ФГБОУ ВО «Воронежский государственный технический университет»

Кафедра систем автоматизированного проектирования и информационных систем

ПРОТОКОЛЫ И АЛГОРИТМЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СИСТЕМ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторным работам по дисциплине "Современные стандарты информационного взаимодействия систем" для студентов направления 09.03.02 «Информационные системы и технологии» очной формы обучения

Воронеж 2019

1. Стек протоколов TCP/IP

Стек протоколов TCP/IP – набор иерархически упорядоченных протоколов, предназначенных для построения транспортной системы, объединяющей разнородные сети в единую систему передачи данных. Под разнородностью сетей понимают различие в технологиях построения “локальных” сетей на физическом и канальном уровнях модели OSI. В настоящее время протоколы стека TCP/IP являются основными протоколами передачи данных в сети Интернет. Название стека происходит от названия базовых протоколов: протокола управления передачей TCP (Transmission Control Protocol) и межсетевого протокола IP (Internet Protocol). Часто, объединяемые сети называют подсетями, а объединенную сеть – интерсетью или сетью интернет. Технические спецификации протоколов сети Интернет оформляются в виде документов RFC (Request for Comments). Документы RFC публикуются в сети Интернет, например, на сайте http://www.rfc–editor.org.

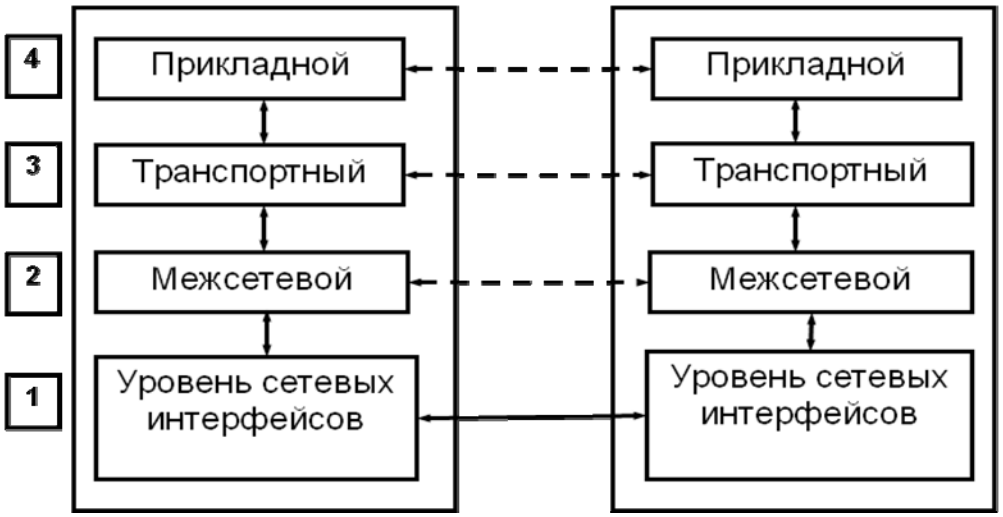

Рис. 2. Структура стека TCP/IP

Модель стека протоколов TCP/IP состоит из четырех уровней (RFC 1122) .

1. Уровень сетевых интерфейсов обеспечивает объединение в составную сеть сетей, построенных на “локальных” технологиях. Под локальными технологиями понимают технологии построения локальных сетей (подсетей) или каналов точка–точка. Основные функции этого уровня:

- инкапсуляция IP-пакетов в кадры технологий локальных и глобальных сетей;
- преобразование адресов межсетевого уровня в адреса, используемые в “локальных” технологиях.

Отметим, что в отличие от физического и канального уровней модели OSI, уровень сетевых интерфейсов не определяет принципы передачи данных на физическом и канальном уровнях.

2. Межсетевой уровень отвечает за выбор маршрутов продвижения пакетов и передачу пакетов дейтаграммным способом (без установления соединения).

Протоколы межсетевого уровня:

- Основной протокол IP (Internet Protocol) – обеспечивает передачу пакетов между узлами составной сети дейтаграммным способом (RFC 791);

- Протоколы маршрутизации – предназначены для обмена маршрутизаторами информацией о конфигурации сети и построения таблиц маршрутизации. Примеры протоколов маршрутизации: BGP (RFC 4271), OSPF (RFC 2328), RIP (RFC 1058);
- Протокол управления группами IGMP (Internet Group Management Protocol) – предназначен для организации групповых рассылок (multicast). IGMP используется для передачи данных одновременно нескольким узлам сети, например, для организации теле или радиовещания (RFC 3376);
- Межсетевой протокол передачи управляющих сообщений ICMP (Internet Control Message Protocol). Основное назначение ICMP – передача служебных сообщений с информацией об ошибках в работе стека TCP/IP (RFC 950).

В настоящее время наиболее распространенным протоколом для организации межсетевого взаимодействия является IP протокол версии 4 (IPv4). Постепенно внедряется IP протокол версии 6 (IPv6).

3. Транспортный уровень предназначен для передачи данных между прикладными процессами. В зависимости от требований предъявляемых к качеству передачи, протоколы транспортного уровня могут обеспечивать доставку данных или дейтаграммным способом или с использованием механизмов надежной доставки.
Основные протоколы транспортного уровня:

- Протокол управления передачей TCP (Transmission Control Protocol) – обеспечивает надежную передачу сообщений между удаленными прикладными процессами. Для реализации надежной доставки используются логические соединения, контроль целостности передаваемых данных, контроль доставки данных и управление потоком передаваемых данных (RFC 793);
- Протокол пользовательских дейтаграмм UDP (User Datagram Protocol) – обеспечивает передачу данных дейтаграммным способом, выполняет функции связующего звена между сетевым уровнем и прикладными процессами (RFC 768).

4. Прикладной уровень предоставляет приложениям высокоуровневые протоколы обеспечивающие преобразование форматов передаваемых данных, поддержку сессий взаимодействия прикладных процессов, доступ к стандартным сетевым службам и.т.д. Примеры протоколов: FTP (RFC 959), HTTP (RFC1945), IMAP (RFC3501), POP3 (RFC1939), SNMP (RFC1155), SMTP (RFC821), SSH (RFC4251), LDAP (RFC4510).

2. IP протокол версии 4

Основная функция IP-протокола – передача пакетов между узлами составной сети дейтаграммным способом. IP-протокол обеспечивает доставку пакетов между узлами сети без установления соединения, контроля доставки, контроля целостности данных и управления потоком пакетов (протокол не гарантирует надежную доставку пакета).

Единицей передачи данных в IP-протоколе является IP-пакет. IP-пакет состоит из заголовка и поля данных. Заголовок может иметь размер от 20 до 60 байт и содержит служебную информацию IP-протокола. Поле данных содержит передаваемые данные.

Заголовок состоит из следующих полей:

Рис. 2. Структура заголовка IP-пакета

- **Версия** (4 бита) – указатель версии IP-протокола. В настоящее время наибольшее распространение получил протокол IP версии 4 (IPv4).
- **Длина** (4 бита) – длина заголовка пакета, измеренная в 32–битных словах. Обычно заголовок имеет длину 20 байт, но может быть увеличен до 60 байт за счет поля “Опции”.
- **Дифференцированное обслуживание** (8 бит) – поле предназначено для указания приоритета пакета и критерия выбора маршрута. В соответствии с RFC 791 до 1998 г. это поле называлось “Тип сервиса”, в RFC 2474 было принято новое название “Дифференцированное обслуживание”.

  В соответствии с RFC 791, первые три бита поля “Тип сервиса” предназначены для указания приоритета (срочности) пакета. Эти биты принимают значения от 0 (низкий приоритет) до 7 (высокий приоритет). Маршрутизаторы, учитывающие приоритет пакета, обрабатывают в первую очередь пакеты с более высоким приоритетом.
  Следующие три бита используются для указания критерия выбора маршрута.
  Варианты интерпретации значений 6,7 и8 битов:

  1. минимизация задержки пакета;
  2. максимизация пропускной способности;
  3. максимизация надежности доставки.

  В соответствии с RFC 2474, интерпретация первых шести битов поля “Дифференцированное обслуживание” зависит от значений четвертого, пятого и шестого битов (последние два бита зарезервированы). Если четвертый, пятый и шестой биты равны 0, первые три бита интерпретируются также, как биты приоритета поля “Тип сервиса”. Если пятый и шестой биты не равны 0, первые шесть бит определяют различные классы трафика.
- **Длина пакета** (2 байта) – используется для указания общей длины пакета. Длина пакета ограничена разрядностью этого поля и не может превышать 65535 байт. В большинстве сетей используются пакеты длиной 1500 байт (максимальный размер поля данных кадра Ethernet II).

- **Идентификатор пакета** (2 байта) – используется для указания IP-пакетов, являющихся фрагментами некоторого исходного IP-пакета. Все фрагменты одного пакета имеют одинаковое значение этого поля.
- **Флаги** – это поле используется для указания признаков фрагментации пакета. Длина поля 3 бита.
- **Смещение фрагмента** (13 бит) – используется для указания смещения поля данных пакета, являющегося фрагментом другого пакета. Смещение указывается от начала поля данных исходного пакета.
- **Время жизни** (8 бит) – это поле предназначено для указания максимального времени перемещения пакета по сети и предотвращения зацикливания пакетов. В первых стандартах IP-протокола предполагалось, что каждый маршрутизатор, через который проходит пакет, уменьшает значение поля "Время жизни" на количество секунд, в течение которых пакет находился в очереди обрабатываемых пакетов. Если значение поля становится равным нулю, пакет должен быть уничтожен маршрутизатором. Поскольку современные маршрутизаторы обрабатывают пакеты менее чем за секунду, маршрутизаторы уменьшают значение этого поля на единицу.
- **Протокол** (8 бит) – указатель на протокол верхнего уровня, которому должны быть переданы данные из поля данных пакета.
- **Контрольная сумма** заголовка (16 бит) – значение контрольной суммы заголовка пакета. Это поле используется для проверки целостности заголовка пакета в процессе передачи. Контрольная сумма вычисляется источником пакета, проверяется и пересчитывается каждым маршрутизатором, через который проходит пакет. Пересчет контрольной суммы необходим в связи с изменением полей заголовка пакета, например, каждый маршрутизатор изменяет значение поля "Время жизни". При вычислении контрольной суммы, значения битов поля "Контрольная сумма" принимаются равными нулю.
- **IP-адрес источника (**32 бита) – адрес узла, отправившего пакет.
- **IP-адрес получателя** (32 бита) – адрес узла, которому предназначен пакет.
- **Опции** – это поле предназначено для указания дополнительных параметров передачи пакета или для записи информации об маршруте прохождения пакета. Поле является необязательным и используется, обычно, только при отладке сети.
- **Заполнение** – поле используется для выравнивания заголовка пакета по 32–битной границе (заполняется нулями).

3. Адресация в IPv4

В стеке протоколов TCP/IP используются три типа адресов:

- Локальные (аппаратные) – адреса, используемые "локальными" технологиями для доставки пакетов в пределах подсети. Например, MAC-адреса в сетях Ethernet, FDDI, WiMAX и т.д.
- IP-адреса – адреса межсетевого уровня, используемые для идентификации сетевых интерфейсов интерсети. На основе IP-адресов организуется универсальная, не зависящая от "локальных" технологий идентификация сетевых интерфейсов интерсети.
- Символьные доменные адреса (имена) – используются для присвоения сетевым интерфейсам легко запоминаемых символьных имен.

3.1 IP-адреса

В заголовке IP- пакета для IP-адресов получателя и отправителя отводится по 32 бита (4 байта). Наиболее часто IP-адрес записывают в виде четырех однобайтовых чисел, разделенных точкой.

Пример 1

Записи IP-адреса в различных форматах:
десятичная: 219.17.25.157
двоичная: 11011011.00010001.00011001.10011101
шестнадцатеричная: DB11199D

Если узел IP-сети имеет несколько сетевых интерфейсов, каждому из них присваивается отдельный IP-адрес. Например, если узел имеет два сетевых интерфейса, с помощью которых он подключен к двум “локальным” сетям, его сетевым интерфейсам будут сопоставлены два IP-адреса.

Способы назначения адресов:

1. администратором (вручную), с помощью утилит конфигурирования операционной системы (ОС);
2. автоматически, с помощью протокола динамической конфигурации узла DHCP (Dynamic Host Configuration Protocol, RFC 2131).

IP-адреса состоят из двух частей – номера сети и номера узла. Номер сети идентифицирует в интерсети подсеть, к которой принадлежит узел, номер узла однозначно определяет узел внутри подсети. Для разделения IP-адреса на части используют две схемы:

- на основе классов адресов,
- на основе масок.

3.2 Разделение IP-адреса на номер сети и номер узла на основе классов

Традиционная схема разделения IP-адреса на номер сети и номер узла основана на понятии класса, определяемого значениями нескольких первых бит адреса.

A. Первый бит равен 0: адрес класса A, первый байт адреса используется для номера сети, остальные три – для номера узла (количество адресов в сети 2^{24}).
   Адреса: 1.0.0.0 – 127.255.255.255
B. Первые биты равны 10: адрес класса B, первые два байта используются для номер сети, остальные – для номер узла (количество адресов в сети 2^{16}).
   Адреса: 128.0.0.0 –191.255.255.255
C. Первые биты равны 110: адрес класса C, первые три байта используются для номера сети, последний байт – для номера узла (количество адресов в сети 2^{8}).
   Адреса: 192.0.0.0 – 223.255.255.255
D. Первые биты равны 1110 – адреса мультикаст (multicast), предназначены для адресации группы узлов.
   Адреса: 224.0.0.0 – 247.255.255.255

В некоторых случаях необходимо отдельно записывать номер сети и номер узла, из которых состоит IP-адрес. В записи номера сети соответствующие номеру узла разряды адреса заменяют нулями, в записи номера узла нулями заменяют разряды, соответствующие номеру сети.

Пример 2

IP-адрес 192.9.7.5 (11000000.00001001.00000111.00000101)

Поскольку первые биты равны 110, следовательно, это адрес класса С.
Номер сети – 192.9.7.0 (11000000.00001001.00000111.00000000),
Номер узла – 0.0.0.5 (00000000.00000000.00000000.00000101).

Пример 3

IP-адрес 62.76.9.17 (00111110.01001100.00001001.00010001)
Поскольку первый бит равен 0, следовательно, это адрес класса А.
Номер сети – 62.0.0.0 (00111110.00000000.00000000.00000000)
Номер узла – 0.76.9.17 (00000000.01001100.00001001.00010001)

Соответствие блоков адресов номерам сетей на основе классов

Номер сети определяет блок адресов с одинаковым префиксом (одинаковой старшей частью), зависящим от класса адреса.

Пример 4

Рассмотрим номер сети 192.168.169.0.
Первые разряды адреса имеют значение 110, следовательно, это адрес класса С. Этому номеру сети соответствует блок адресов 192.168.169.0 – 192.168.169.255, все адреса этого блока имеют одинаковые первые три октета, равные 192.168.169.

Пример 5

Рассмотрим номер сети 62.0.0.0.
Первый разряд адреса имеет значение 0, следовательно, этот адрес класса А. Этому номеру сети соответствует блок адресов 62.0.0.0 – 62.255.255.255, все адреса этого блока имеют одинаковый первый октет, равный 62.

Неэффективность адресации на основе классов

Как показывает практика, выделение сетям блоков адресов на основе классов (адресация на основе классов) не обеспечивает оптимальное использование адресного пространства IPv4. Например, для большинства организаций средней величины блок адресов класса С (256 адресов) слишком мал, а блок класса В (65534 адресов) слишком велик. Как правило, в таких организациях для адресации узлов используют менее половины адресов. В настоящее время адресация на основе классов считается устаревшей и на практике почти не используется.

Возможные пути решения проблемы:

1. Увеличить количество бит, выделяемых для номера сети в классах А, В. Например, можно в классе В выделить под номер сети 19–20 бит;
2. Использовать схему адресации, в которой для номера сети можно использовать произвольное количество бит адреса.

3.3 Разделение IP-адреса на номер сети и номер узла на основе масок

Маска – это используемое совместно с IP-адресом четырехбайтовое число, двоичная запись которого содержит единицы в разрядах, соответствующих в адресе номеру сети, и нули в разрядах, соответствующих номеру узла. Единицы в маске начинаются в первом разряде адреса и не могут чередоваться с нулями.

С помощью маски можно выделять произвольное количество разрядов для номера сети, что позволяет отказаться от понятий классов адресов и сделать более гибкой систему адресации.

Примеры 6. Запись маски и IP-адреса
Десятичная форма:
192.168.74.64/255.255.255.192
Двоичная форма:
11000011. 10101000. 01001010 .01000000/11111111.11111111.11111111.11000000

Для указания количества разрядов, выделенных для номера сети, также используется указание префикса адреса. Запись адреса с префиксом имеет вид: *IP-адрес/Префикс,* где *Префикс* – число разрядов, выделенных для номера сети.
Например, запись 192.168.75.64/26 означает, что в адресе 192.168.75.64 под номер сети отведено 26 двоичных разрядов, соответствующая маска 255.255.255.192.

Значения масок стандартных классов адресов:

```
класс A – 11111111.00000000.00000000.00000000 (255.0.0.0);
класс B – 11111111.11111111.00000000.00000000 (255.255.0.0);
класс C – 11111111.11111111.11111111.00000000 (255.255.255.0).
```

Вычисление номера сети и номера узла по заданному IP-адресу и маске

Для вычисления номера сети по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и маске. Такая операция называется наложением маски на адрес.

На рисунке 3 представлено табличное побитовой операции “И”.

1-ый операнд	**2-ой операнд**	**Значение “И”**
0	0	0
1	0	0
0	1	0
1	1	1

Рис. 3. Определение побитовой операции “И”

Для вычисления номера узла по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и результату применения побитовой операции “НЕ” к маске.

На рисунке 4 представлено табличное определение унарной операции побитового отрицания “НЕ” (побитового дополнения).

Операнд	**Значение “НЕ”**
0	1
1	0

Рис. 4. Определение побитовой операции “НЕ”

Пример 7

Применим побитовую операцию “И” к однобайтовым числам 185 и 221.
Представим числа в двоичной форме: 185 = 10111001, 221 = 11011101.

$$\begin{array}{ll} & 10111001 \\ \text{и} & \underline{11011101} \\ & 10011001 \end{array}$$

Применим побитовую операцию “НЕ” к числу 185.

$$\text{НЕ}\ \frac{10111001}{01000110}$$

Пример 8

Вычислим номер сети и номер узла для адреса 215.17.125.177 и маски 255.255.255.240.

```
IP-адрес: 215.17.125.177  (11010111.00010001.01111101.10110001)
Маска:    255.255.255.240 (11111111.11111111.11111111.11110000)
```

В этом случае номер сети (Н.с.) и номер узла (Н.у.) будут следующими:

```
Н.с.:     215.17.125.176  (11010111.00010001.01111101.10110000)
Н.у.:     0.0.0.1         (00000000.00000000.00000000.00000001)
```

Пример 9

Вычислим номер сети и номер узла для адреса 67.38.173.245 и маски 255.255.240.0.

```
IP-адрес: 67.38.173.245 (01000011.00100110.10101101.11110101)
Маска:    255.255.240.0 (11111111.11111111.11110000.00000000)
Н.с.:     67.38.160.0   (01000011.00100110.10100000.00000000)
Н.у.:     0.0.13.245    (00000000.00000000.00001101.11110101)
```

Соответствие блоков адресов номерам сетей на основе масок

При использовании маски, так же, как и в случае адресации на основе классов, номер сети определяет блок адресов с одинаковым префиксом.

Пример 10

В маске 255.255.255.192 (11111111.11111111.11111111.11000000) выделено 26 разрядов под номер сети и 6 разрядов под номер узла.

Номеру сети 192.168.74.64 с данной маской соответствует блок адресов:

```
Маска:    11111111.11111111.11111111.11000000  (255.255.255.192)
Н.с:      11000011.10101000.01001010.01000000  (192.168.74.64)
Адрес 1:  11000011.10101000.01001010.01000000  (192.168.74.64)
Адрес 2:  11000011.10101000.01001010.01000001  (192.168.74.65)
Адрес 3:  11000011.10101000.01001010.01000010  (192.168.74.66)
.....
Адрес 63: 11000011.10101000.01001010.01111110 (192.168.74.126)
Адрес 64: 11000011.10101000.01001010.01111111 (192.168.74.127)
```

Всего в этом блоке $2^6 = 64$ адресов (192.168.74.64 – 192.168.74.127). Все адреса имеют одинаковый префикс (первые 26 разрядов):

```
11000011.10101000.01001010.01
```

Пример 11

В маске 255.255.254.0 (1111111.11111111.11111110.00000000) выделено 23 разряда под номер сети и 9 разрядов под номер узла.

Номеру сети 192.168.74.0 с данной маской соответствует блок адресов:

```
Маска:     11111111.11111111.11111110.00000000 (255.255.254.0)
Н.с:       11000011.10101000.01001010.00000000 (192.168.74.0)
Адрес 1:   11000011.10101000.01001010.00000000 (192.168.74.0)
Адрес 2:   11000011.10101000.01001010.00000001 (192.168.74.1)
```

```
Адрес 3:   11000011.10101000.01001010.00000010 (192.168.74.2)
……….
Адрес 511: 11000011.10101000.01001011.11111110 (192.168.75.254)
Адрес 512: 11000011.10101000.01001011.11111111 (192.168.75.255)
```

Всего в этом блоке $2^9 = 512$ адресов (192.168.74.0 – 192.168.75.255). Все адреса имеют одинаковый префикс (первые 23 разряда):
`11000011.10101000.0100101`

Замечание: размер блока адресов, соответствующий некоторой маске, всегда равен степени двойки.

Деление блоков адресов на части с помощью маски

При проектировании сетей возникает задача выделения подсетям блоков адресов из некоторого заданного непрерывного блока адресов с одинаковым префиксом. Задача решается выделением дополнительных разрядов для номеров сети, т.е. исходному блоку сопоставляется маска, которая позволяет выделить блоки адресов нужного размера. Отметим, что каждый выделяемый блок представляет непрерывную последовательность адресов, имеющих одинаковый префикс (номер сети).

Пример 12

Пусть задан блок адресов, определяемый номером сети 213.59.30.0/255.255.255.0 (213.59.30.0/24), этому номеру соответствуют адреса: 213.59.30.0 – 213.59.30.255.

Все адреса этого блока имеют одинаковый префикс (см. рис. 5)

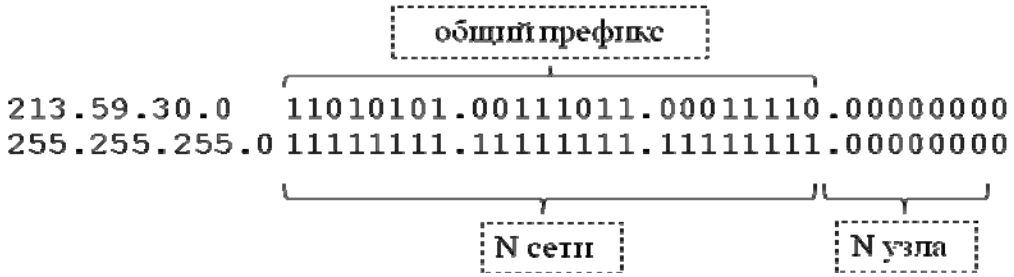

Рис. 5. Префикс блока адресов

Заметим, что в исходном блоке адресов имеется восемь разрядов (выделенных под номер узла), часть которых можно выделить под номера сетей. Например, выделив два дополнительных разряда для номера сети и оставив шесть разрядов для номера узла (см. рис. 6), можно получить четыре блока адресов по шестьдесят четыре адреса в каждом.

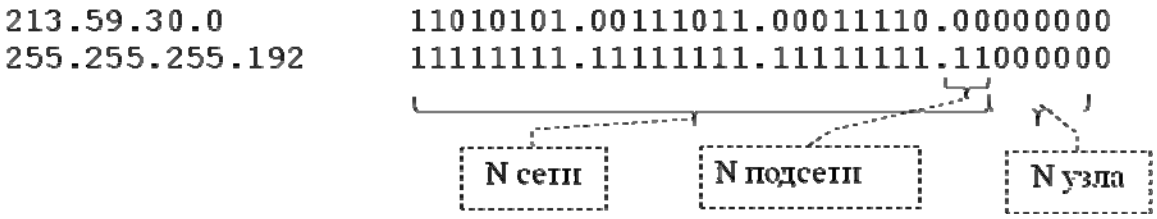

Рис. 6. Выделение дополнительных разрядов для номера сети

То есть два дополнительных разряда в маске дают четыре битовые комбинации, с помощью которых можно получить 4 номера сети, и шесть разрядов для номера узла дают 64 битовые комбинации, с помощью которых можно в каждом блоке получить 64 адреса.
Дополнительные разряды, выделяемые для номера сети, часто называют разрядами, используемыми для идентификации подсетей.

Адресное пространство исходного блока можно представить в виде таблицы (см. рис. 7).

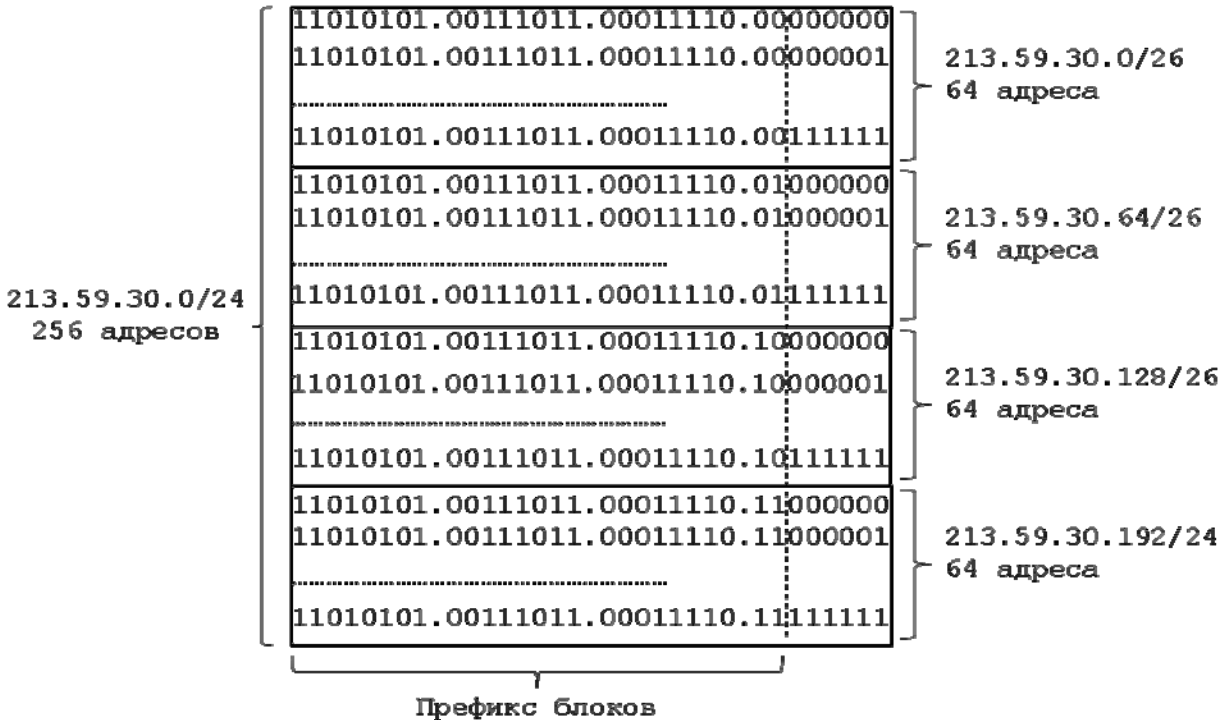

Рис. 7. Распределение адресов на основе маски 255.255.255.192

Отметим, что адреса каждого блока имеют одинаковые значения разрядов, выделенных для идентификации подсети. Для первого блока эти разряды имеют значения 00, для второго 01, для третьего 10, для четвертого 11. Соответственно, мы получили четыре номера сети с префиксом 26 (см. рис. 8).

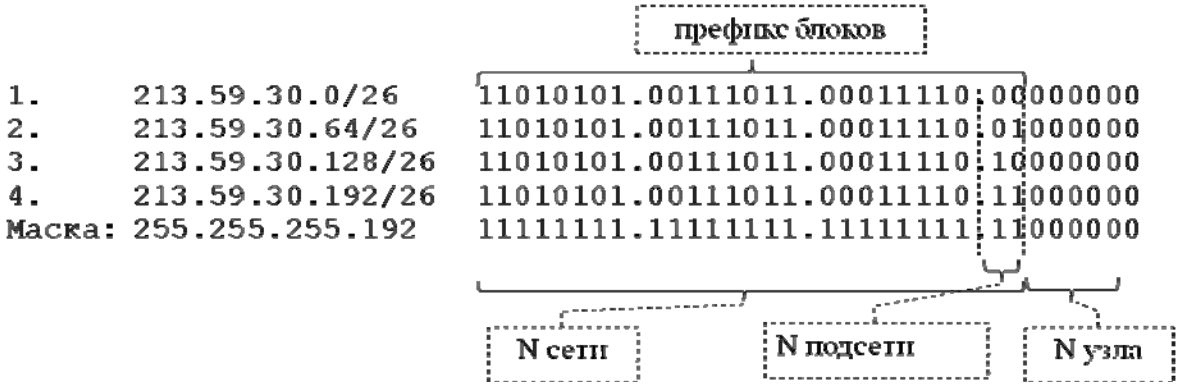

Рис. 8. Номера сетей

Использование масок (префиксов) различной длины

Используя маски различной длины, можно разбить блок адресов на части с различным количеством адресов.

Пример 13

Пусть задан блок адресов, определяемый номером сети 213.59.30.0/255.255.255.0 (класс С) , этому номеру соответствуют адреса: 213.59.30.0 – 213.59.30.255 (см. рис. 9).

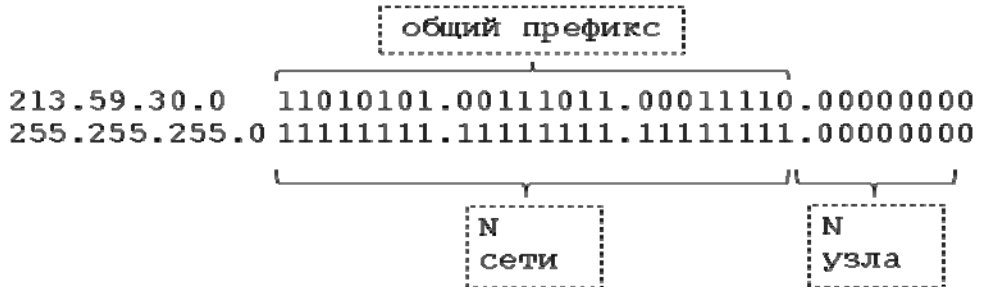

Рис. 9. Деление разрядов адреса на номер сети и узла

Заметим, что в исходном блоке адресов имеется восемь разрядов (выделенных под номер узла), часть которых можно выделить под номера подсетей. Например, выделив два дополнительных разряда для номера подсети и шесть разрядов для номера узла, используя маску 255.255.255.192, можно выделить блоки адресов по 64 адреса в каждом. Выделив один дополнительный разряд для номера подсети и семь разрядов для номера узла, используя маску 255.255.255.128, можно выделить блок из 128 адресов. Выделяя в заданном блоке адресов части, имеющие одинаковый префикс, соответствующий указанным маскам, можно получить два блока из 64 адресов и один блок из 128 адресов (см. рис. 10).

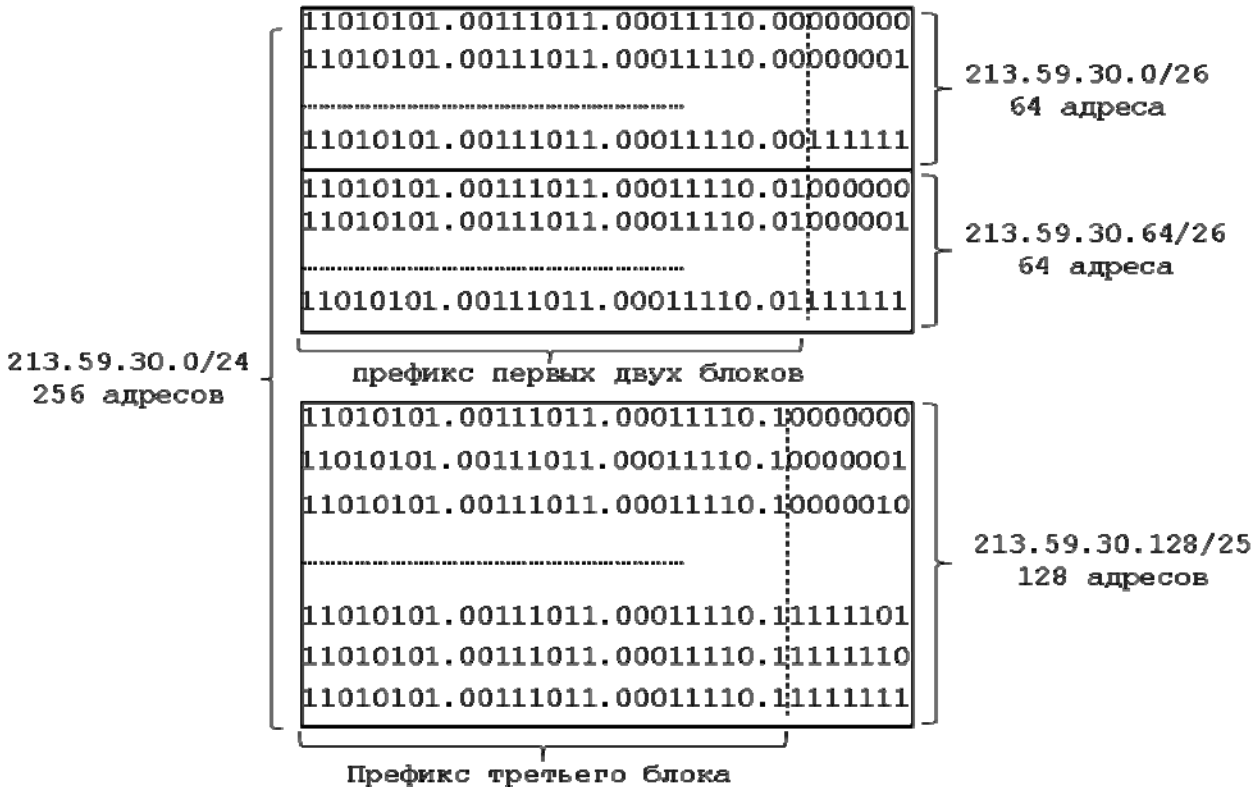

Рис. 10. Распределение адресов

Отметим, что адреса каждого блока имеют одинаковые значения разрядов, выделенных для идентификации подсети (см. рис. 11). Для первого блока эти разряды имеют значения 00, для второго 01, для третьего 1. Соответственно, мы получили два номера сети с префиксом 26 (маска 255.255.255.192) и один номер сети с префиксом 27 (маска 255.255.255.128).

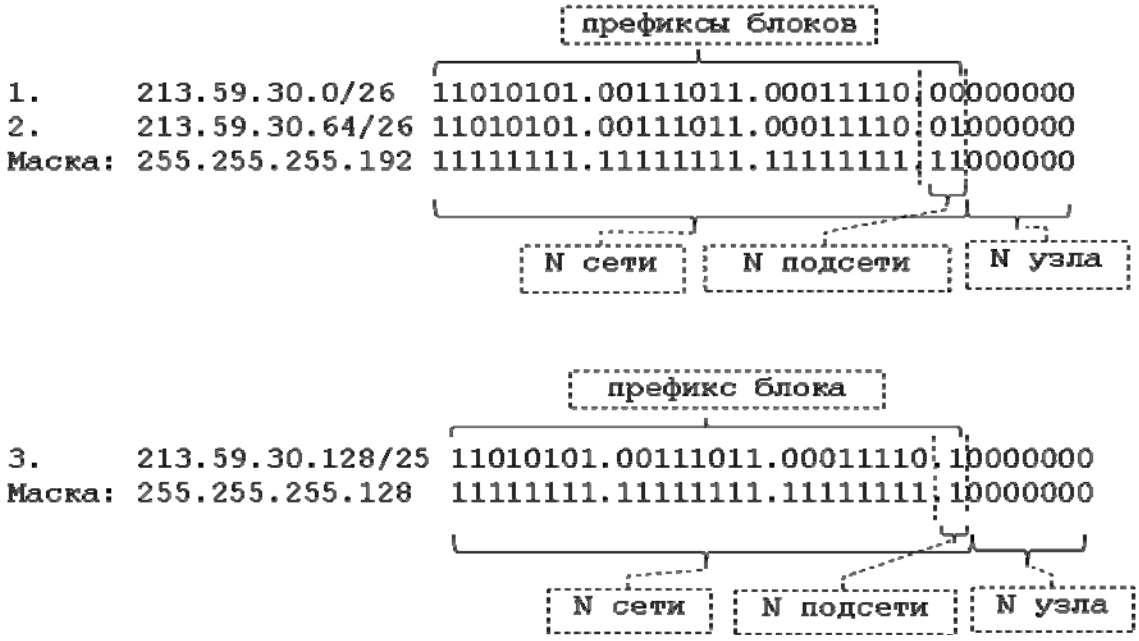

Рис. 11. Номера сетей

Правила выделения адресных блоков

1. Если исходный блок адресов имеет префикс n, то выделяемые блоки адресов могут иметь префикс m: $n < m \leq 32$. В случае деления исходного блока на блоки одинакового размера, число получаемых в результате блоков равно 2^{m-n}, число адресов в каждом блоке равно 2^{32-m}.
2. Если выделяется блок из 2^k адресов, то в маске для номера узла необходимо выделить k разрядов (количество нулей в маске).
3. Адреса выделяются непрерывными блоками, все адреса блока имеют одинаковый префикс.
4. Количество адресов в выделяемых блоках всегда равно некоторой степени двойки.
5. Если необходимо получить блок для адресации N узлов, то количество адресов в выделяемом блоке должно быть 2^k, где
   $2^k \geq N+2$ и $2^{k-1} < N+2$,
   поскольку при выделении блоков адресов необходимо учитывать, что два адреса в блоке будут иметь специальное назначение и не могут использоваться для нумерации узлов. Адреса, имеющие специальное назначение, – это номер сети и адрес, используемый для ограниченного широковещания (первый и последний адреса блока).
6. В таблице 1 представлены возможные значения масок, префиксов и соответствующее им количество адресов в выделяемых блоках.

Таблица 1. Соответствие масок префиксов и количества адресов

Количество разрядов в номере узла	Префикс	Маска	Количество адресов
0	/32	255.255.255.255	2^0
1	/31	255.255.255.254	2^1
2	/30	255.255.255.252	2^2
3	/29	255.255.255.248	2^3
4	/28	255.255.255.240	2^4

5	/27	255.255.255.224	2^5
6	/26	255.255.255.192	2^6
7	/25	255.255.255.128	2^7
8	/24	255.255.255.0	2^8
9	/23	255.255.254.0	2^9
10	/22	255.255.252.0	2^{10}
11	/21	255.255.248.0	2^{11}
12	/20	255.255.240.0	2^{12}
13	/19	255.255.224.0	2^{13}
14	/18	255.255.192.0	2^{14}
15	/17	255.255.128.0	2^{15}
16	/16	255.255.0.0	2^{16}
17	/15	255.254.0.0	2^{17}
18	/14	255.252.0.0	2^{18}
19	/13	255.248.0.0	2^{19}
20	/12	255.240.0.0	2^{10}
21	/11	255.224.0.0	2^{21}
22	/10	255.192.0.0	2^{22}
23	/9	255.128.0.0	2^{23}
24	/8	255.0.0.0	2^{24}
25	/7	254.0.0.0	2^{25}
26	/6	252.0.0.0	2^{26}
27	/5	248.0.0.0	2^{27}
28	/4	240.0.0.0	2^{28}
29	/3	224.0.0.0	2^{29}
30	/2	192.0.0.0	2^{30}
31	/1	128.0.0.0	2^{31}
32	/0	0.0.0.0	2^{32}

3.4 Распределение IP-адресов

Распределение адресов в сети Интернет организовано на основе централизованной иерархической системы. Главным органом этой системы является неправительственная некоммерческая организация **ICANN** (Internet Corporation for Assigned Numbers).

ICANN координирует региональные отделения – **ARIN** (Америка), **RIPE** (Европа), **APNIC** (Азия и Тихоокеанский регион). Региональные отделения выдают блоки адресов крупным провайдерам услуг Интернет. Провайдеры в свою очередь выдают блоки адресов своим клиентам. Для получения российским провайдером блока адресов, провайдер должен стать членом RIPE NCC и получить статус Локального Интернет–Реестра (LIR).

В соответствии с RFC 1518, 1519 блоки адресов выделяются на основе одинакового префикса, выделение блоков на основе классов адресов считается устаревшим и в настоящее время не используется.

3.5 IP-адреса для изолированных сетей

Если для передачи данных в локальной сети используется IP-протокол, но сеть не подключена к Интернет или необходимо ограничить доступ из локальной сети в сеть Интернет, для адресации узлов, в соответствии с RFC 1918, рекомендуется использовать следующие адреса:

10.0.0.0 (блок адресов класса A),
172.16.0.0–172.31.0.0 (блок адресов класса B),
192.168.0.0–192.168.255.0 (блок адресов класса C).

Адреса из этих блоков называют частными (private) адресами. IP-пакеты с частными адресами уничтожаются магистральными маршрутизаторами Интернет. Для доступа в Интернет из сетей с такими адресами используют технологии NAT и Proxy.

3.6 Специальные IP-адреса

- Адреса с первыми разрядами равными 11110 зарезервированы для будущих применений.
- Пакет с адресом 255.255.255.255 должен рассылаться всем узлам, находящимся в той же подсети, что и источник пакета. Такой способ рассылки называется ограниченным широковещанием (limited broadcast).
- Если разряды адреса, соответствующие номеру узла, содержат только единицы, то пакет рассылается всем узлам сети с заданным номером. Такой способ рассылки называется широковещательным (broadcast).

Пример 14

192.168.7.255 – широковещательный адрес для сети 192.168.7.0/255.255.255.0
213.1.18.127 – широковещательный адрес для сети 213.1.18.64/255.255.255.192

- Если в адресе получателя в поле номера сети содержатся только нули, то узел–получатель принадлежит той же подсети, что и узел, который отправил пакет.
- Блок адресов 127.0.0.0/8 используется для тестирования и взаимодействия сетевых процессов в пределах отдельного компьютера. Например, при передаче пакетов на адрес 127.0.0.1, пакеты не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые. Иначе говоря, передача пакетов на адрес 127.0.0.1 означает связь с самим собой. Адрес 127.0.0.1 соответствует виртуальному петлевому (loopback) сетевому интерфейсу, который реализуется программно и не связан с физическими интерфейсами (RFC 3330). Например, этот интерфейс может быть использован клиентскими сетевыми процессами для взаимодействия с серверным процессом, выполняющимся на том же компьютере.

4. Протокол ARP

ARP (Address Resolution Protocol) – протокол определения адреса, предназначенный для получения “локального адреса” по известному IP-адресу (RFC 826).

В соответствии с принципами модели стека TCP/IP, при передаче IP-пакетов меду узлами “локальной сети” производится инкапсуляция пакетов в кадры технологии, на основе которой построена “локальная сеть”.

Пример 15

Рассмотрим сеть Ethernet, построенную на основе коммутатора, к которому подключены четыре компьютера (см. рис. 12).

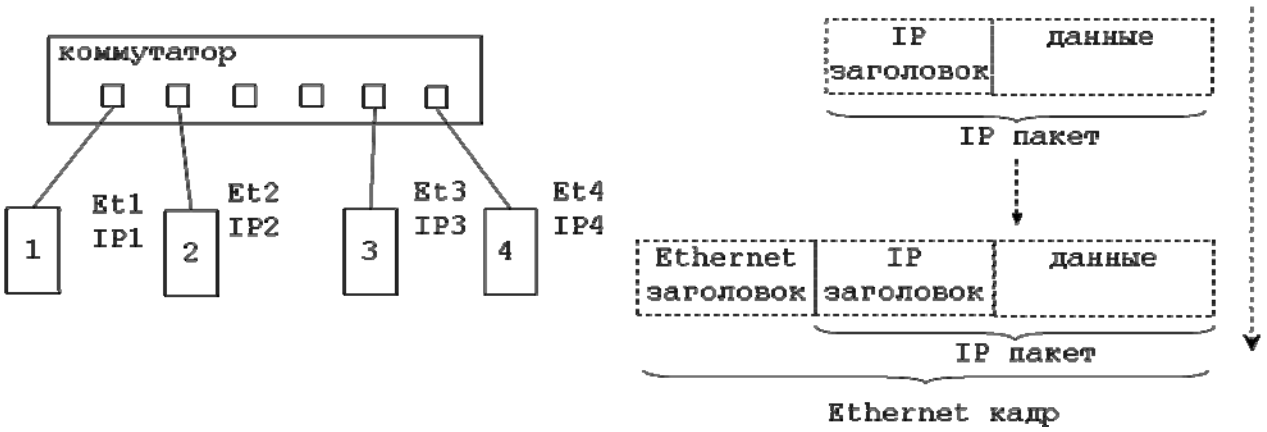

Рис. 12. Инкапсуляция IP-пакетов в Ethernet-кадры

Предположим, что узлу №1 с IP-адресом *IP1* необходимо передать IP-пакет узлу №2 с адресом *IP2*. Модулю операционной системы, реализующему функции IP-протокола в узле №1, известен IP-адрес узла 2, указанный в заголовке IP-пакета. Для передачи пакета узел №1 должен определить по известному IP-адресу *IP2* соответствующий узлу №2 Ethernet-адрес *Et2*, инкапсулировать IP-пакет в Ethernet-кадр и передать этот кадр на основе технологии Ethernet.

Алгоритм работы протокола ARP зависит от технологии "локальной" сети. Например, в "локальных сетях", поддерживающих широковещательные рассылки, ARP протокол основан на использовании широковещательных рассылок.

Рассмотрим принципы работы ARP–протокола на примере технологии Ethernet.

Схема определения MAC-адресов в Ethernet-сетях:

1. При передаче IP-пакета на уровень сетевых интерфейсов модуль межсетевого взаимодействия обращается к модулю ARP для определения Ethernet-адреса.
2. Модуль ARP формирует запрос на определение адреса и передает его драйверу Ethernet.
3. Драйвер Ethernet посылает в сеть широковещательный кадр, содержащий запрос (все узлы сети получают этот кадр).
4. Узел сети, имеющий указанный в запросе IP-адрес, посылает ARP–ответ, в котором указывает свой Ethernet-адрес.
5. Модуль ARP источника запроса, получив ответ, передает полученный Ethernet-адрес модулю межсетевого взаимодействия.

Информация о соответствии IP- адресов Ethernet-адресам временно сохраняется (кэшируется) модулем ARP в ARP таблице. ARP таблица состоит из трех полей: "IP-адрес", "Ethernet адрес" и "Тип записи".

Виды записей в таблице ARP:

- **динамические** – заносятся в таблицу автоматически, имеют ограниченный срок жизни и по истечении нескольких минут удаляются из таблицы;
- **статические** – заносятся в таблицу администратором с помощью специальной утилиты операционной системы (в большинстве ОС для этого используется утилита arp), время жизни таких записей не ограничено.

С помощью статических записей можно повысить безопасность сети и сократить число широковещательных рассылок.

5. Маршрутизация

5.1 Принципы маршрутизации

Сети, объединяемые в интерсеть на основе IP-протокола, соединяются между собой сетевыми устройствами, называемыми маршрутизаторами.

Маршрутизатор – это сетевое устройство, которое собирает информацию о топологии межсетевых связей и на ее основе пересылает IP-пакеты в сеть назначения. Маршрутизаторы обычно имеют более одного сетевого интерфейса, каждый из которых обеспечивает передачу данных на основе технологии "локальной сети", к которой он подключен.

Маршрут – последовательность маршрутизаторов, через которые должен пройти пакет.

На рисунке 13 представлены шесть локальных сетей (обозначены овалами), объединяемых между собой четырьмя маршрутизаторами (обозначены квадратами).

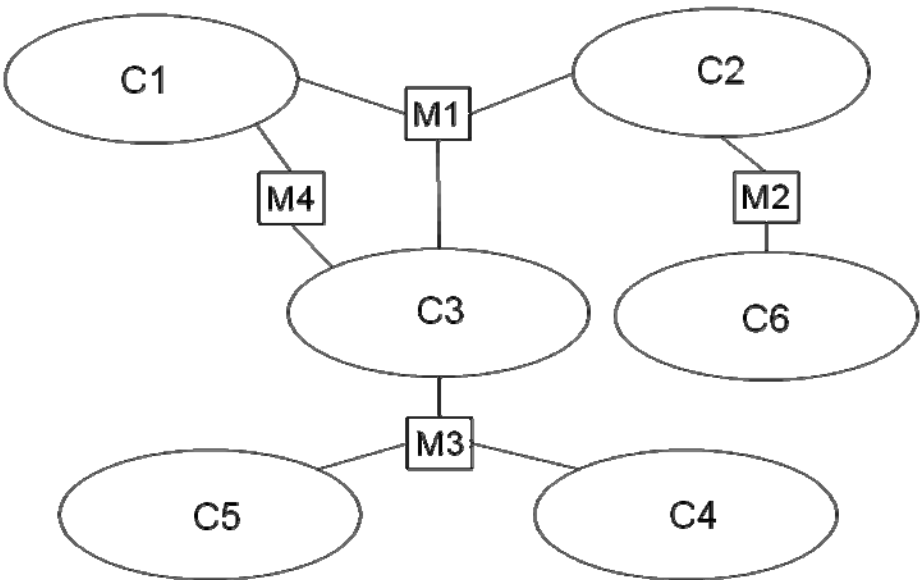

Рис. 13. Объединение сетей с помощью маршрутизаторов

Каждой подсети сопоставляется блок адресов, определяемый номером сети и маской, т.е. все адреса одной подсети имеют одинаковый номер сети (одинаковую старшую часть). Блоки адресов различных подсетей отичаются номерами сетей (имеют различную старшую часть).

Конечные узлы и маршрутизаторы сети хранят информацию о текущей конфигурации маршрутов в электронных таблицах, называемых таблицами маршрутизации. Каждая строка таблицы определяет маршрутизатор для продвижения пакетов в некоторую сеть. Количество полей в таблице маршрутизации может различаться в зависимости от ОС. В большинстве ОС таблицы маршрутизации содержат следующие поля: "Адрес назначения", "Маска", "Шлюз", "Интерфейс".

Назначение полей:

1. **Адрес назначения** – адрес сети или узла, для которого описывается маршрут.
2. **Маска** – маска соответствующая адресу, указанному в поле **Адрес назначения**.
3. **Шлюз** – IP-адрес интерфейса маршрутизатора, которому должен быть передан пакет. Или данное поле содержит адрес локального интерфейса, на который должен быть передан пакет для пересылки в непосредственно подключенную "локальную сеть".
4. **Интерфейс** – идентификатор интерфейса, через который должен быть передан пакет.

Таблицы маршрутизации создаются администратором сети “вручную”, с помощью специальной утилиты ОС или автоматически – в результате обмена маршрутизаторами информацией о топологии сети.

В процессе построения таблиц маршрутизации и, следовательно, при выборе маршрута могут учитываться следующие факторы:

- величина задержки доставки пакета до сети назначения,
- пропускная способность каналов передачи данных,
- загруженность линий связи,
- количество маршрутизаторов на пути продвижения пакета (число хопов).

На практике наиболее часто при выборе маршрутов учитывают количество маршрутизаторов на пути продвижения пакета.

Пример записей в таблице маршрутизации:

Адрес н-я	Маска	Шлюз	Интерфейс
77.243.120.0	255.255.255.0	192.168.0.2	192.168.0.1
77.243.121.64	255.255.255.192	192.168.1.3	192.168.1.4

В первой строке таблицы прописано, что IP-пакеты, адресованные в сеть с номером 77.243.120.0 и маской 255.255.255.0 должны быть переданы маршрутизатору с IP-адресом 192.168.0.1 через интерфейс с IP-адресом 192.168.0.1.

Во второй строке прописано, что IP-пакеты, адресованные в сеть с номером 77.243.121.64 и маской 255.255.255.192 должны быть переданы маршрутизатору с IP-адресом 192.168.1.3 через интерфейс с IP-адресом 192.168.1.4.

Замечания:

- В приведенном примере, для идентификации интерфейсов используются их IP-адреса. С другой стороны, вместо IP-адресов могут использоваться символьные имена, построенные в соответствии с правилами ОС (например, eth0, em0, lo).
- В некоторых ОС поля “Адрес назначения” и “Маска” объединяют в одно поле “Адрес назначения”, в котором указывают номер сети с префиксом.
- В случае адресации на основе классов, в таблице маршрутизации поле “Маска” отсутствует, поскольку по первым разрядам IP-адреса можно определить класс адреса и, следовательно, получить номер сети.

Таблицу маршрутизации в ОС Windows и *nix можно получить с помощью команд *route* и *netstat*. Для модификации таблиц используется команда *route.*

Основные функции маршрутизаторов

- На уровне сетевых интерфейсов: согласование электрических сигналов, линейное и логическое кодирование, получение доступа к среде передачи данных, формирование, отправка и получение кадров, подсчет контрольных сумм кадров, передача поля данных кадра вышестоящему уровню.
- На межсетевом уровне: проверка контрольных сумм IP-пакета, проверка времени жизни пакета, корректировка содержимого некоторых полей пакета (TTL, пересчет контрольной суммы), фильтрация трафика, фрагментация пакетов, анализ таблицы маршрутизации, разрешение локальных адресов, обмен информацией о топологии сети, формирование таблиц маршрутизации.

В общем случае при получении кадра маршрутизатор выполняет следующие действия:

1. Извлекает из кадра пакет сетевого уровня.
2. Извлекает из заголовка пакета IP- адрес получателя.

3. Выполняет поиск в таблице маршрутизации адреса шлюза, которому должен быть передан пакет.
4. При необходимости фрагментирует пакет.
5. Модифицирует некоторые поля заголовка пакета (например, TTL).
6. С помощью протокола разрешения локальных адресов определяет адрес узла (маршрутизатора), которому должен быть передан пакет.
7. Формирует кадр канального уровня (инкапсулируя в кадр сетевой пакет) в соответствии с базовой технологией сети, в которую (через которую) должен быть передан пакет. Отправляет кадр через интерфейс, указанный в таблице маршрутизации.

Замечание: в описанном выше алгоритме не рассматривается случай, когда получателем пакета является сам маршрутизатор.

Обобщенный алгоритм поиска маршрута в таблице маршрутизации:

1. Последовательно с каждой строкой таблицы производятся следующие действия (строка для маршрутизатора по умолчанию обрабатывается последней):
   - выполняется операция наложения маски значения поля “Маска” на IP-адрес получателя;
   - полученное значение сравнивается со значением поля “Адрес назначения”, если значения совпадают, то система запоминает строку таблицы.
2. Если на предыдущем шаге была найдена одна строка, то из поля “Шлюз” этой строки извлекается адрес шлюза, который будет использован для продвижения пакета. Если найдено несколько строк, то для выбора маршрутизатора используют строку с наибольшим количеством единиц в маске. Если строк не обнаружено, пакет уничтожается и отправителю посылается сообщение об ошибке с помощью протокола ICMP.

Замечание: если ОС упорядочивает таблицу по полю “Маска”, просмотр таблицы прекращается после первого совпадения.

Таблицы маршрутизации компьютеров и маршрутизаторов, находящихся на периферии сети, могут содержать записи для маршрутизатора по умолчанию. Маршрутизатор по умолчанию (default router) – это маршрутизатор, которому будет передан пакет в том случае, когда другие строки таблицы маршрутизации не описывают путь к узлу-получателю (см. таблицу 2).

Таблица 2. Пример таблицы маршрутизации с записью для маршрутизатора по умолчанию

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	192.168.3.3	192.168.3.1
77.243.120.0	255.255.255.0	192.168.0.2	192.168.0.1
77.243.121.64	255.255.255.192	192.168.1.3	192.168.1.4

Представленная таблица характерна для семейства ОС Windows, где строка таблицы для маршрутизатора по умолчанию содержит 0.0.0.0 в полях “Адрес назначения” и “Маска”. Это объясняется тем, что при наложении на любой IP-адрес маски 0.0.0.0 получим 0.0.0.0, т.е. указанная строка может быть использована для продвижения пакетов в любую IP-сеть.

Пример 16

Рассмотрим выбор пути передачи IP-пакета с адресом получателя 77.243.121.97 в таблице №2.

Просмотр строк таблицы начинается со второй строки (строка для маршрутизатора по умолчанию обрабатывается последней). Извлечем значение поля “Маска” и применим операцию наложения маски к полученному значению и IP-адресу получателя:

```
IP-адрес:  77.243.121.97  01001101.11110011.1111001.01100001
Маска:     255.255.255.0  11111111.11111111.1111111.00000000
Результат: 77.243.121.0   01001101.11110011.1111001.00000000
```

Значение поля “Адрес назначения” – 77.243.120.0 и результат наложения маски – 77.243.121.0 не равны, следовательно, эта строка не может использоваться для передачи пакета.

Переходим к третьей строке таблицы. Извлечем значение поля “Маска” и применим операцию наложения маски к полученному значению и IP-адресу получателя:

```
IP-адрес:  77.243.121.97   01001101.11110011.1111001.01100001
Маска:     255.255.255.192 11111111.11111111.1111111.11000000
Результат: 77.243.121.64   01001101.11110011.1111001.01000000
```

Значение поля “Адрес назначения” – 77.243.121.64 и результат наложения маски – 77.243.121.64 равны. Поскольку других строк, за исключением строки для маршрутизатора по умолчанию, в таблице нет, то эта строка будет использована для определения маршрута. Пакет будет передан маршрутизатору с IP-адресом 192.168.1.3 (значение поля “Шлюз”) через интерфейс с IP-адресом 192.168.1.4 (значение поля “Интерфейс”).

Пример 17

Рассмотрим выбор пути продвижения IP-пакета с адресом получателя 77.243.121.129 в таблице №2.

Просмотр строк таблицы начинается со второй строки (строка для маршрутизатора по умолчанию обрабатывается последней). Извлечем значение поля “Маска” и применим операцию наложения маски к полученному значению и IP-адресу получателя:

```
IP-адрес:  77.243.121.129 01001101.11110011.1111001.10000001
Маска:     255.255.255.0  11111111.11111111.1111111.00000000
Результат: 77.243.121.0   01001101.11110011.1111001.00000000
```

Значение поля “Адрес назначения” – 77.243.120.0 и результат наложения маски – 77.243.121.0 не равны, следовательно, эта строка не может использоваться для выбора пути продвижения пакета.

Переходим к третьей строке таблицы. Извлечем значение поля “Маска” и применим операцию наложения маски к полученному значению и IP-адресу получателя:

```
IP-адрес:  77.243.121.129  01001101.11110011.1111001.10000001
Маска:     255.255.255.192 11111111.11111111.1111111.11000000
Результат: 77.243.121.128  01001101.11110011.1111001.10000000
```

Значение поля “Адрес назначения” – 77.243.121.64 и результат наложения маски – 77.243.121.128 не равны, следовательно, эта строка не может использоваться для выбора пути продвижения пакета.

Поскольку других строк, за исключением строки для маршрутизатора по умолчанию, в таблице нет, то для определения маршрута будет использована строка для маршрутизатора по умолчанию. Пакет будет передан маршрутизатору с IP-адресом 192.168.3.3 (значение поля “Шлюз”) через интерфейс с IP-адресом 192.168.3.1 (значение поля “Интерфейс”).

Отметим, что при передаче IP-пакета узлом “локальной сети” возможны два варианта (см. рис. 14).

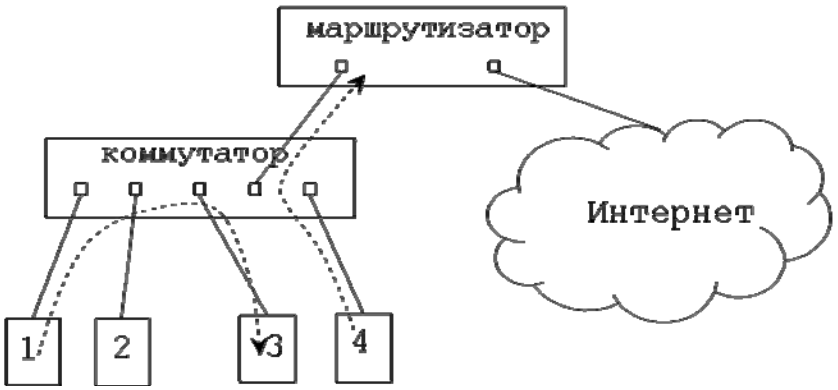

Рис. 14. Варианты передачи пакета

1. Пакет предназначен узлу, который находится в той же “локальной сети”, что и узел отправитель (номер сети узла отправителя равен номеру сети узла получателя). На рисунке этот вариант соответствует передаче пакета от узла 1 узлу 3.
В данном случае с помощью протокола ARP определяется локальный адрес узла–получателя, IP-пакет упаковывается в кадр локальной технологии и передается в соответствии с алгоритмом этой технологии.
2. Пакет предназначен узлу, который находится в другой сети и должен быть передан маршрутизатору. На рисунке этот вариант соответствует передаче пакета от узла 4 через маршрутизатор во внешнюю сеть.
В данном случае с помощью таблицы маршрутизации определяется адрес шлюза, которому должен быть передан пакет, с помощью протокола ARP определяется MAC–адрес шлюза, IP-пакет упаковывается в кадр “локальной” технологии и передается в соответствии с алгоритмом этой технологии.

Виды алгоритмов маршрутизации

По способу составления таблиц маршрутизации различают следующие алгоритмы:

- алгоритмы статической (фиксированной) маршрутизации;
- алгоритмы адаптивной (динамической) маршрутизации.

В алгоритмах статической маршрутизации таблица составляется администратором “вручную” с помощью специальных утилит и настраивается маршрутизатором во время его загрузки. При изменении топологии сети таблица не изменяется операционной системой автоматически, требуются дополнительные действия администратора для модификации таблицы.

Разновидностью фиксированной маршрутизации является метод заливки – пакеты передаются на все интерфейсы маршрутизатора кроме того, с которого он получен.

Алгоритмы адаптивной маршрутизации обеспечивают автоматическое построение и оперативное обновление таблиц маршрутизации.
Адаптивные алгоритмы маршрутизации подразделяют на два вида:

1. Алгоритмы, основанные на использовании векторов расстояний.
Примеры протокола: RIP (Routing Information Protocol) RFC 1058, 2453.

2. Алгоритмы, учитывающие состояния линий.
Примеры протоколов: OSPF (Open Shortest Path First) RFC 2328, IS–IS (Intermediate System to Intermediate System) RFC 1142.

Минимальная таблица маршрутизации

Операционные системы автоматически создают минимальную таблицу маршрутизации, которая содержит строки, вычисляемые ОС автоматически на основе конфигурации сетевых интерфейсов (IP-адресов, масок) и адреса маршрутизатора по умолчанию. В большинстве ОС минимальная таблица маршрутизации содержит запись для маршрутизатора по умолчанию, записи для непосредственно подключенных к узлу сетей и записи для организации широковещательных рассылок.

Рассмотрим сеть IP-сеть, построенную на основе сети Ethernet (см. рис. 15).

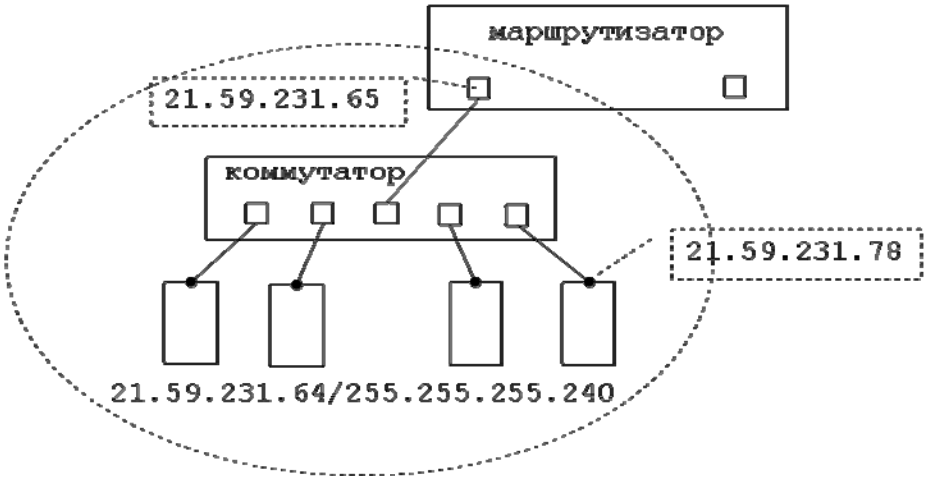

Рис. 15. Пример IP-сети

В данной сети для нумерации узлов выделен блок IP-адресов, определяемый номером сети 21.59.231.64 с маской 255.255.255.240. Предположим, что узлу №4 выделен IP-адрес 21.59.231.78/255.255.255.240, тогда минимальная таблица маршрутизации этого узла в ОС Windows имеет следующий вид:

Таблица 3. Минимальная таблица маршрутизации

	Адрес н-я	Маска	Шлюз	Интерфейс
1	0.0.0.0	0.0.0.0	21.59.231.65	21.59.231.78
2	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
3	21.59.231.78	255.255.255.255	127.0.0.1	127.0.0.1
4	21.59.231.64	255.255.255.240	21.59.231.78	21.59.231.78
5	21.255.255.255	255.255.255.255	21.59.231.78	21.59.231.78
6	224.0.0.0	240.0.0.0	21.59.231.78	21.59.231.78
7	255.255.255.255	255.255.255.255	21.59.231.78	21.59.231.78

Замечание: номера строк, помещенные в окружности, не являются частью таблицы.

Назначение строк:

1. Путь к маршрутизатору по умолчанию. В данной сети узел №4 имеет единственный путь продвижения пакетов во внешние сети через маршрутизатор, Ethernet-интерфейс которого имеет адрес 21.59.231.65.
2. Путь продвижения пакетов на loopback–адреса 127.0.0.0/255.0.0.0. Пакеты, передаваемые в эту сеть, направляются на петлевой интерфейс с адресом 127.0.0.1 и обрабатываются локально.

3. Путь продвижения пакетов с адресом назначения равным IP-адресу компьютера №4. Пакеты передаются на петлевой интерфейс и обрабатываются локально.
4. Маршрут продвижения пакетов в данную локальную сеть, к которой принадлежит узел № 4. Передаваемые в эту сеть пакеты направляются через Ethernet интерфейс узла №4 непосредственно узлу получателю (маршрутизатор для передачи пакетов в эту сеть не используется).
5. Путь для широковещательных рассылок в сеть с номером 21.0.0.0 равным номеру сети адреса 21.59.231.78 в соответствии с адресацией на основе классов. Данная строка характерна для таблиц маршрутизации семейства ОС Windows, в минимальных таблицах большинства других ОС по умолчанию отсутствует.
6. Маршрут для групповых (multicast) рассылок. Данная строка характерна для таблиц маршрутизации семейства ОС Windows, в минимальных таблицах большинства других ОС по умолчанию отсутствует.
7. Маршрут для организации ограниченного широковещания. Широковещательные IP-пакеты доставляются всем узлам локальной сети Ethernet с помощью широковещательных Ethernet-кадров.

Замечания:
1. Интерфейсы в ОС Windows идентифицируются основными IP-адресами интерфейсов.
2. Для непосредственно подключенной к узлу сети в таблице маршрутизации в поле "Шлюз**"** указан IP-адрес интерфейса. Это означает, что пакет, адресованный в эту сеть, необходимо передать средствами технологии Ethernet, определив MAC-адрес узла получателя с помощью протокола ARP.

5.2 Статическая маршрутизация

В этой главе будут рассмотрены примеры составления статических таблиц маршрутизации в IP-сети.

При составлении таблиц маршрутизации будем придерживаться правил, которые часто применяются на практике:

1. При наличии нескольких путей продвижения пакетов в некоторую сеть, выбирается путь с наименьшим количеством маршрутизаторов (путь минимальной длины);
2. Если через маршрутизатор по умолчанию лежит путь минимальной длины в некоторую сеть, то в таблице не допускаются другие строки, описывающие путь продвижения пакетов в эту сеть (минимизация размера таблицы).

Пример 18

Пусть дана сеть, состоящая из пяти сегментов и одиннадцати компьютеров (см. рис. 16), для адресации компьютеров выделен блок адресов 25.15.1.0/24.

Необходимо:

1. Присвоить всем компьютерам IP-адреса с учетом того, что число компьютеров в каждом сегменте будет увеличено до 16;
2. Указать таблицы маршрутизации для компьютеров 4, 7 и 10.

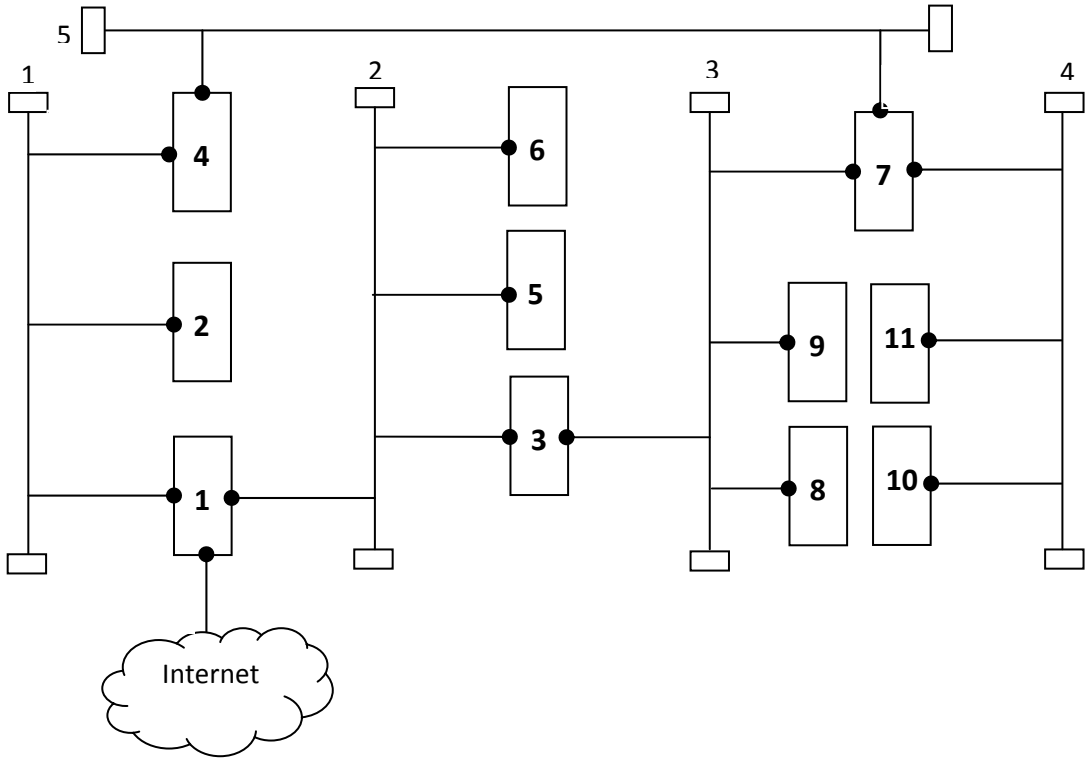

Рис. 16. Схема сети

Компьютеры с номерами 1, 3, 4, 7 имеют более одного сетевого интерфейса и выполняют функции маршрутизаторов, через маршрутизатор №1 осуществляется подключение к сети Интернет

Замечания:

- Для упрощения схемы на рисунке 10 представлены Ethernet-сети на основе коаксиального кабеля. Исходя из принципов работы стека протоколов TCP/IP, принципы передачи IP-пакетов не изменятся, если вместо коаксиального кабеля используются повторители или коммутаторы.
- В таблицах маршрутизации не будут приведены строки минимальной таблицы маршрутизации, за исключением строк, соответствующих путям продвижения пакетов в непосредственно подключенные сети.

Рассмотрим, какие маршруты должны быть представлены в таблицах маршрутизации с учетом выше указанных замечаний:

1. Маршрут для передачи пакетов во внешние сети через маршрутизатор по умолчанию;
2. Маршруты продвижения пакетов в сети, для которых путь через маршрутизатор по умолчанию не является кратчайшим;
3. Маршруты для передачи пакетов в непосредственно подключенные сети.

Назначение компьютерам IP-адресов

С точки зрения межсетевого уровня данная сеть состоит из пяти подсетей, объединенных с помощью маршрутизаторов.

Выделим блоки адресов для каждой подсети. Заметим, что в исходном адресном блоке 25.15.1.0/24 имеется восемь разрядов, часть которых можно использовать для идентификации подсетей и номеров узлов (см. рис. 17).

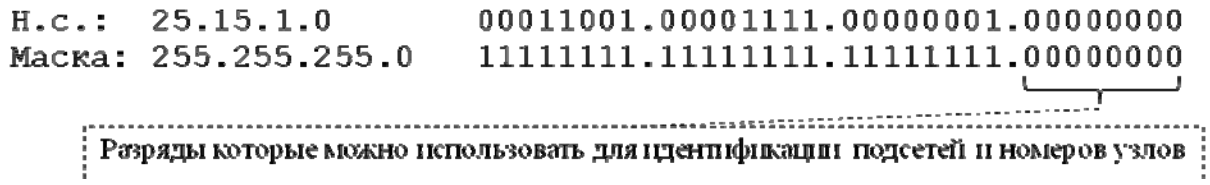

Рис. 17. Двоичное представление номера сети и маски исходного блока

Отдельный блок адресов должен содержать адреса для всех сетевых интерфейсов подсети плюс два специальных адреса - для номера сети и широковещания. В данном случае, каждой подсети необходимо выделить блок из не менее чем 18 адресов (16 адресов + 2 специальных адреса).

Определим сколько разрядов необходимо выделить в адресе под номер узла для получения 18 адресов. В соответствии с правилами выделения адресных блоков (см. параграф 3.3) под номер узла должно быть выделено m разрядов, где $2^{m-1} < 16+2 \leq 2^m$. Следовательно, под номер узла выделяем 5 разрядов ($2^4 < 16+2 < 2^5$). Для идентификации подсетей остаётся 3 разряда – эти разряды дают 8 битовых комбинаций, с помощью которых можно идентифицировать 8 адресных блоков (см. рис. 18, 19).

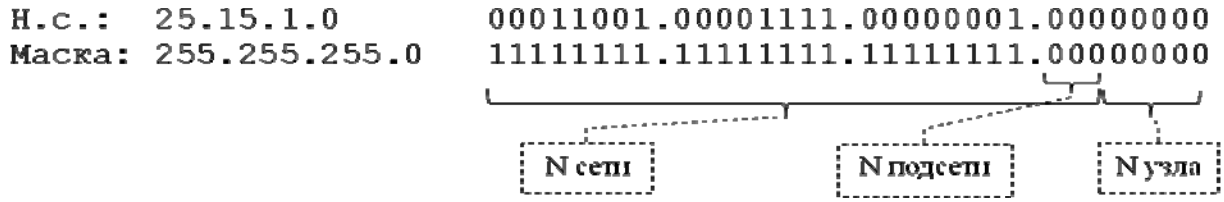

Рис. 18. Назначение разрядов

Рис. 19. Варианты номеров сетей

Сопоставим подсетям номера сетей и соответствующие им адресные блоки:

Сегмент №1 – номер сети 25.15.1.0/27, блок адресов 25.15.1.0 – 25.15.1.31;

Сегмент №2 – номер сети 25.15.1.32/27, блок адресов 25.15.1.32 – 25.15.1.63;

Сегмент №3 – номер сети 25.15.1.128/27, блок адресов 25.15.1.128 – 25.15.1.159;

Сегмент №4 – номер сети 25.15.1.160/27, блок адресов 25.15.1.160 – 25.15.1.191;

Сегмент №5 – номер сети 25.15.1.192/27, блок адресов 25.15.1.192 – 25.15.1.223;

Заметим, что для данной сети необходимо всего пять блоков адресов, три блока адресов использоваться не будут.

Присвоим сетевым интерфейсам адреса из соответствующих блоков (см. рис. 20).

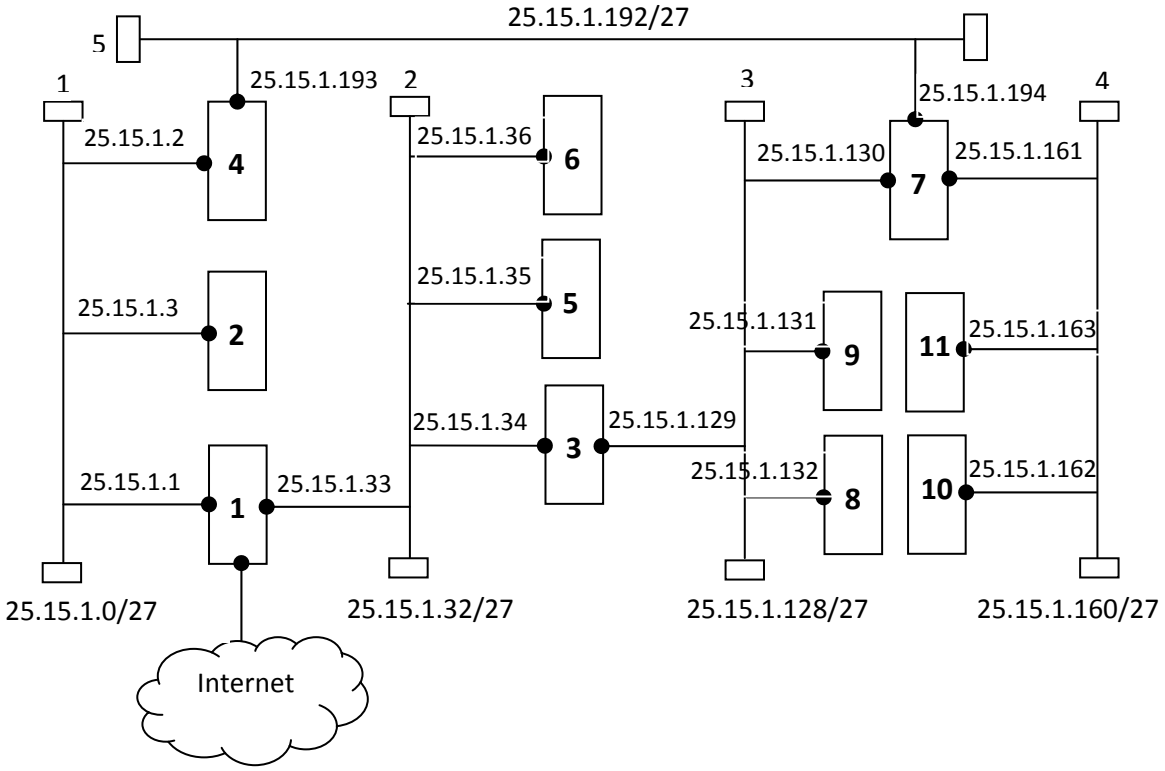

Рис. 20. Присвоение адресов сетевым интерфейсам

Составление таблиц маршрутизации

Заметим, что для узла №4 имеются два пути продвижения пакетов в сеть Интернет: первый – через маршрутизатор №1 (длина пути равна 1), второй – через маршрутизатор №7 (длина пути равна 3). Кратчайший путь лежит через маршрутизатор №1, следовательно, маршрутизатором по умолчанию необходимо назначить этот маршрутизатор. Пакеты маршрутизатору №1 будут пересылаться на интерфейс с адресом 25.15.1. 1 через интерфейс с адресом 25.15.1. 2, следовательно, в таблице маршрутизации должна содержаться строка:

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.1	25.15.1.2

В сеть 25.15.1.32/27 имеются два пути продвижения пакетов: через маршрутизатор №1 (длина пути равна 1) и маршрутизатор №7 (длина пути равна 2). Следовательно, путь через маршрутизатор по умолчанию является кратчайшим и дополнительная строка в таблице маршрутизации для этой сети не нужна.

В сети 25.15.1.128/27 и 25.15.1.160/27 имеются два пути продвижения пакетов: через маршрутизатор №1 (длина пути равна 2) и маршрутизатор №7 (длина пути равна 1). Кратчайший путь лежит через маршрутизатор №7, пакеты этому маршрутизатору будут передаваться на интерфейс с адресом 25.15.1.194 через интерфейс с адресом 25.15.1.193. Следовательно, в таблице маршрутизации должны содержаться строки:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.128	255.255.255.224	25.15.1.194	25.15.1.193
25.15.1.160	255.255.255.224	25.15.1.194	25.15.1.193

К маршрутизатору №4 непосредственно подключены две сети, их адреса:

1. 25.15.1.0/27
2. 25.15.64.192/27

Пакеты с адресами из указанных блоков должны передаваться непосредственно в соответствующие локальные сети без участия других маршрутизаторов, следовательно, в таблице маршрутизации необходимо прописать следующие строки:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.0	255.255.255.224	25.15.1.2	25.15.1.2
25.15.1.192	255.255.255.224	25.15.1.193	25.15.1.193

Таблица 4. Таблица маршрутизации узла №4

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.1	25.15.1.2
25.15.1.128	255.255.255.224	25.15.1.194	25.15.1.193
25.15.1.160	255.255.255.224	25.15.1.194	25.15.1.193
25.15.1.0	255.255.255.224	25.15.1.2	25.15.1.2
25.15.1.192	255.255.255.224	25.15.1.193	25.15.1.193

Заметим, что для маршрутизатора №7 имеются два пути продвижения пакетов в сеть Интернет: первый – через маршрутизатор №3 (длина пути равна 2), второй – через маршрутизатор №4 (длина пути равна 2). Длины путей равны, поэтому можно выбрать в качестве маршрутизатора по умолчанию любой из указанных маршрутизаторов (на практике выбирают наименее загруженный маршрутизатор или маршрутизатор через который проходит наибольшее количество маршрутов). Выберем маршрутизатором по умолчанию маршрутизатор №4. Пакеты этому маршрутизатору будут пересылаться на интерфейс с адресом 25.15.1. 193 через интерфейс с адресом 25.15.1. 194, следовательно, в таблице должна содержаться строка:

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.193	25.15.1.194

В сеть 25.15.1.0/27 имеются два пути продвижения пакетов: через маршрутизатор №3 (длина пути равна 2) и маршрутизатор №4 (длина пути равна 1). Следовательно, путь через маршрутизатор по умолчанию является кратчайшим и дополнительная строка в таблице маршрутизации для этой сети не нужна.

В сети 25.15.1.32/27 имеются два пути продвижения пакетов: через маршрутизатор №3 (длина пути равна 1) и маршрутизатор №4 (длина пути равна 2). Кратчайший путь лежит через маршрутизатор №3, пакеты этому маршрутизатору будут передаваться на интерфейс с адресом 25.15.1.129 через интерфейс с адресом 25.15.1.130. Следовательно, в таблице маршрутизации должна содержаться строка:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.32	255.255.255.224	25.15.1.129	25.15.1.130

К маршрутизатору №7 непосредственно подключены три сети, их адреса:

1. 25.15.1.128/27
2. 25.15.1.160/27
3. 25.15.1.192/27

Пакеты в эти сети должны передаваться непосредственно в соответствующие локальные сети без участия других маршрутизаторов, следовательно, в таблице маршрутизации должны содержаться строки:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.128	255.255.255.224	25.15.1.130	25.15.1.130
25.15.1.160	255.255.255.224	25.15.1.161	25.15.1.161
25.15.1.192	255.255.255.224	25.15.1.194	25.15.1.194

Таблица 5. Таблица маршрутизации узла №7

Адрес н-я	Маска	Шлюз	Интерфейс

0.0.0.0	0.0.0.0	25.15.1.193	25.15.1.194
25.15.1.32	255.255.255.224	25.15.1.129	25.15.1.130
25.15.1.128	255.255.255.224	25.15.1.130	25.15.1.130
25.15.1.160	255.255.255.224	25.15.1.161	25.15.1.161
25.15.1.192	255.255.255.224	25.15.1.194	25.15.1.194

Заметим, что для узла №10 имеется единственный путь продвижения пакетов во внешние сети – через маршрутизатор №7. Выберем его маршрутизатором по умолчанию, пакеты этому маршрутизатору будут пересылаться на интерфейс с адресом 25.15.1. 161 через интерфейс с адресом 25.15.1. 162. Следовательно, в таблице должна содержаться строка:

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.161	25.15.1.162

К узлу №1 непосредственно подключена единственная сеть 25.15.1.160/27. Пакеты в эту сеть должны передаваться непосредственно в локальную сеть без участия других маршрутизаторов, следовательно, в таблице маршрутизации должна содержаться строка:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.160	255.255.255.224	25.15.1.162	25.15.1.162

Таблица 6. Таблица маршрутизации узла №10

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.161	25.15.1.162
25.15.1.160	255.255.255.224	25.15.1.162	25.15.1.162

Агрегация маршрутов

В таблице маршрутизации узла №4 (таблица 4) имеются две строки:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.128	255.255.255.224	25.15.1.194	25.15.1.193
25.15.1.160	255.255.255.224	25.15.1.194	25.15.1.193

Заметим:

1. В первой строке определяется путь продвижения пакетов для сети 25.15.1.128/27, которой соответствует блок адресов 25.15.1.128 – 25.15.1.159.
2. Во второй строке определяется путь продвижения пакетов для сети 25.15.1.160/27, которой соответствует блок адресов 25.15.1.160 – 25.15.1.191.
3. Шлюзом для сетей 25.15.1.128/27 и 25.15.1.160/27 указан один и тот же маршрутизатор с адресом 25.15.1.194.
4. Адреса указанных выше блоков имеют одинаковый префикс (см. рис. 21).

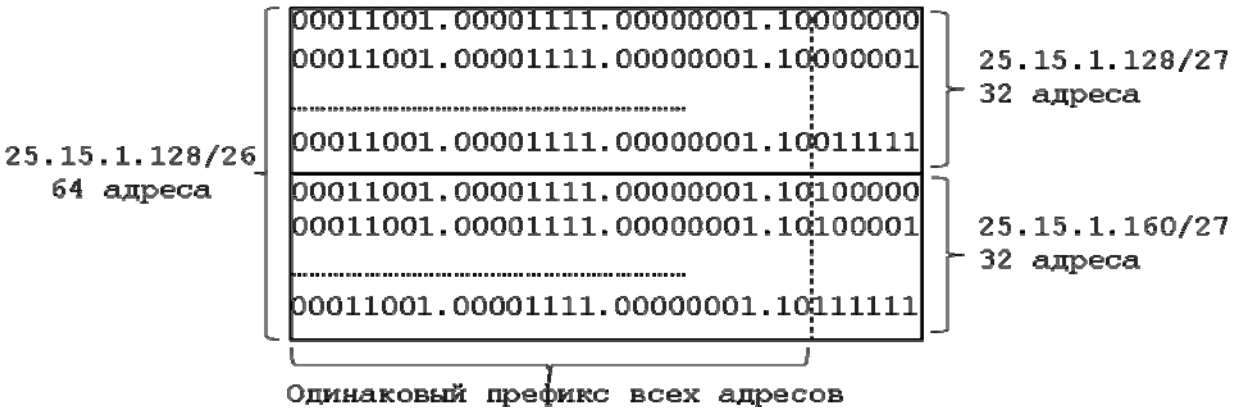

Рис. 21. Представление адресов в двоичной форме

Этот префикс определяет номер сети 25.15.1.128/26, которому соответствует блок адресов 25.15.1.128–25.15.1.191 равный объединению блоков адресов сетей 25.15.1.128/27 и 25.15.1.160/27.

Следовательно, две строки в таблице маршрутизации узла №4 можно заменить одной строкой:

Адрес н-я	Маска	Шлюз	Интерфейс
25.15.1.128	255.255.255.192	25.15.1.194	25.15.1.193

С точки зрения маршрутизации путь продвижения пакетов не изменился – эта строка определяет тот же маршрут и для того же блока адресов, что и указанные выше строки. Таким образом, таблица маршрутизации узла №4 (таблица 4) эквивалентна следующей таблице:

Таблица 7. Таблица маршрутизации узла №4 с агрегирование маршрутных записей.

Адрес н-я	Маска	Шлюз	Интерфейс
0.0.0.0	0.0.0.0	25.15.1.1	25.15.1.2
25.15.1.128	255.255.255.192	25.15.1.194	25.15.1.193
25.15.1.0	255.255.255.224	25.15.1.2	25.15.1.2
25.15.1.192	255.255.255.224	25.15.1.193	25.15.1.193

Операция объединения нескольких маршрутных записей в одну на основе одинакового префикса называется **агрегированием маршрутов**. Для того, чтобы с помощью агрегирования можно было значительно сократить таблицы маршрутизации необходимо на этапе проектирования сети распределять подсетям адресные блоки с учетом возможности их дальнейшего объединение в маршрутных записях.

Бесклассовая междоменная маршрутизация

Бесклассовая междоменная маршрутизация (Classless Inter Domain Routing, CIDR) – основной метод маршрутизации, используемый в Интернет в настоящее время (RFC 1518, 1519). CIDR основана на выделении провайдерам услуг Интернет непрерывных блоков адресов, имеющих одинаковый префикс (одинаковую старшую часть). Использование блоков адресов на основе одинакового префикса позволяет отказаться от адресации на основе классов и сократить таблицы маршрутизации за счет агрегирования записей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Семенов, Ю.А. Протоколы и алгоритмы маршрутизации в Интернет [Электронный ресурс] : учебное пособие / Ю.А. Семенов. - Протоколы и алгоритмы маршрутизации в Интернет ; 2020-03-31. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 998 с. - ISBN 978-5-94774-707-2. URL: http://www.iprbookshop.ru/62826.html

2. Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). URL: http://biblioclub.ru/index.php?page=book&id=429094

3. Пуговкин, А.В. Сети передачи данных [Электронный ресурс] : учебное пособие / А.В. Пуговкин. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 138 с. URL: http://www.iprbookshop.ru/72179.html

4. Олифер, В. Г. Основы сетей передачи данных [Электронный ресурс] / В. Г. Олифер, Н. А. Олифер. - Основы сетей передачи данных ; 2021-01-23. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 219 c. - ISBN 2227-8397. URL: http://www.iprbookshop.ru/73702.html