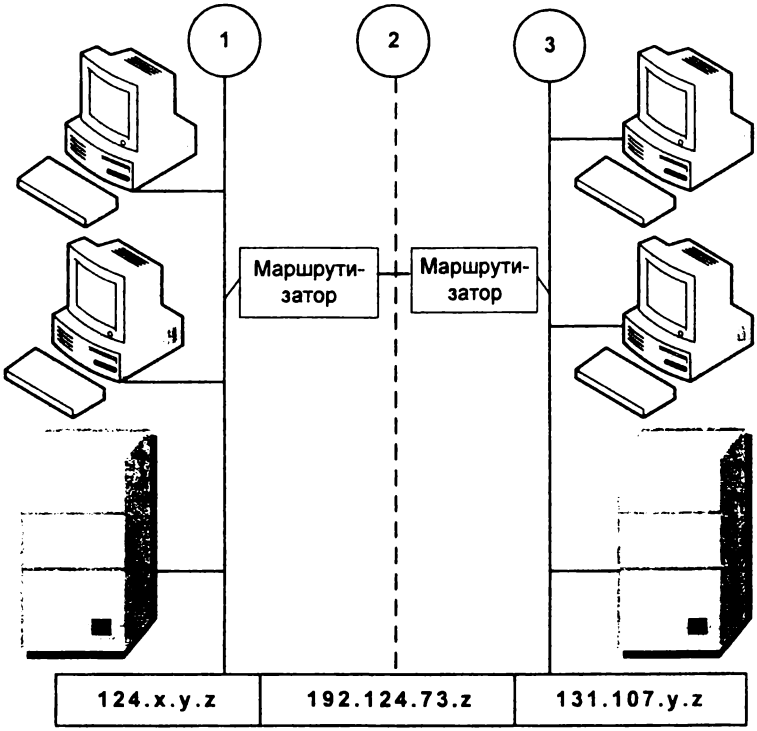


Рис. 7. Соединение сетей через маршрутизаторы

На рис. 7 сети 1 и 3 соединены через маршрутизаторы. Маршрутизаторы соединяются через глобальную сеть 2. Для сети 2 необходим отдельный идентификатор, чтобы соответствующие ей интерфейсы маршрутизаторов могли иметь уникальные идентификаторы узлов.

Пространство IP-адресов, предназначенных для использования в изолированных сетях, определено в RFC 1918 [6, с. 281].

Назначение идентификаторов узлов. Идентификатор узла служит для обозначения TCP/IP-узла в некоторой сети и должен иметь уникальное значение для данного идентификатора сети. Всем TCP/IP-узлам, включая

интерфейсы маршрутизаторов, необходимы уникальные идентификаторы. Идентификатор узла для маршрутизатора соответствует значению IP-адреса, указываемого в качестве адреса шлюза по умолчанию в конфигурации рабочей станции [6, с. 289].

Например, для узла из подсети 1, сетевой интерфейс которой имеет IP-адрес **124.0.0.27**, адресом шлюза по умолчанию будет **124.0.0.1** (рис. 8).

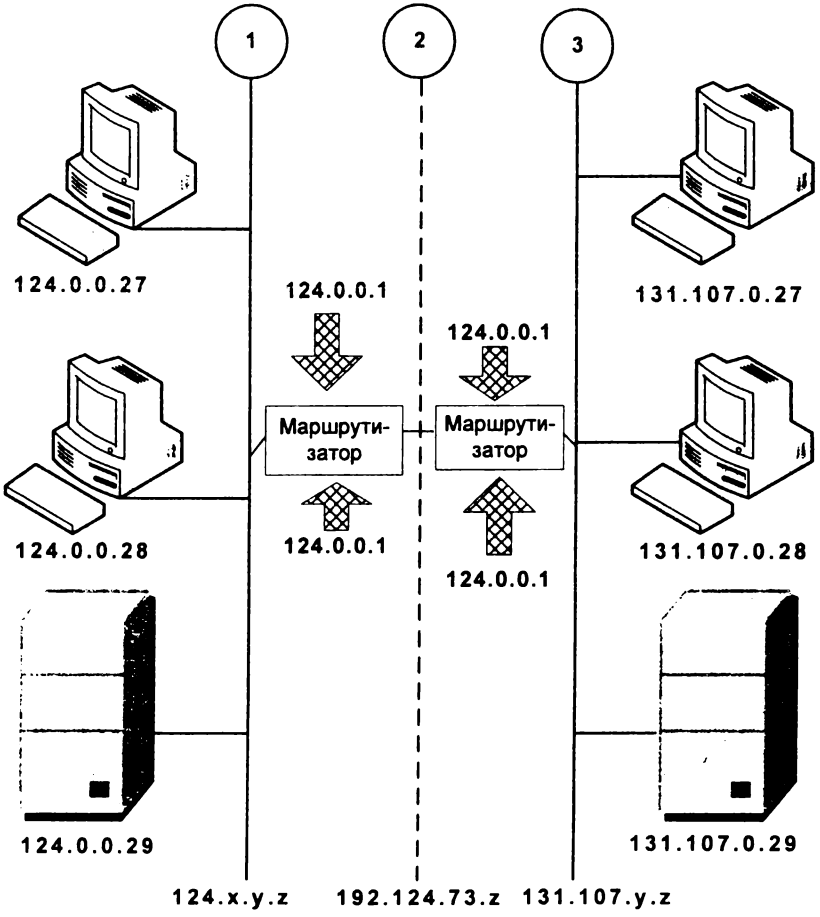


Рис.8. Назначение идентификаторов узлов

Корректные идентификаторы узлов. В табл. 4 указаны корректные значения идентификаторов узлов в сети.

Таблица 4

Корректные идентификаторы узлов

Класс адреса	Начало диапазона	Конец диапазона
A	**w.0.0.1**	**w.255.255.254**
B	**w.x.0.1**	**w.x.255.254**
C	**w.x.y.1**	**w.x.y.254**

Практические задания

1. Определите, какие IP-адреса не могут быть назначены узлам, и объясните, почему такие IP-адреса не являются корректными:

1) 230.14.67.90;
2) 150.150.255.255;
3) 111.256.4.0;
4) 0.56.78.91;
5) 1.1.0.0;
6) 257.0.0.1;
7) 0.56.78.91;
8) 220.84.73.0;
9) 254.254.254.254;
10) 172.64.0.0;
11) 12.255.255.255;
12) 195.31.14.255;
13) 255.255.255.25;
14) 5.54.0.0.

2. По IP-адресу определите класс, адрес сети и адрес узла:

1) 230.14.67.90;
2) 150.150.255.255;
3) 111.256.4.0;
4) 0.56.78.91;
5) 1.1.0.0;
6) 257.0.0.1;
7) 0.56.78.91;
8) 220.84.73.0;
9) 254.254.254.254;
10) 172.64.0.0;
11) 12.255.255.255;
12) 195.31.14.255;
13) 255.255.255.25;
14) 5.54.0.0.

Резюме

При назначении IP-адресов следует соблюдать определенные правила. Чтобы все узлы одной сети взаимодействовали друг с другом, они должны иметь одинаковые идентификаторы сети. Каждому узлу TCP/IP, включая интерфейсы маршрутизаторов, необходим уникальный идентификатор узла.

Вопросы и задания для самоконтроля

1. Какое из следующих утверждений верно описывает IP-адреса? Выберите все правильные ответы:

• логические 64-битные адреса идентифицируют TCP/IP-узел;

• каждая плата сетевого адаптера в компьютере с запущенным TCP/IP требует уникальный IP-адрес;

• **192.138.0.108** – пример IP-адреса класса C;

• идентификатор узла в IP-адресе – всегда последние два октета в адресе.

2. Обоснуйте правильность тезиса о том, что каждый идентификатор узла должен быть уникальным для соответствующего идентификатора сети.

3. Объясните, почему все биты идентификатора сети или узла не могут быть одновременно установлены в **1**.

4. Объясните, почему идентификатор сети не может быть равен **127**.

5. Для чего предназначен идентификатор узла?

Глава 5. IP-адреса и маски подсетей

Основные понятия и определения

В настоящее время единого толкования понятия «маска подсети» не существует. В данном пособии мы основываемся на определении, предложенном В. Г. Олифер и Н. А. Олифер: *маска подсети* – это 32-разрядное значение, используемое для выделения (маскирования) из IP-адреса его частей – идентификаторов сети и узла [3]. Такая процедура необходима при выяснении того, относится тот или иной IP-адрес к локальной либо удаленной сети.

В общем случае *маска* представляет собой упорядоченную последовательность единиц, сменяющихся упорядоченной последовательностью нулей (например, **11111111.11111111.11111111.11100000** в двоично-точечном формате и **255.255.255.224** в десятичном формате).

Каждый узел TCP/IP должен иметь маску подсети – либо задаваемую по умолчанию (в том случае, когда сеть не делится на подсети), либо специальную (если сеть разбита на несколько подсетей) (табл. 5).

Таблица 5

Соответствие классов IP-адресов маскам

Класс адреса	Биты, используемые для маски подсети	Десятично-точечная запись маски подсети
A	**11111111.00000000.00000000.00000000**	**255.0.0.0**
B	**11111111.11111111.00000000.00000000**	**255.255.0.0**
C	**11111111.11111111.11111111.00000000**	**255.255.255.0**

Пример 1

Дан IP-адрес класса B **156.108.20.200.** Определить маску подсети, идентификаторы сети и узла.

Решение

Этап 1. По табл. 4 определяем соответствие для класса B десятично-точечной записи маски подсети: **255.255.0.0**.

Этап 2. Определяем идентификатор сети и идентификатор узла.

Идентификатор сети – **156.108.Y. Y.** Идентификатор узла – **X. X.20.200.**

Этап 3. Получаем: маска подсети – **255.255.0.0**; идентификатор сети – **156.108.Y.Y**; идентификатор узла – **X. X.20.200**.

Маска подсети, задаваемая по умолчанию. Задаваемая по умолчанию маска подсети используется в том случае, если сеть TCP/IP не разделяется на подсети. Даже в сети, состоящей из одного сегмента, всем узлам TCP/IP необходима маска подсети. Значение маски подсети по умолчанию зависит от используемого класса IP-адресов.

В маске подсети биты, соответствующие идентификатору сети, устанавливаются в **1**.Таким образом, значение каждого октета будет равно **255**. Все биты, соответствующие идентификатору узла, устанавливаются в **0**.

Пример 2

Определить адрес сети, зная IP-адрес и маску: **192.168.150.111** и **255.255.255.224.**

Решение

Этап 1. Маска позволяет однозначно определить адрес сети и адрес узла. Распишем последний октет маски **224** в двоичном формате: **11100000**. По правилу все единицы в маске идентифицируют адрес сети.

Этап 2. Распишем последний октет IP-адреса **111** в двоичном формате: **01101111**.

Этап 3. Соотнесем последние октеты IP-адреса и маски (рис. 9).

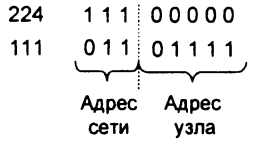


Рис. 9. Соотношение IP-адреса и маски

Этап 4. Переведем адрес сети **011 96** и адрес узла **01111 15** в десятичный формат.

Адрес сети – **192.168.150.96**, адрес узла – **0.0.0.15**.

Этап 5. Получаем: адрес сети – **192.168.150.96**, адрес узла – **0.0.0.15**.

Практические задания

1. Определите, какие IP-адреса из приведенных ниже не могут быть назначены узлам, и объясните, почему они не являются корректными:

1) 230.14.67.90;
2) 150.150.255.255;
3) 111.256.4.0;
4) 0.56.78.91;
5) 131.107.80.256;
6) 222.222.255.222;
7) 231.200.1.1;
8) 126.1.0.0;
9) 0.127.4.100;
10) 190.7.2.0;
11) 127.1.1.1;
12) 198.121.254.255;
13) 255.255.255.255;
14) 255.190.0.4.

2. Укажите корректные комбинации адреса сети и сетевой маски и определите максимальное количество компьютеров в данной сети:

1) 10.0.0.31 и 255.255.255.240;
2) 10.1.0.96 и 255.255.255.224;
3) 10.1.0.16 и 255.255.255.232;
4) 131.20.15.5 и 255.0.0.0;
5) 124.5.5.0 и 255.192.0.0;
6) 192.56.2.0 и 255.255.192.0;
7) 150.124.15.1 и 255.255.192.1;
8) 192.10.0.1 и 255.255.255.192;
9) 192.10.0.0 и 255.255.255.0;
10) 136.256.0.1 и 255.255.0.0;
11) 136.250.0.1 и 255.255.0.0;
12) 244.30.1.1 и 255.255.255.224;
13) 192.168.15.1 и 255.255.255.224;
14) 130.6.10.1 и 255.255.0.0;
15) 192.56.2.0 и 255.255.192.0;
16) 150.124.15.1 и 255.255.192.90;
17) 124.5.5.0 и 255.192.0.0.

3. Определите класс сети и максимальное количество узлов сети, для которых задана маска:

1) 255.255.0.0;
2) 252.0.0.0;
3) 255.192.0.0;
4) 255.248.192.0;
5) 255.255.255.224;
6) 255.255.15.0;
7) 255.255.240.0;
8) 255.0.0.0;
9) 255.255.224.0;
10) 255.224.0.0;
11) 255.255.192.0;
12) 128.0.0.0;
13) 255.64.0.0;
14) 255.255.255.254.

4. Определите адрес сети, зная IP-адрес и маску:

1) 192.10.50.215 и 255.255.255.248;
2) 130.20.0.0 и 255.255.240.0;
3) 20.0.0.0 и 255.255.192.0;
4) 199.9.9.0 и 255.255.255.224;
5) 192.168.10.0 и 255.255.255.192;
6) 192.168.150.200 и 255.255.255.224.

Резюме

Маска подсети по умолчанию используется в сетях TCP/IP, которые не разделены на подсети. Специальные значения маски подсети используются в том случае, когда сети состоят из нескольких подсетей.

Вопросы и задания для самоконтроля

1. Дайте определение маски подсети.

2. Установите соответствие по классам IP-адресов и маски в десятично-точечном формате:

Класс A	**255.255.255.0**
Класс B	**255.255.0.0**
Класс C	**255.0.0.0**

3. Чему равно значение каждого октета идентификатора сети?

4. Чему равно значение каждого октета идентификатора узла?

Глава 6. IP-адресация в IP версии 6.0

Основные проблемы протокола IPv4 и пути их решения

1. Быстрое исчерпание адресного пространства. В настоящее время наблюдается дефицит IP-адресов. Например, очень трудно получить адрес класса B и практически невозможно стать обладателем адреса класса A. Дефицит обусловлен не только ростом сетей, но и тем, что имеющееся множество IP-адресов не всегда используется рационально. Очень часто

владельцы сети класса С расходуют лишь небольшую часть из имеющихся у них 254 адресов. Например, две сети необходимо соединить глобальной связью. В таких случаях в качестве канала связи используют два маршрутизатора, соединенных по схеме «точка – точка» (рис. 10). Для вырожденной сети, образованной каналом, связывающим порты двух смежных маршрутизаторов, приходится выделять отдельный номер сети, хотя в этой сети имеются всего два узла.

Рис. 10. Пример нерационального использования пространства IP-адресов

Кроме того, к Интернету теперь подключаются не только стационарные компьютеры, но и карманные, а также мобильные телефоны и другие устройства, вплоть до холодильников и утюгов.

Если некоторая IP-сеть создана для работы в автономном режиме, т. е. без связи с Интернетом, то администратор этой сети может назначить ей произвольно выбранный номер. В стандартах Интернета определено несколько диапазонов адресов, рекомендуемых для локального использования. Эти адреса не обрабатываются маршрутизаторами Интернета. Адреса, зарезервированные для локальных целей:

- в классе А – сеть **10.0.0.0**;
- в классе В – диапазон из 16 номеров сетей: **172.16.0.0–172.31.0.0**;
- в классе С – диапазон из 255 номеров сетей: **192.168.0.0–192.168.255.0**.

Проблема отсутствия свободного адресного пространства привела к необходимости использования трансляторов сетевых адресов NAT (Network Address Translator), которые отображают несколько частных адресов в один открытый IP-адрес. Основные проблемы, создаваемые этим механизмом, – дополнительные издержки при обработке данных и отсутствие сквозного соединения.

2. Отсутствие поддержки иерархии. Вследствие предопределенной внутренней организации классов в протоколе IPv4 отсутствует поддержка подлинной иерархии. Невозможно структурировать IP-адреса таким обра-

зом, каким они на самом деле отображаются в топологии сети. Это делает необходимым использование большой таблицы маршрутизации для доставки пакетов IPv4 в любое место Интернета.

3. Сложность настройки сети. Для использования протокола IPv4 адреса должны присваиваться статически или с помощью таких протоколов конфигурации, как DHCP. В идеальной ситуации хосты должны не полагаться на администрацию инфраструктуры протоколом DHCP, а иметь способность к самостоятельному конфигурированию на основе сегмента сети, в котором они расположены.

4. Отсутствие встроенных систем проверки подлинности и конфиденциальности. Протокол IPv4 не требует поддержки какого-либо механизма, который при обмене данными обеспечивал бы проверку их подлинности или шифрование.

Для решения отмеченных проблем разработчики стека TCP/IP предлагают разные подходы. Принципиальным решением является переход на протокол (Internet Protocol) версии 6 (IPv6).

В июне 1992 г. в Кобе (Япония) прошла встреча, на которой были выдвинуты предложения относительно нового IP-протокола. В 1994 г. уже можно было говорить о появлении нового протокола IPv6, хотя работа над ним еще продолжалась. Скачок от версии 4 сразу к версии 6 объясняется тем, что номер «5» был уже занят параллельно разрабатываемым экспериментальным протоколом для передачи данных в реальном времени.

Протокол IPv6 – это новый набор стандартных протоколов для сетевого уровня Интернета. Новый набор протоколов должен удовлетворять следующим основным требованиям:

- широкомасштабная маршрутизация и адресация с низкими дополнительными издержками;
- автоконфигурация для разных способов подключения;
- встроенная система проверки подлинности и конфиденциальности.

Переход на новый протокол может затянуться на длительное время, в течение которого две версии протокола IP должны мирно сосуществовать[1].

Поэтому способ перехода должен предусматривать сохранение совместимости новых узлов и сетей с доминирующим сейчас в сети протоко-

[1] В документах рабочей группы IETF (Internet Tngineering Task Force – Инженерный совет Интернета) по вопросам смены версий протокола IP (Next Generation Transition, NGTRANS) указывается, что IPv4 и IPv6 могут сосуществовать в течение неограниченного времени.

лом IPv4. Логика работы и форматы данных двух протоколов существенно отличаются, поэтому их совместимость должна обеспечиваться внешними по отношению к ним механизмами.

Протокол IPv6

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Используемый в настоящее время и рассматриваемый в данном учебном пособии протокол IP называется IPv4 – протокол IP 4-й версии. Для преодоления ограничений IPv4 был разработан протокол IP 6-й версии – IPv6 (RFC 2373, 2460).

В новой версии протокола IP – IPv6, ранее именовавшейся *IP нового поколения* (IP – The Next Generation, IPng), воплощен ряд идей по обновлению IP.

IPv6 создавался специально для решения двух основных проблем: нехватки имеющегося пространства адресов и возможного дефицита их в будущем. *В IPv6 адрес состоит из 16 октетов.* На письме он изображается в виде *восьми пар октетов*, разделенных двоеточиями. *Октеты записываются в шестнадцатеричном формате.*

В IPv6 применена принципиально иная структура пакета, не совместимая с версией 4. Она имеет ряд преимуществ: расширенное адресное пространство, упрощенный формат заголовка, поддержка ориентированного на реальное время трафика и механизм добавления новых возможностей.

Расширенное адресное пространство – одна из ключевых особенностей IPv6. В этой версии используются 128-разрядные адреса получателей и отправителей (что в четыре раза больше, чем в IPv4). В 128 разрядах содержится более $3 \cdot 10^{48}$ возможных значений, что обеспечивает достаточно адресов на ближайшее и отдаленное будущее.

Адрес в IPv6 может выглядеть так:

4A3F:AE57.F240:56C4:3409.AE52:440F:1403.

Заголовок пакета IPv6 разработан таким образом, чтобы минимизировать содержащуюся в нем информацию. Поля опций и поля, не являющиеся необходимыми, вынесены в специальные расширения, расположен-

ные после заголовка. Все, что не входит в основное содержание заголовка IPv6, может быть размещено в следующих за ним расширениях.

Новое специальное поле позволяет предварительно выделять сетевые ресурсы на пути следования пакета, что гарантирует полосу пропускания с ограниченной задержкой для таких сервисов реального времени, как передача по сети голоса и видео.

И наконец, важнейшее преимущество IPv6 – его способность к увеличению за счет расширений, располагаемых непосредственно после основного заголовка. Важно, что при этом обеспечивается встроенная поддержка новых аппаратных и программных средств.

Таким образом, протокол IPv6 имеет следующие основные особенности:

1. Длина адреса – 128 бит: такая длина обеспечивает адресное пространство 2^{128}, или примерно $3{,}4 \cdot 10^{38}$, адресов. Такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам.

2. Автоматическая конфигурация: протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP.

3. Встроенная безопасность: для передачи данных является обязательным использование протокола защищенной передачи – IPsec.

Протокол IPv4 также может использовать IPsec, но не обязан этого делать. В настоящее время многие производители сетевого оборудования включают поддержку протокола IPv6 в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 несовместим с IPv4 и процесс перехода обратно сопряжен с определенными трудностями.

Формы представления адресов в IPv6

В протоколе IPv6 адреса имеют длину 128 бит (16 байт). Рекомендованы три формы представления адресов:

1. Форма шестнадцатеричных чисел и двоеточий. Эта форма является предпочтительной и имеет вид n:n:n:n:n:n:n:n. Каждый знак n соответствует четырехзначному шестнадцатеричному числу (всего 8 шестнадцатеричных чисел, для каждого числа отводится 16 бит).

Например: **3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562.**

2. Сжатая форма. По причине большой длины адрес обычно содержит много нулей подряд. Для упрощения записи адресов используется сжатая форма, в которой смежные последовательности нулевых блоков заменяются парой двоеточий (::). Однако такой символ может встречаться в адресе только один раз.

Например, адрес групповой рассылки **FFED:0:0:0:0:BA98:3210:4562** имеет сжатую форму **FFED::BA98:3210:4562**. Адрес одноадресной рассылки **3FFE:FFFF:0:0:8:800:20C4:0** в сжатой форме имеет вид

3FFE:FFFF::8:800:20C4:0.

Шлейфовый адрес **0:0:0:0:0:0:0:1** в сжатой форме выглядит как **::1**. Неопределенный адрес **0:0:0:0:0:0:0:0** превращается в **::**.

3. Смешанная форма. Эта форма представляет собой сочетание адресов протоколов IPv4 и IPv6. В данном случае адрес имеет формат

n:n:n:n:n:n:d.d.d.d,

где каждый символ n соответствует четырехзначному шестнадцатеричному числу (6 шестнадцатеричных чисел, для каждого числа отводится 16 бит), а d.d.d.d – часть адреса, записанная в формате IPv4 (32 бита).

Типы адресов в IPv6

Конкретный тип адреса протокола IPv6 определяют его начальные биты. Поле, содержащее эти биты, называется *префиксом формата* (FP), или адресным префиксом, и имеет переменную длину. Адрес одноадресной рассылки в протоколе IPv6 разделяется на две части. Первая часть содержит адресный префикс, а вторая – идентификатор интерфейса. Краткий способ представления адреса выглядит следующим образом: IPv6-адрес/длина префикса. Например, адрес с 64-битным префиксом

3FFF:FFFF:0:CD30:0:0:0:0/64.

Префиксом в этом примере является **3FFE:FFFF:0:CD30**.

Адрес также может быть записан в сжатой форме, например:

3FFE:FFFF:0:CD30::/64.

Протокол IPv6 определяет следующие типы адресов:

1. Адрес одноадресной рассылки. Идентификатор в адресе определяет один интерфейс. Пакет, посланный на этот адрес, доставляется по ука-

занному адресу. Адреса одноадресной рассылки отличаются от адресов групповой рассылки значением старшего октета. Старший октет адресов групповой рассылки имеет шестнадцатеричное значение FF. Все остальные значения этого октета определяют адрес одноадресной рассылки.

Рассмотрим различные типы адресов одноадресной рассылки.

Адреса локальной связи. Эти адреса используются для одной линии связи и имеют формат FE80::InterfaceID. Адреса локальной связи используются между узлами для автоконфигурации адресов, обнаружения соседа или при отсутствии маршрутизаторов. Адреса локальной связи используются в основном во время запуска и в случае, если система еще не получила адреса в большем адресном пространстве.

Адреса локальных веб-узлов. Эти адреса используются на одном веб-узле и имеют формат FEC0::SubnetID:InterfaceID. Адреса локальных веб-узлов используются для адресации внутри узла и не требуют глобального префикса.

Глобальные адреса одноадресной рассылки протокола IPv6. Эти адреса могут использоваться для связи через Интернет и имеют формат 010 (FP, 3 бита) TLA ID (13 бит) Резерв (8 бит) NLA ID (24 бита) SLA ID (16 бит) InterfaceID (64 бита).

2. Адрес групповой рассылки. Идентификатор в адресе определяет набор интерфейсов (обычно принадлежащих различным узлам). Пакет, посланный на такой адрес, доставляется всем интерфейсам, идентифицирующимся этим адресом. Типы групповых адресов замещают широковещательные адреса протокола IPv4.

3. Адрес для всех типов рассылок. Идентификатор в адресе определяет набор интерфейсов (обычно принадлежащих различным узлам). Пакет, посланный на такой адрес, доставляется только одному интерфейсу из идентифицирующихся данным адресом. Этот интерфейс является ближайшим из идентифицируемых метрикой маршрутизации.

Адреса для всех типов рассылок получаются из пространства адресов одноадресной рассылки и синтаксически не отличаются друг от друга. Для адресуемого интерфейса разница между адресом для всех типов рассылок и адресом одноадресной рассылки определяется во время конфигурации.

Как правило, узел всегда имеет адрес локальной связи. Также у него могут быть адрес локального веб-узла и один или несколько глобальных адресов.

Резюме

В адресном пространстве текущей версии IP возник дефицит адресов. В IPv6 используется принципиально иная структура пакета, имеющая ряд преимуществ: расширенное адресное пространство, упрощенный формат заголовка, поддержка ориентированного на реальное время трафика и механизм добавления новых функциональных возможностей.

Вопросы и задания для самоконтроля

1. По какой причине потребовалось создание IP нового поколения?
2. Назовите главные отличия IP-адресов версии 4 от IP-адресов версии 6 (укажите как минимум два отличия).
3. Назовите преимущества IPv6.
4. Обозначьте недостатки IPv6.

Глава 7. Общие сведения о подсетях

Основные понятия и определения

Подсеть (subnet) – это физический сегмент TCP/IP-сети, в котором используются IP-адреса с общим идентификатором сети. Для того чтобы разделить сеть на несколько подсетей, необходимо использовать различные идентификаторы сети (в данном случае подсети) для каждого сегмента [3, с. 238].

Как показано на рис. 11, уникальные идентификаторы подсетей создаются путем разбиения идентификатора узла на две группы бит. Первая из них служит для идентификации сегмента объединенной сети, вторая – для идентификации конкретного узла.

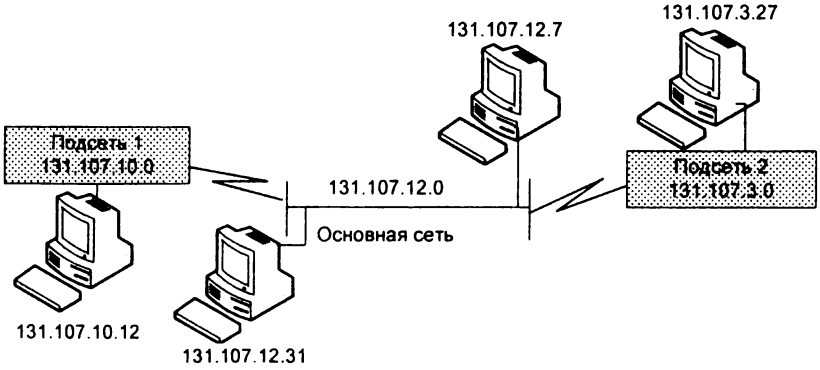


Рис. 11. Пример деления сети на подсети

Такой механизм называется делением на подсети (subnetting или subnetworking). Подсети соединяются между собой маршрутизаторами. Деление на подсети не является необходимым в изолированной сети (т. е. в сети, не имеющей выхода в Интернет).

Использование подсетей. Перед началом работы с подсетью необходимо определить, каким требованиям должна отвечать сеть сейчас и каким – в будущем.

Порядок работы с подсетью:

1. Определите число физических сегментов вашей сети.

2. Определите количество IP-адресов, необходимое для каждого сегмента. Каждому узлу TCP/IP нужен по крайней мере один IP-адрес.

3. В соответствии с вашими требованиями определите:

- одну маску подсети для всей вашей сети;
- уникальные идентификаторы подсети для каждого физического сегмента;
- диапазон идентификаторов узлов для каждой подсети.

Биты маски подсети. Перед тем как сформировать маску подсети, приблизительно определите, сколько сегментов и узлов в сегменте вам потребуется в будущем.

Задав больше бит для маски подсети, вы сможете увеличить количество подсетей, но максимальное число узлов в каждой из них сократится.

Следующий пример для сети класса B иллюстрирует эту зависимость.

Например, максимально для 8 бит возможны 254 подсети, в каждой из которой 254 узла (так как $2^8 = 256$, а количество узлов вычисляется по формуле $2^n - 2$).

Если Вы используете больше бит, чем необходимо, это позволит в будущем увеличить число подсетей, но ограничит количество узлов в каждой из них. И наоборот, при использовании меньшего количества бит остается возможность для увеличения числа узлов в подсети, но ограничивается количество подсетей.

✍Практические задания

1. По IP-адресам определите, лежат ли узлы в одной подсети:

1) **192.168.10.4/26**, **192.168.10.60/26**, **192.168.10.68/26**;

2) **130.60.54.0/20**, **130.60.90.0/20**, **130.60.128.7/16**;

3) **131.107.100.27/16**, **131.107.100.1/16**, **131.107.33.3/16**;

4) **192.168.10.10/20**, **192.168.10.0/15**, **192.168.10.68/26**.

2. Определите, сколько подсетей изображено на представленных ниже схемах (рис. 12–25).

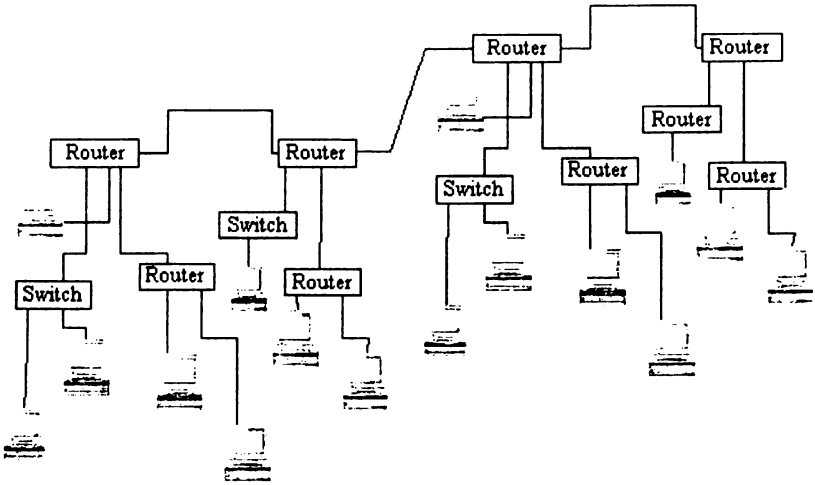


Рис. 12. Вариант 1

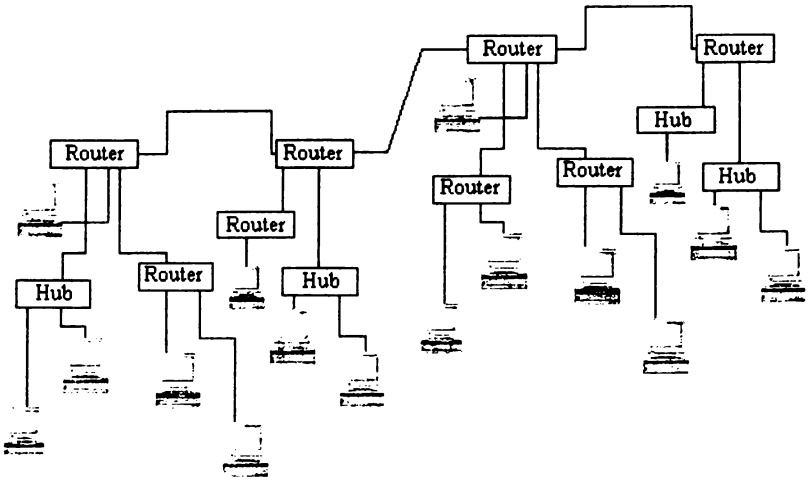


Рис. 13. Вариант 2

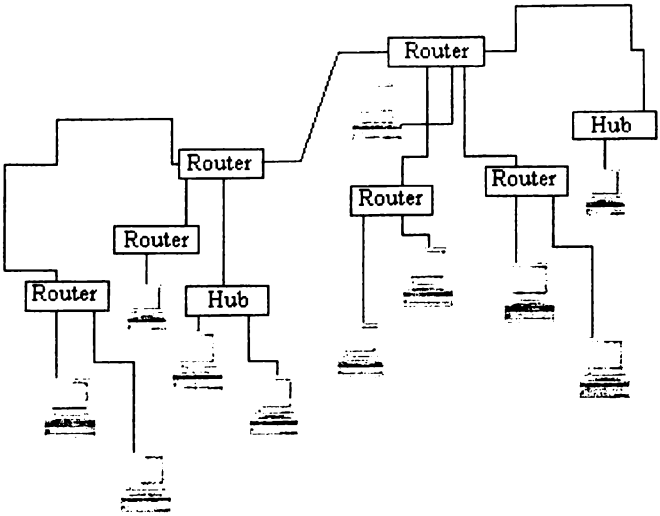


Рис. 14. Вариант 3

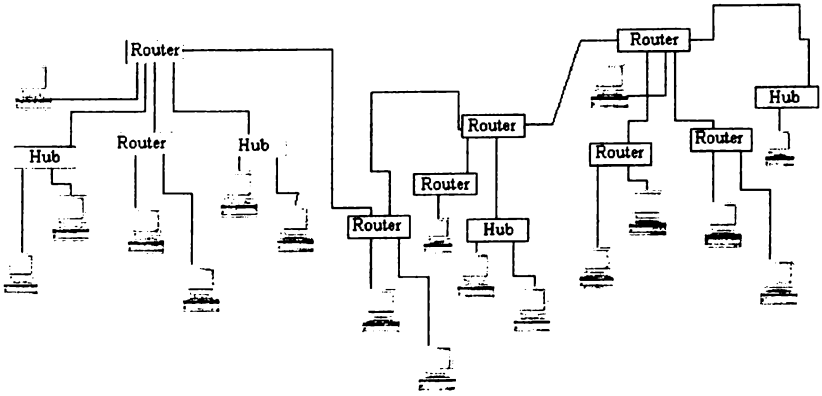


Рис. 15. Вариант 4

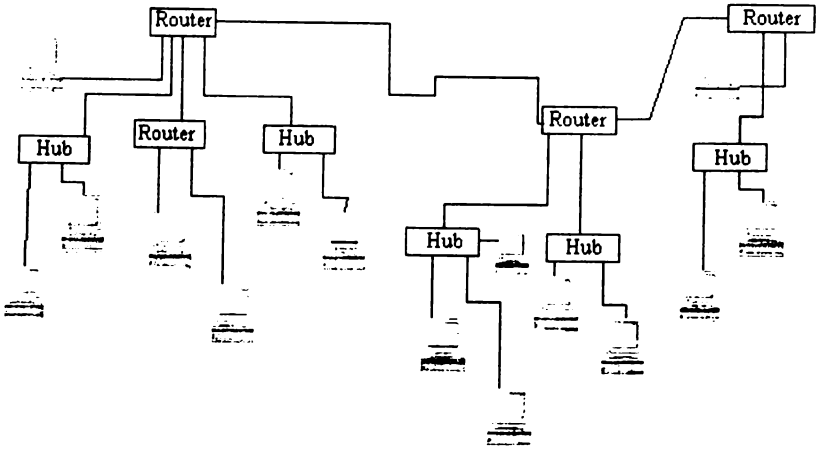


Рис. 16. Вариант 5

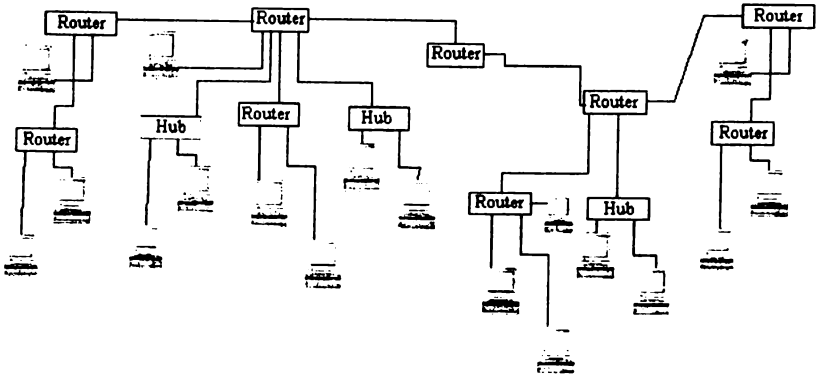


Рис. 17. Вариант 6

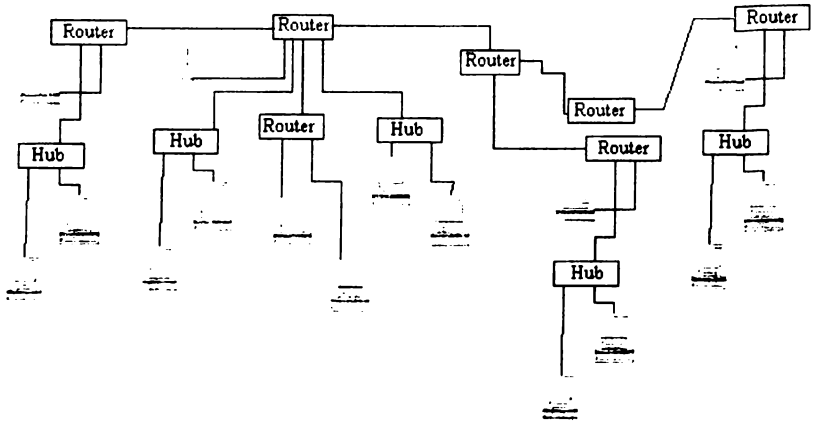


Рис. 18. Вариант 7

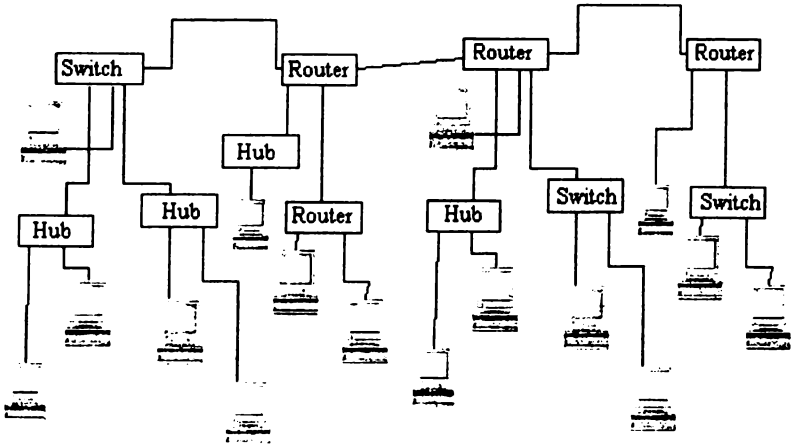


Рис. 19. Вариант 8

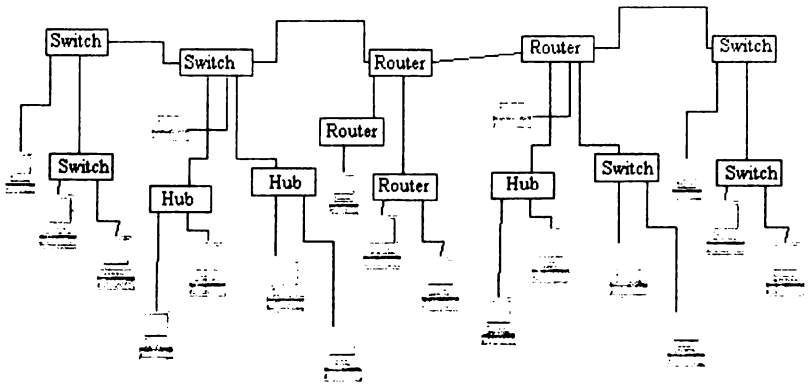


Рис. 20. Вариант 9

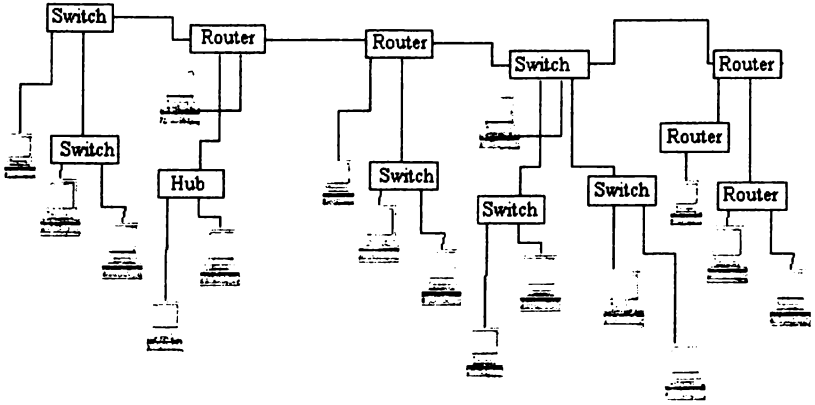


Рис. 21. Вариант 10

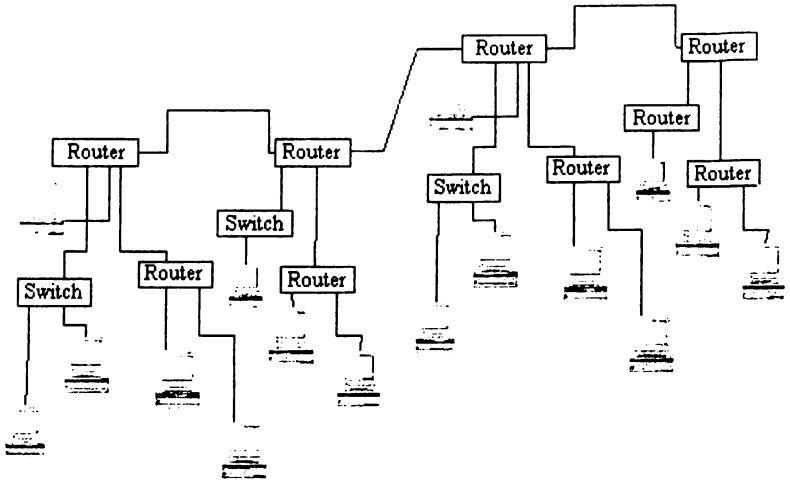


Рис. 22. Вариант 11

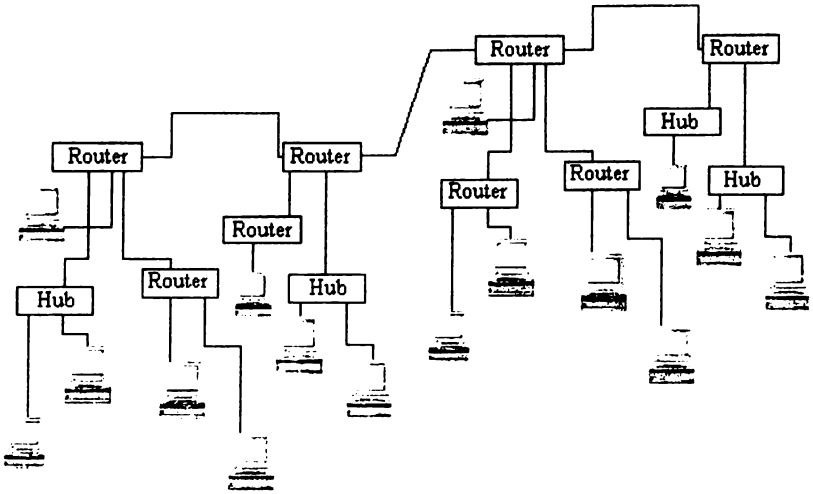


Рис. 23. Вариант 12

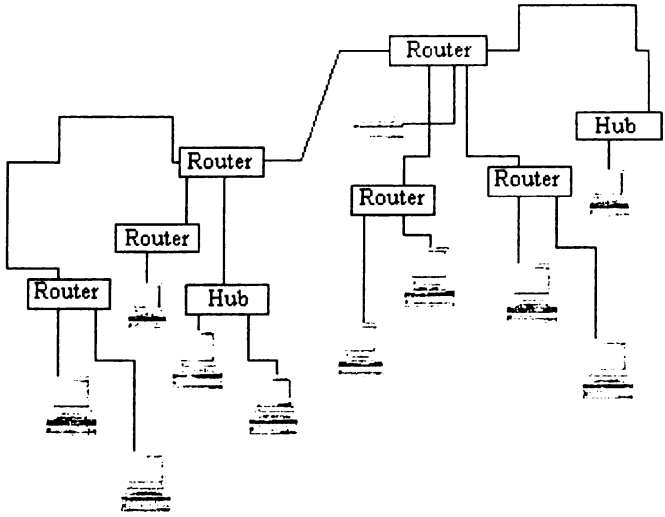


Рис. 24. Вариант 13

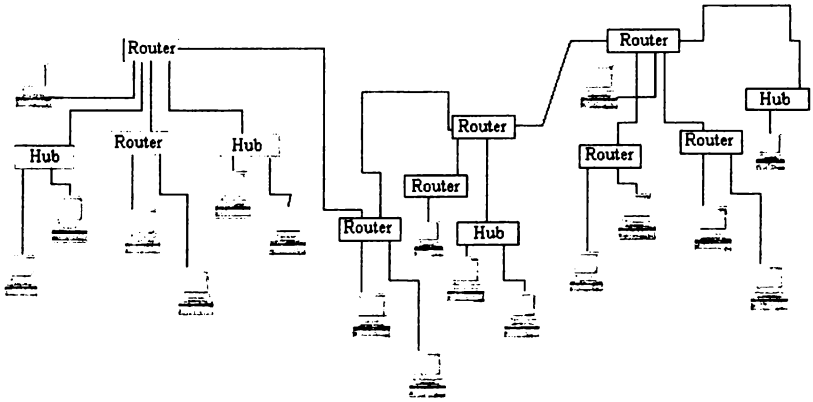


Рис. 25. Вариант 14

Резюме

Подсеть – это физический сегмент TCP/IP-сети, в котором используются IP-адреса с одним идентификатором сети. Механизм назначения IP-адресов для подсетей называется делением на подсети. Количество бит, отводимых для маски подсети, определяет максимальное число подсетей и узлов в них.

Вопросы и задания для самоконтроля

1. Дайте определение понятия «подсеть».
2. Дайте определение понятия «механизм деления на подсети».
3. Каким образом подсети соединяются между собой?
4. Перечислите основные требования для деления сети на подсети.
5. Для чего при делении сети на подсети необходимо задавать больше бит для маски подсети?

Глава 8. Разбиение сети на подсети масками одинаковой длины

Основные понятия и определения

Перед тем как начать разрабатывать сеть на базе протокола IP, сетевому администратору необходимо ответить на следующие вопросы:

1. Сколько подсетей требуется?
2. Сколько хостов существует в наибольшей подсети?

Первый этап процесса планирования сети для организации – определение *максимального количества требуемых подсетей*. Данное значение округляется до ближайшей степени числа «2» (например, 9 (подсетей) $\leqslant 2^4$). Затем следует убедиться в том, что выделенный организации класс адреса предоставляет достаточное количество бит, необходимых для формирования подсетей[1].

Второе, что необходимо сделать, – определить *шаг сети* (шаг сети – это номер последнего установленного бита в октете, которым заканчивается маска). Для этого необходимо определить порядковый номер последнего установленного бита в двоичной записи маски.

Если маска **255.255.255.224 (11111111.1111111.11111111.11100000)**, то номер последнего установленного бита в четвертом октете равен **6**. $2^6 = 32$, таким образом, шаг сети равен **32**.

Правила определения диапазонов адресов подсети:

1. Первое значение диапазона допустимых значений IP-адресов на 1 больше адреса сети.

[1] Степень двойки – это то количество бит, которое необходимо добавить к старой маске подсети.

2. Последнее значение допустимых IP-адресов на 2 меньше следующего адреса сети.

3. Если значение на 1 меньше следующего адреса сети, это широковещательный адрес.

Пример 1

Даны IP-адрес **202.185.10.0** и маска **255.255.255.0**. Необходимо разбить данную сеть на пять подсетей и для каждой подсети указать диапазон допустимых IP-адресов.

Решение

Этап 1. Определяем максимальное количество требуемых подсетей. Данное значение округляется до ближайшей степени числа «2».

5 (подсетей) $\leqslant 2^3$; следовательно, максимальное количество подсетей равно 8.

Этап 2. Определяем количество бит, которое необходимо добавить к маске подсети (смотрим на степень двойки), и получаем новую маску.

По условию маска равна 24 единицам, следовательно, **255.255.255.0 – 11111111.11111111.11111111.00000000**. Добавляем 3 бита к маске **24** и получаем маску **27: 255.255.255.224 (11111111.11111111.11111111.11100000)**.

Этап 3. Определяем шаг сети.

Шаг сети равен 32, так как степень последнего установленного бита в четвертом октете маски равна 32.

Этап 4. Определяем адреса пяти подсетей с учетом шага сети:

I подсеть: **202.185.10.0/27**;

II подсеть: **202.185.10.32/27**;

III подсеть: **202.185.10.64/27**;

IV подсеть: **202.185.10.96/27**;

V подсеть: **202.185.10.128/27**.

Этап 5. Определяем диапазоны допустимых адресов в каждой подсети с учетом правил:

I подсеть: **202.185.10.1 – 202.185.10.30**;

II подсеть: **202.185.10.33 – 202.185.10.62**;

III подсеть: **202.185.10.65 – 202.185.10.94**;

IV подсеть: **202.185.10.97 – 202.185.10.126**;

V подсеть: **202.185.10.129 – 202.185.10.158**.

Этап 6. Получаем при разбиении сети на пять подсетей IP-адрес **202.185.10.0**, маску **255.255.255.224**. Определен диапазон допустимых адресов в каждой подсети:

I подсеть: **202.185.10.1 – 202.185.10.30**;

II подсеть: **202.185.10.33 – 202.185.10.62**;

III подсеть: **202.185.10.65 – 202.185.10.94**;

IV подсеть: **202.185.10.97 – 202.185.10.136**;

V подсеть: **202.185.10.129 – 202.185.10.158**.

Пример 2

Даны IP-адрес **25.102.0.0** и маска **255.252.0.0**. Необходимо разбить данную сеть на четыре подсети и для каждой подсети указать диапазон допустимых IP-адресов.

Решение

Этап 1. Определяем максимальное количество требуемых подсетей. Данное значение округляется до ближайшей степени числа 2.

4 (подсети) $\leqslant 2^2$; следовательно, максимальное количество подсетей равно 4.

Этап 2. Определяем количество бит, которое необходимо добавить к маске подсети (смотрим на степень двойки), и получаем новую маску.

По условию маска равна 14 единицам, следовательно, **255.252.0.0 – 11111111.11111100.00000000.00000000**. Добавляем два бита к маске **14** и получаем маску **16**: **255.255.0.0 (11111111.11111111.00000000.00000000)**.

Этап 3. Определяем шаг сети.

Степень последнего установленного бита во втором октете маски равна 1. Таким образом, шаг сети равен 1.

Этап 4. Определяем адреса четырех подсетей с учетом шага сети:

I подсеть: **25.102.0.0/16**;

II подсеть: **25.103.0.0/16**;

III подсеть: **25.104.0.0/16**;

IV подсеть: **25.105.0.0/16**.

Этап 5. Определяем диапазоны допустимых адресов в каждой подсети с учетом правил:

I подсеть: **25.102.0.1 – 25.102.255.254**;

II подсеть: **25.103.0.1 – 25.103.255.254**;

III подсеть: **25.104.0.1 – 25.104.255.254**;

IV подсеть: **25.105.0.1 – 25.105.255.254**.

Этап 6. Получаем при разбиении сети на четыре подсети IP-адрес **25.102.0.0,** маска **255.255.0.0**. Определен диапазон допустимых адресов в каждой подсети:

I подсеть: **25.102.0.1 – 25.102.255.254**;

II подсеть: **25.103.0.1 – 25.103.255.254**;

III подсеть: **25.104.0.1 – 25.104.255.254**;

IV подсеть: **25.105.0.1 – 25.105.255.254**.

✍Практическое задание

Даны IP-адрес и маска. При помощи масок одинаковой длины разбейте данную сеть на указанное количество подсетей и для каждой из пяти подсетей укажите диапазон допустимых IP-адресов:

1) **145.90.64.0/18** – 7 подсетей;

2) **15.32.0.0/11** – 11 подсетей;

3) **152.110.0.0/20** – 12 подсетей;

4) **56.192.0.0/14** – 6 подсетей;

5) **160.190.64.0/19** – 10 подсетей;

6) **105.128.0.0/10** – 14 подсетей;

7) **125.10.96.0/19** – 5 подсетей;

8) **5.64.0.0/13** – 17 подсетей;

9) **145.50.0.0/18** – 21 подсеть;

10) **192.168.10.64/26** – 10 подсетей;

11) **199.9.9/27** – 24 подсети;

12) **201.0.240.0/24** – 5 подсетей;

13) **178.192.0.0/16** – 8 подсетей;

14) **194.164.192.0/24** – 19 подсетей.

Резюме

Если Вы хотите разделить свою сеть на подсети, необходимо задать маску подсети. Это можно сделать так: преобразовать количество физических сегментов сети в двоичный формат; подсчитать требуемое для его двоичной записи число бит; перевести его в десятичный формат. Для задания маски подсети можно использовать больше восьми бит – это увеличит гибкость схемы адресации.

Вопросы и задания для самоконтроля

1. IP-адрес 15.0.0.0 был выделен для 54 подсетей. Распределите диапазон IP-адресов при помощи масок одинаковой длины. Укажите диапазоны допустимых значений IP-адресов для 2-й и 53-й подсетей.

2. У организации для создания корпоративных сетей есть адрес – 200.151.40.0/26. Определите максимальное количество подсетей, количество идентификаторов узлов каждой подсети.

3. Определите необходимую маску подсети для различных ситуаций (помните, что деление на подсети применяется не всегда):

- адрес класса A в локальной сети;
- адрес класса B в локальной сети, состоящей из 4000 узлов;
- адрес класса C в локальной сети, состоящей из 254 узлов;
- адрес класса A в сети, содержащей 6 подсетей;
- адрес класса B в сети, содержащей 126 подсетей.

4. Определите адрес класса A, если в настоящее время сеть содержит 30 подсетей, а в следующем году планируется увеличить их число до 65, причем в каждой подсети будет более 50000 узлов.

5. Определите маску подсети, соответствующую указанному диапазону IP-адресов:

- от 61.8.0.1 до 61.15.255.254;
- от 172.88.32.1 до 172.88.63.254;
- от 111.224.0.1 до 111.239.255.254;
- от 3.64.0.1 до 3.127.255.254;
- от 128.71.1.1 до 128.71.254.254;
- от 130.10.160.1 до 130.10.191.254;
- от 111.32.0.1 до 111.63.255.254;
- от 192.168.10.97 до 192.168.10.126.

Глава 9. Разбиение сети на подсети масками переменной длины

Основные понятия и определения

Маски подсети переменной длины используются для получения адреса на основе класса и преобразования его в более масштабируемый и менее расточительный диапазон адресов [3, с. 259]. Недостатком адресов на

основе классов является то, что они обычно предоставляют либо слишком большой, либо слишком маленький диапазон адресов для использования в большинстве ситуаций.

Предположим, некая компания имеет сеть, в которой после организации подсетей на основе адреса класса B с использованием 20-битной маски (**255.255.240.0**) будет получено 14 подсетей и 4094 хоста в каждой подсети. Но что делать, если компании не нужно в каждой из этих 14 подсетей такое количество IP-адресов? Если есть возможность не расходовать адреса (например, нужны две подсети по 4094 адреса в каждой и 12 подсетей по 250 адресов) [3, с. 592], то лучше применить *метод создания маски подсети переменной длины* (VLSM).

Метод VLSM предусматривает разбиение на подсети адресного пространства, основанного на использовании классов, а затем разбиение подсетей на подподсети до тех пор, пока не будет достигнуто требуемое количество хостов в каждой подсети.

✍Практические задания

1. Разбейте сеть на подсети, указывая шаг сети и IP-адрес третьей подсети:

1) **190.192.0.0/19** – 2 подсети;

2) **123.0.0.0/12** – 4 подсети;

3) **47.0.0.0/17** – 4 подсети;

4) **56.192.0.0/13** – 6 подсетей;

5) **202.224.128.0/26** – 7 подсетей;

6) **222.162.248.0/27** – 3 подсети;

7) **22.0.0.0/14** – 3 подсети;

8) **134.0.0.0/19** – 4 подсети;

9) **63.0.0.0/11** – 2 подсети;

10) **75.0.0.0/21** – 4 подсети;

11) **132.0.0.0/17** – 6 подсетей;

12) **80.0.0.0/17** – 6 подсетей;

13) **108.0.0.0/19** – 5 подсетей;

14) **167.248.0.0/24** – 7 подсетей.

2. Разбейте адресное пространство на подсети, используя маски подсетей переменной длины (рис. 26–35):

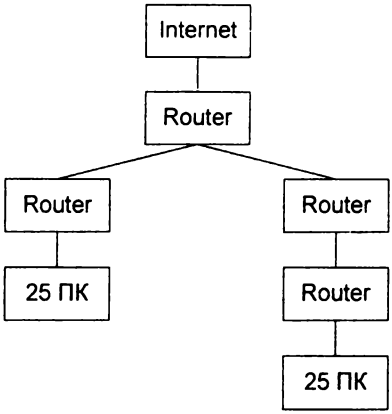


Рис. 26. Вариант 1.
IP-адрес 171.2.0.0; маска 255.255.0.0

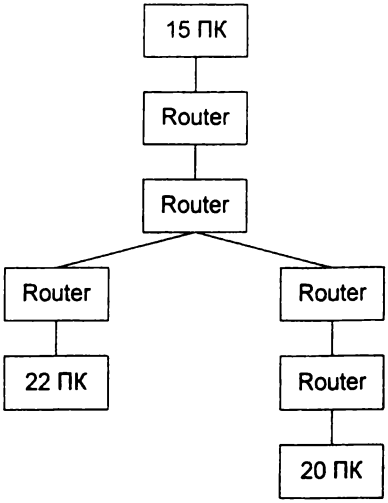


Рис. 27. Вариант 2.
IP-адрес 131.42.0.0; маска 255.255.128.0

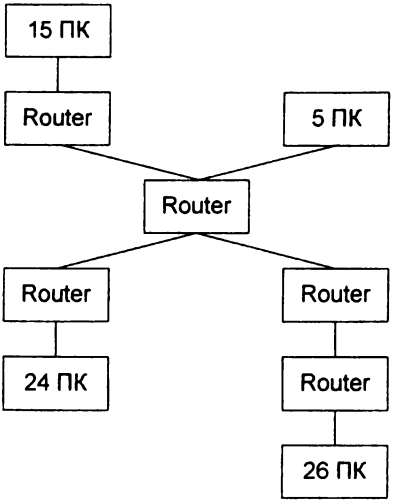


Рис. 28. Вариант 3.
IP-адрес 189.142.128.0; маска 255.255.128.0

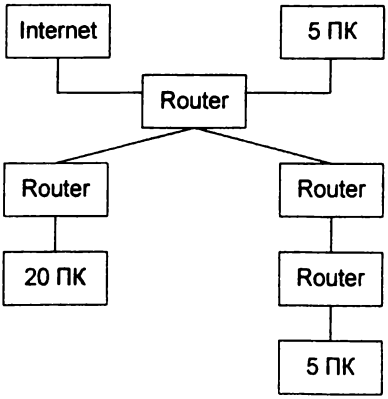


Рис. 29. Вариант 4.
IP-адрес 189.142.128.0; маска 255.255.128.0

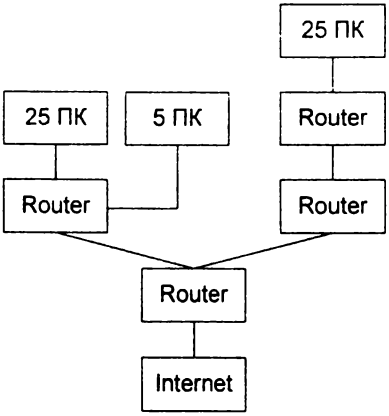


Рис. 30. Вариант 5.
IP-адрес 13.192.0.0; маска 255.224.0.0

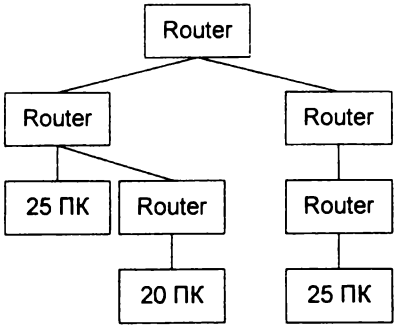


Рис. 31. Вариант 6.
IP-адрес 101.128.0.0; маска 255.192.0.0

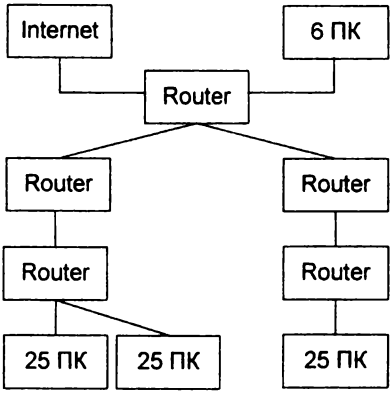


Рис. 32. Вариант 7.
IP-адрес 119.32.0.0; маска 255.255.0.0

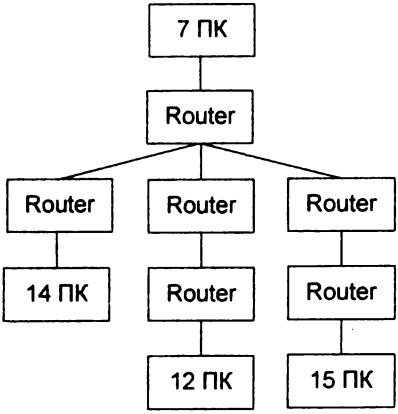


Рис. 33. Вариант 8.
IP-адрес 91.0.0.0; маска 255.0.0.0

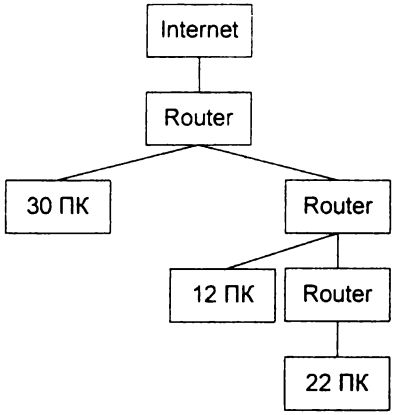


Рис. 34. Вариант 9.
IP-адрес 144.142.0.0; маска 255.255.0.0

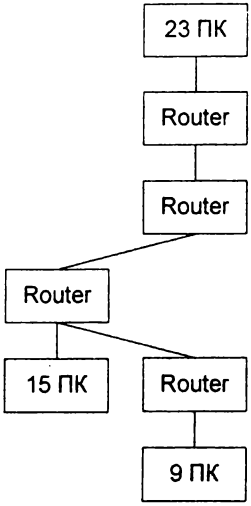


Рис. 35. Вариант 10.
IP-адрес 193.162.0.0; маска 255.255.128.0

Резюме

Маска подсети переменной длины используется для получения адреса на основе класса и преобразования его в более масштабируемый и менее расточительный диапазон адресов. Метод VLSM предусматривает разбиение на подсети адресного пространства, основанного на использовании классов, а затем разбиение подсетей на подподсети до тех пор, пока не будет достигнуто требуемое количество хостов в каждой подсети.

Вопросы и задания для самоконтроля

1. Укажите недостаток адресов на основе классов.
2. Для чего используются маски подсети переменной длины?
3. Каким образом разбивается сеть при помощи маски переменной длины?

Глава 10. Объединение нескольких сетей

Основные понятия и определения

Чтобы пространство идентификаторов сетей не было исчерпано, организации, координирующие развитие Интернета, разработали схему *объединения сетей* (supernetting) [1, с. 206].

При объединении сетей часть бит идентификатора сети маскируется как идентификатор узла – это увеличивает эффективность маршрутизации. Например, вместо того чтобы предоставить один идентификатор сети класса B организации, имеющей 2000 узлов, InterNIC выделяет ей восемь идентификаторов сетей класса C. Каждая такая сеть может содержать до 254 узлов, что в совокупности обеспечивает 2032 идентификатора узлов. Таким образом экономятся идентификаторы сетей класса B.

Однако при использовании этой технологии возникает новая проблема. Для реализации обычных механизмов маршрутизации необходимо, чтобы маршрутизаторы в сети Интернет поддерживали в своих таблицах еще семь дополнительных записей – это требуется для направления пакетов в сеть организации. Чтобы разгрузить маршрутизаторы Интернета, была разработана *технология бесклассовой маршрутизации* (Classless Inter-Dornain Routing – CIDR), которая позволяет объединить все восемь записей таблицы маршрутизации в одну, относящуюся одновременно ко всем выделенным организации сетям класса C.

Таким образом, было выделено восемь идентификаторов сетей класса C – с **220.78.168.0** до **220.78.175.0**. Запись в таблице маршрутизации формируется следующим образом:

- идентификатор сети (например, **220.78.168.0**);
- маска подсети (**255.255.248.0**);
- маска подсети в двоичном виде

11111111.11111111.11111000.00000000.

При объединении сетей та сеть, для которой предназначен пакет, определяется выполнением операции логического «И» с использованием маски подсети и IP-адреса получателя. Если результат операции совпадает с идентификатором сети, пакет отправляется в соответствующую сеть.

Резюме

При объединении сетей часть бит идентификатора сети маскируется как идентификатор узла для повышения эффективности маршрутизации.

Вопросы и задания для самоконтроля

1. В каком случае применяется способ деления сети на подсети при объединении сетей?

2. Для чего была разработана технология бесклассовой маршрутизации?

3. Что произойдет, если при объединении сети идентификатор сети совпадет с идентификатором узла?

Глава 11. Отображение доменных имен на IP-адреса

Компьютерам, работающим в сети Интернет, принято присваивать специальные имена. Эта система имен получила название *доменной системы имен* (Domain Name System – DNS). Для реализации DNS был разработан специальный протокол прикладного уровня.

В сети Интернет доменная система имен имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей (на практике их количество редко превышает пять).

Отдельные части имени называют *доменами*. Старшая часть имени всегда стоит первой справа – она носит название *домена первого уровня*. Следом за ней идет домен второго, более низкого, уровня и т. д. Замыкает имя стоящая слева младшая часть, которая соответствует конечному узлу.

Домены второго, третьего и т. д. уровней иногда называют *поддоменами вышестоящего домена*. Имя поддомена назначает администратор вышестоящего домена. Например, www.microsoft.com. В данном случае домен первого уровня – com. По домену первого уровня можно определить местоположение (страну) или профиль организации. Имена верхних доменов зафиксированы в международном стандарте (ISO 3166). Так, первоначально для США было выделено пять доменов верхнего уровня:

- gov – для правительственных организаций;
- edu – для образовательных организаций;
- mil – для военных организаций;
- org – для общественных некоммерческих организаций;
- net – для организаций, предоставляющих сетевые услуги.

Кроме того, каждая страна имеет свой двухбуквенный домен верхнего уровня.

Ответственность за присвоение имен несет администратор домена следующего уровня: это обеспечивает уникальность имени компьютера в сети Интернет.

Служба DNS – это централизованная служба, основанная на распределенной базе данных, содержащей взаимно однозначное отображение «доменное имя – IP-адрес компьютера»[1].

Служба DNS использует в своей работе протокол типа «клиент – сервер». DNS-клиент обращается к DNS-серверу с запросом о разрешении доменного имени в IP-адрес. Для каждого домена имен создается свой DNS-сервер. Этот сервер хранит таблицы отображения «доменное имя – IP-адрес» для домена, включая все поддомены.

В основании иерархического дерева имен (над доменами первого уровня) находится так называемый *корневой домен*, который управляется центром InterNIC.

Существуют две основные процедуры разрешения доменных имен в IP-адреса: интерактивная и рекурсивная. Практически в Интернете используется рекурсивная процедура.

Вопросы и задания для самоконтроля

1. Расшифруйте аббревиатуру DNS.
2. Каково назначение доменов первого уровня?
3. Определите в адресе www.intuit.ru домены и поддомены.
4. Каково назначение службы DNS?

Глава 12. Протокол ARP – протокол разрешения адресов

Основные понятия и определения

Протокол IP действует на сетевом уровне модели OSI, поэтому *IP-адреса называются сетевыми*. Они предназначены для передачи сообщений в составных сетях, связывающих подсети, которые построены на различных локальных или глобальных сетевых технологиях, например, Ethernet или ATM. Однако для непосредственной передачи сообщения в рамках одной подсети вместо IP-адреса нужно использовать локальный

[1] Первое успешное тестирование DNS было проведено 23 июня 1983 г. в Институте информационных наук (ISI) Университета Южной Калифорнии. DNS разработали сотрудники института Пол Мокапетрис и Джон Постел, решившие создать новый вид каталога хостов интернет-сети, в которой в то время насчитывалось в общей сложности 200 компьютеров. До создания DNS адреса и имена всех машин хранились в центральном каталоге. П. Мокапетрис и Д. Постел изобрели систему доменов, дававшую свободу подключения новых машин к Интернету и присвоения им имен.

(аппаратный) адрес технологии канального уровня, чаще всего MAC-адрес. При этом к IP-пакету добавляются заголовок и концевик кадра канального уровня (в заголовке указываются MAC-адреса источника и приемника кадра) (рис. 36).

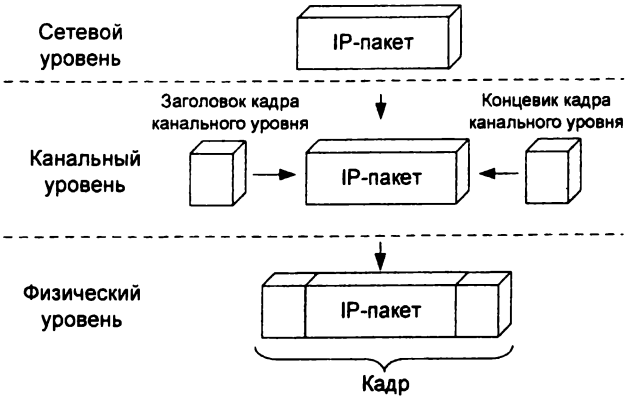


Рис. 36. Формирование кадра на канальном уровне

При формировании кадра канального уровня возникает проблема: каким образом по известному IP-адресу определить соответствующий MAC-адрес? Указанная проблема решается при помощи *протокола разрешения адресов* (Address Resolution Protocol – ARP). Он определяет MAC-адреса следующим образом:

1. Осуществляется рассылка всем узлам сети специального кадра, который называется *ARP-запрос* (ARP Request). В этом кадре содержится IP-адрес компьютера, у которого требуется узнать MAC-адрес. Каждый узел сети принимает ARP-запрос и сравнивает IP-адрес из запроса со своим IP-адресом. Если адреса совпадают, узел высылает *ARP-ответ* (ARP Reply), содержащий требуемый MAC-адрес.

2. Результаты своей работы протокол ARP сохраняет в специальной таблице, хранящейся в оперативной памяти, которая называется *ARP-кэш*. При необходимости разрешения IP-адреса протокол ARP сначала ищет IP-адрес в ARP-кэше и только в случае отсутствия нужной записи производит рассылку ARP-запроса.

Записи в ARP-кэше могут быть двух типов: *статические* и *динамические* (табл. 6). Статические записи заносятся в кэш администратором при помощи утилиты arp с ключом /s. Динамические записи помещаются в кэш после полу-

ченного ARP-ответа и по истечении двух минут удаляются. Удаление происходит для того, чтобы при перемещении компьютера с MAC-адресом, занесенным в таблицу, в другую подсеть, кадры не отправлялись бессмысленно в сеть.

Таблица 6

ARP-кэш

IP-адрес	MAC-адрес	Тип записи
192.168.1.1	03–E8–48–A1–57–7B	Статический
192.168.1.2	03–E8–48–A1–43–88	Динамический
192.168.1.3	03–E8–48–A1–F8–D9	Динамический

Процесс получения по известному IP-адресу MAC-адреса называется *разрешением IP-адреса.*

Иногда требуется по известному MAC-адресу найти IP-адрес (например, при начале работы компьютера без жесткого диска, у которого есть MAC-адрес сетевого адаптера, и ему нужно определить свой IP-адрес). В этом случае используется *реверсивный протокол RARP* (Reverse ARP).

Резюме

Все устройства в локальной сети должны следить за ARP-запросами, но только те устройства, чей IP-адрес совпадает с IP-адресом, содержащимся в запросе, должны откликнуться путем сообщения своего MAC-адреса устройству, создавшему запрос (источнику). Если IP-адрес устройства совпадает с IP-адресом, содержащимся в ARP-запросе, устройство откликается, посылая источнику свой MAC-адрес. Эта процедура называется ARP-ответом. Если источник не может обнаружить MAC-адрес пункта назначения в своей ARP-таблице, он создает ARP-запрос и отправляет его в широковещательном режиме всем устройствам в сети. Если устройство не знает собственного IP-адреса, оно использует протокол RARP. Когда устройство, создавшее RARP-запрос, получает ответ, оно копирует свой IP-адрес в кэш-память, где этот адрес будет храниться на протяжении всего сеанса работы.

Вопросы и задания для самоконтроля

1. Какой интернет-протокол используется для отображения IP-адресов на MAC-адреса?
2. Кто инициирует ARP-запросы?
3. Как называются две части заголовка кадра?
4. Почему важна актуальность ARP-таблиц?
5. Зачем осуществляются RARP-запросы?

Раздел 2. ИТОГОВАЯ ПРАКТИЧЕСКАЯ РАБОТА

Приведенные ниже вопросы и задания помогут вам лучше усвоить основной материал учебного пособия. Если вы не сумеете ответить на вопрос, повторите необходимый материал.

1. Сколько бит содержит IP-адрес?

2. Какую роль в IP-адресе играет номер сети?

3. Какую роль в IP-адресе играет номер хост-машины?

4. Какое десятичное число является эквивалентом двоичного числа **11111111?**

5. Что такое подсеть?

6. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

7. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему? Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

8. Когда необходим уникальный идентификатор сети?

9. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

10. Каково назначение маски подсети?

11. Когда необходима маска подсети?

12. Когда маска подсети используется по умолчанию?

13. Когда необходимо задать специальную маску подсети?

14. Определите, какие IP-адреса из приведенных ниже не могут быть назначены узлам, и объясните, почему они не являются корректными (если маска не указана, то она считается стандартной для класса адреса):

а) **111.256.4.0**;

б) **231.200.1.1**;

в) **127.1.1.1**;

г) **167.255.143.255/20**;

д) **179.12.34.55** mask: **255.225.0.0**.

15. Охарактеризуйте приведенные IP-адреса согласно сетевой маске (адрес узла, идентификатор сети или широковещательный запрос, неверная комбинация IP-адрес/маска), объясните свое решение и определите, сколько узлов позволяет идентифицировать маска подсети:

а) **147.254.34.12**, mask: **255.255.255.232**;

б) **150.124.15.1**, mask: **255.255.192.1**;

в) **136.250.0.1**, mask: **255.255.0.0**;

г) **192.56.2.0**, mask: **255.255.192.0**.

16. Определите класс сети и максимальное количество узлов сети, для которых задана следующая маска:

а) **255.192.0.0**;

б) **255.255.240.0**;

в) **255.255.192.0**.

17. Определите адрес сети, зная IP-адрес и маску:

а) **189.17.30.52**, mask: **255.255.192.0**;

б) **199.9.8.0**, mask: **255.255.255.224**.

18. Рассмотрите схему сети (рис. 37), определите, какие проблемы могут возникнуть, как они могут проявиться. Ответьте на следующие вопросы:

1) Для каких узлов маска подсети задана неправильно?

2) Как неправильное значение маски подсети влияет на работу этих узлов?

3) Каково правильное значение маски подсети?

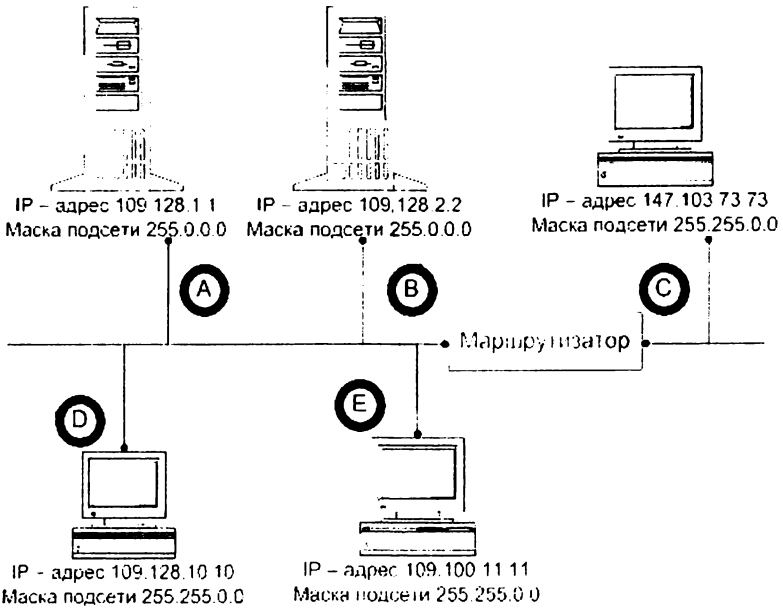


Рис. 37. Пример схемы сети

19. Какая часть адреса **182.54.4.233** обозначает подсеть?

20. Если сеть класса С разделена на подсети и имеет маску

255.255.255.192,

то какое максимальное количество подсетей можно создать?

21. IP-адрес хост-машины – **192.168.5.121**, маска подсети –

255.255.255.248.

Какой адрес имеет сеть этого хоста?

22. Какая часть IP-адреса **205.129.12.5** представляет хост-машину?

23. Какая часть IP-адреса **129 219.51.18** представляет сеть?

24. Пусть IP-адрес некоторого узла подсети **198.65.12.67**, а маска этой подсети – **255.255.255.240**. Определите номер подсети. Какое максимальное число узлов может быть в этой подсети?

25. Для IP-адреса **129.64.134.5** указана маска **255.255.128.0**. Определите номер подсети и номер узла.

26. Номер сети, который получил администратор от поставщика услуг, – **129.44.0.0**. В качестве маски было выбрано значение **255.255.192.0**. Сколько подсетей может организовать администратор?

27. Маска сети **255.255.255.248**, IP-адрес **192.168.1.219**. Определите адрес сети и максимальное число сетевых устройств, которые могут быть подключены к данной сети.

28. Маска сети **255.255.255.248**, IP-адрес **192.168.1.219**. Определите широковещательный адрес (broadcast) для данной сети.

Заключение

В результате работы с данным учебным пособием вы познакомились с основными правилами построения сетей на базе объединения подсетей; с понятиями «IP-адрес», «класс IP-адреса», «маска подсети».

Также вы научились определять корректность IP-адресов; присваивать IP-адреса узлам; выявлять проблемы, связанные с IP-адресацией.

Далее вы можете перейти к изучению материалов программно-методических комплексов «Принципы функционирования глобальных компьютерных сетей», «Глобальная компьютерная сеть Internet» и «Корпоративные компьютерные сети».

Библиографический список

1. *Джонс А.* Руководство системного администратора Widows. Для профессионалов / А. Джонс. Санкт-Петербург: Питер, 2001. 368 с.

2. *Кузин А. В.* Компьютерные сети: учебное пособие / А. В. Кузин. Москва: Форум: Инфра-М, 2011. 192 с.

3. *Кульгин М.* Технологии корпоративных сетей: энциклопедия / М. Кульгин. Санкт-Петербург: Питер, 2000. 704 с.

4. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. 4-е изд. Санкт-Петербург: Питер, 2010. 944 с.

5. *Основы* современных компьютерных технологий: учебник / под ред. А. Д. Хомоненко. Санкт-Петербург: Корона-Принт, 2005. 672 с.

6. *Соловьева Л. Ф.* Сетевые технологии: учебный практикум / Л. Ф. Соловьева. Санкт-Петербург: БХВ-Петербург, 2004. 416 с.

7. *Столлингс В.* Передача данных /В. Столлингс. 4-е изд. Санкт-Петербург: Питер, 2004. 750 с.

8. *Управление* сетевой средой Microsoft Windows 2000: учебный курс MCSA/MCSE: перевод с английского / Microsoft Corporation. Москва: Русская редакция, 2003. 896 с.

Приложение

Таблицы преобразования

Таблица 1

Маски подсетей для сетей класса А,
заданные с использованием одного октета

Количество подсетей	Требуемое число бит	Маска подсети	Количество узлов в подсети
0	1	Не используется	Не используется
2	2	255.192.0.0	4 194 302
6	3	255.224.0.0	2 097 150
14	4	255.240.0.0	1 048 574
30	5	255.248.0.0	524 286
62	6	255.252.0.0	262 142
126	7	255.254.0.0	131 070
254	8	255.255.0.0	65 534

Таблица 2

Маски подсетей для сетей класса В,
заданные с использованием одного октета

Количество подсетей	Требуемое число бит	Маска подсети	Количество узлов в подсети
0	1	Не используется	Не используется
2	2	255.255.192.0	16 382
6	3	255.255.224.0	8 190
14	4	255.255.240.0	4 094
30	5	255.255.248.0	2 046
62	6	255.255.252.0	1 022
126	7	255.255.254.0	510
254	8	255.255.255.0	254

Таблица 3

Маски подсетей для сетей класса С,
заданные с использованием одного октета

Количество подсетей	Требуемое число бит	Маска подсети	Количество узлов в подсети
Не используется	1	Не используется	Не используется
2	2	255.255.255.192	62
6	3	255.255.255.224	30
14	4	255.255.255.240	14
30	5	255.255.255.248	6
62	6	255.255.255.252	2
Не используется	7	Не используется	Не используется
Не используется	8	Не используется	Не используется

Оглавление

Предисловие ... 3
Раздел 1. IP-адресация и подсети ... 4
Глава 1. Адресация в TCP/IP-сетях ... 4
Вопросы и задания для самоконтроля ... 5
Глава 2. IP-адрес ... 5
Вопросы и задания для самоконтроля ... 9
Глава 3. Классы IP-адресов ... 10
Вопросы и задания для самоконтроля ... 14
Глава 4. Назначение IP-адресов ... 14
Вопросы и задания для самоконтроля ... 19
Глава 5. IP-адреса и маски подсетей ... 19
Вопросы и задания для самоконтроля ... 22
Глава 6. IP-адресация в IP версии 6.0 ... 22
Вопросы и задания для самоконтроля ... 29
Глава 7. Общие сведения о подсетях ... 29
Вопросы и задания для самоконтроля ... 38
Глава 8. Разбиение сети на подсети масками одинаковой длины ... 38
Вопросы и задания для самоконтроля ... 42
Глава 9. Разбиение сети на подсети масками переменной длины ... 42
Вопросы и задания для самоконтроля ... 46
Глава 10. Объединение нескольких сетей ... 47
Вопросы и задания для самоконтроля ... 48
Глава 11. Отображение доменных имен на IP-адреса ... 48
Вопросы и задания для самоконтроля ... 49
Глава 12. Протокол ARP – протокол разрешения адресов ... 49
Вопросы и задания для самоконтроля ... 51
Раздел 2. Итоговая практическая работа ... 52
Заключение ... 55
Библиографический список ... 56
Приложение. Таблицы преобразования ... 57

Учебное издание

Ломовцева Наталья Викторовна
Волкова Любовь Викторовна

IP-АДРЕСАЦИЯ

Учебное пособие

Редактор О. Е. Мелкозерова
Компьютерная верстка Н. А. Ушениной

Печатается по постановлению
редакционно-издательского совета университета

Подписано в печать 20.02.12. Формат 60×84/16. Бумага для множ. аппаратов. Печать плоская. Усл. печ. л. 4,5. Уч.-изд. л. 4,8. Тираж 200 экз. Заказ № 99.
Издательство Российского государственного профессионально-педагогического университета. Екатеринбург, ул. Машиностроителей, 11.

Отпечатано ООО "ТРИКС"
Свердловская обл., г. Верхняя Пышма, ул. Феофанова, 4
www.printvp.ru