IP-протокол

Общие сведения

Сервис

Формат пакета (дейтаграммы)

Поля заголовка, ToS, Фрагментация, Опции

Формат IP-адреса, CIDR, VLSM

СОДЕРЖАНИЕ

Общие сведения

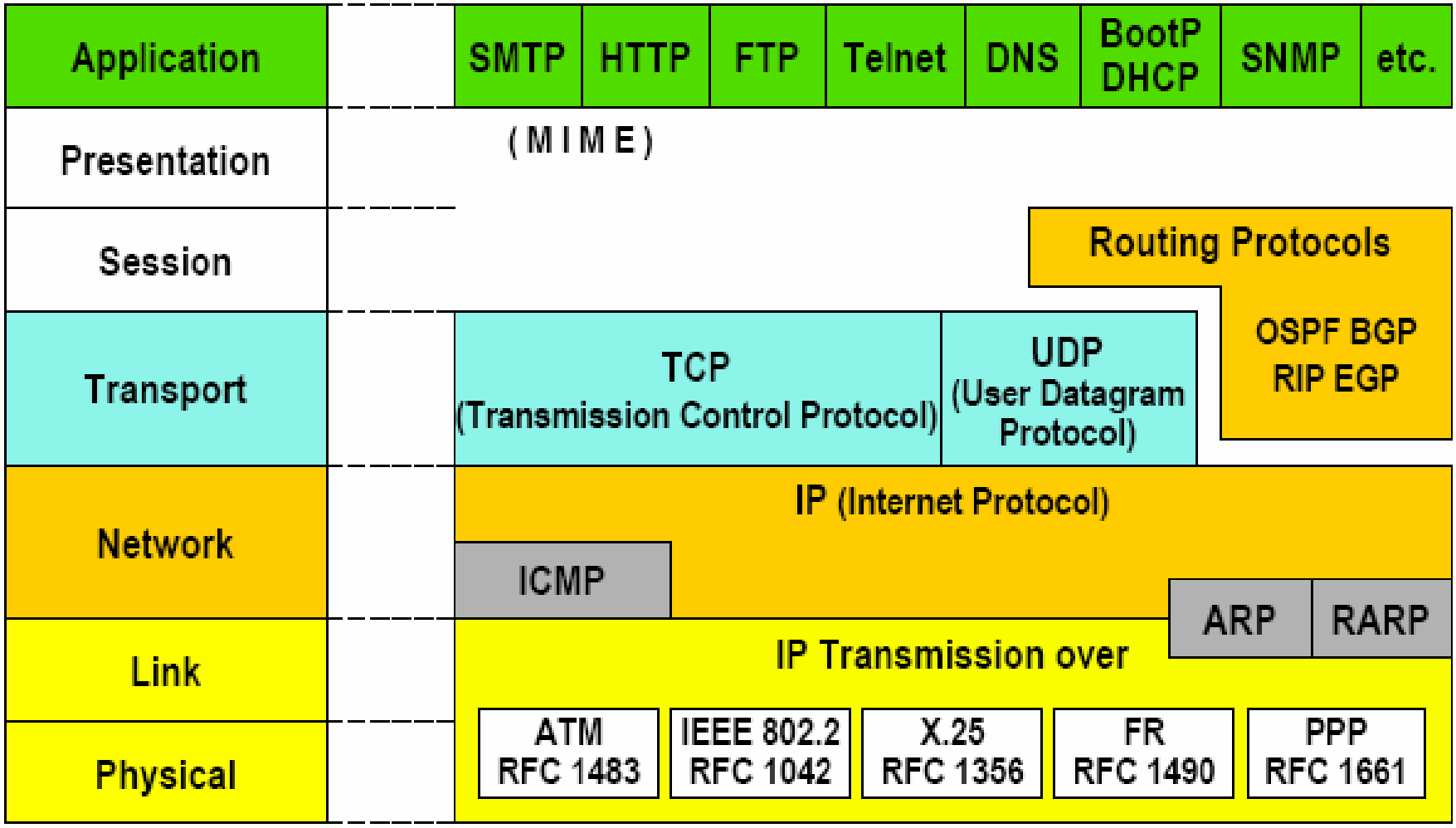
IP – технология (L3 OSI RM)

- **Технология пакетной коммутации**
  - Пакетные коммутаторы называют Маршрутизатор (router или gateway в терминологии IETF)
  - Конечные системы называют IP-хост
  - Структурирован L3 адрес (IP-адрес)
- **Сервис**
  - Не ориентирован на соединения
    - ✓ Пакеты (датаграммы) передаются без предварительного установления соединения
  - Наилучшие условия доставки
    - ✓ Пакеты уничтожаются в случае их искажения или перегрузки сети

TCP – технология (L4 OSI RM)

- **Разделена ответственность между сетью (network) и оконечными системами (end systems, IP-хост)**
  - Роутеры отвечают за доставку пакетов удаленным конечным системам на основании их IP-адреса
  - IP-хосты отвечают за управление end-to-end (из конца в конец)
- **Управление end-to-end**
  - Осуществляется вышележащими уровнями в IP-хостах
  - TCP (Transmission Control Protocol)
    - ✓ Ориентирован на соединения
    - ✓ Последовательная нумерация, оконный принцип
    - ✓ Исправление ошибок передачи
    - ✓ Управление потоком

IP в стеке TCP/IP



IP (Internet Protocol)–общие сведения

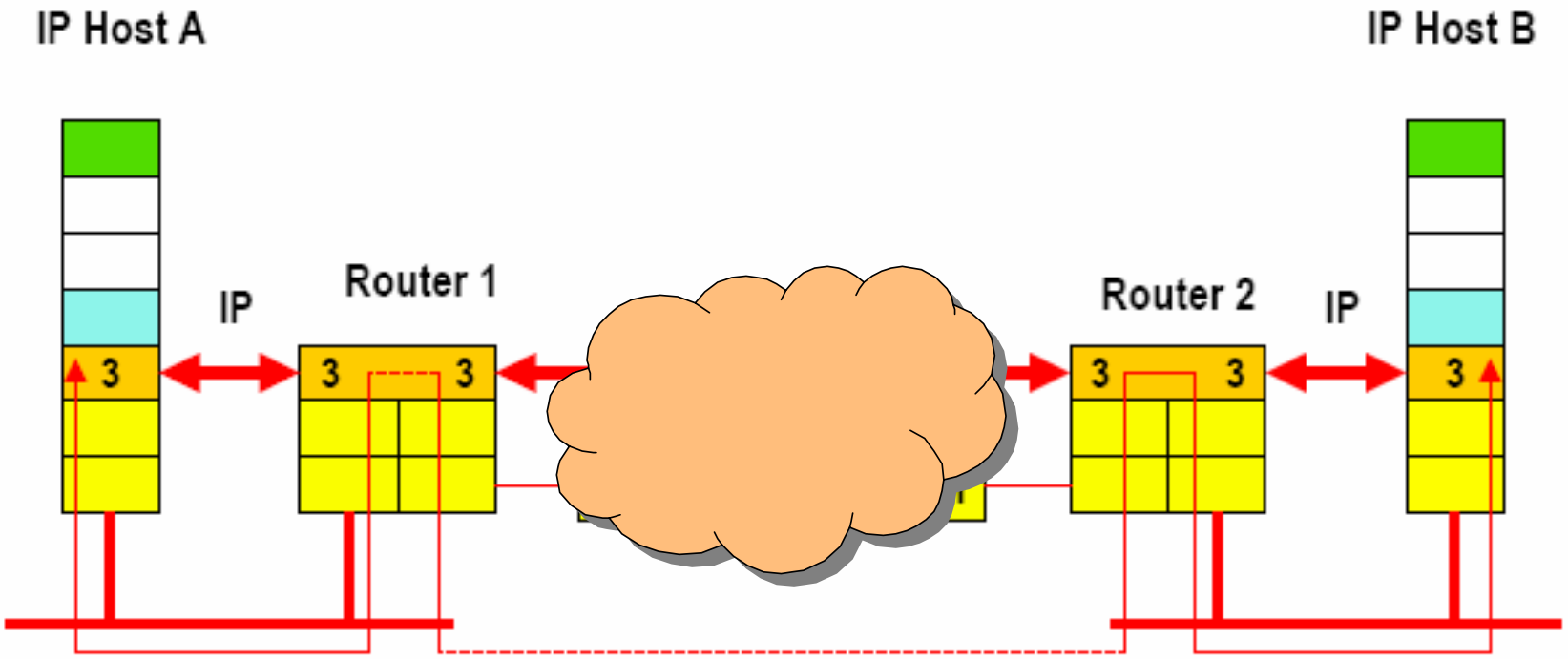
- **Протокол сетевого уровня (L3 OSI RM)**
  - Совместно с протоколом ICMP (Internet Control Message Protocol) образует сетевой уровень
- **IP PDU называется пакетом или дейтаграммой**
  - Пакет, поскольку коммутация пакетов
  - Дейтаграмма, поскольку:
    - ✓ независимость их следования друг от друга
    - ✓ каждая обрабатывается как независимая единица данных
    - ✓ без установления соединения
- **Формат IP-пакета (IP PDU) описан в RFC791 (19??)**

Назначение IP

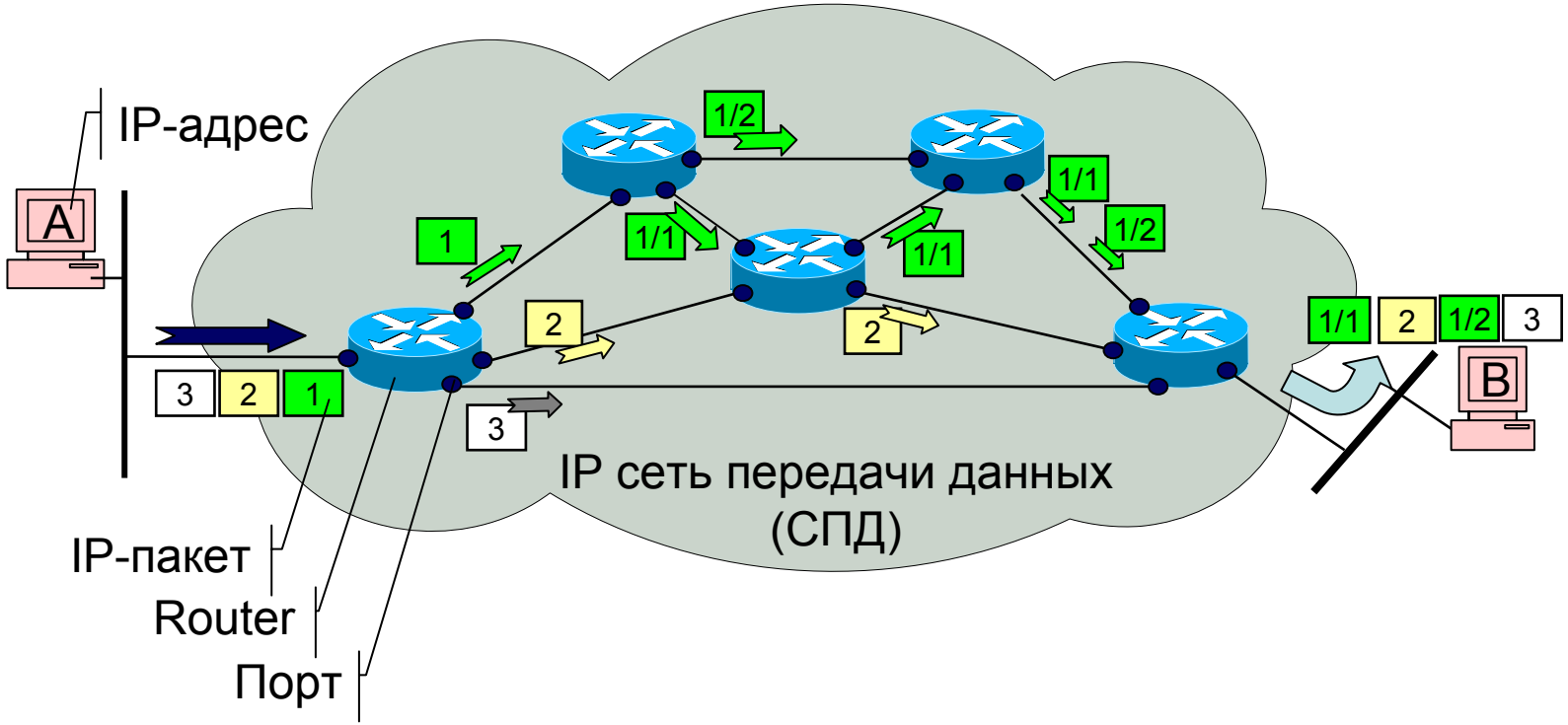
- **Доставка пакетов получателю (end-to-end)**
- **Характеристики доставки**
  - Ненадежная, пакет удаляется роутером
    - ✓ если в заголовке пакета ошибка
    - ✓ если роутер перегружен
    - ✓ если истекло время жизни пакета
  - Неупорядоченная (пакеты могут доставляться не в порядке передачи)
  - Возможно назначение пакетам приоритета для обеспечения требуемого качества обслуживания (QoS) приложений
  - Имеется опциональный сервис (принудительная маршрутизация и т.д.)

IP расположен на L3 OSI RM

Layer 3 Protocol = IP
Layer 3 Routing Protocols = RIP, OSPF, EIGRP, BGP



Маршрутизация - основная функция IP



Все хосты в Интернет имеют уникальный IP-адрес

Каждый роутер выполняет маршрутизацию пакетов на основе таблицы маршрутизации

Таблица маршрутизации формируется протоколами маршрутизации

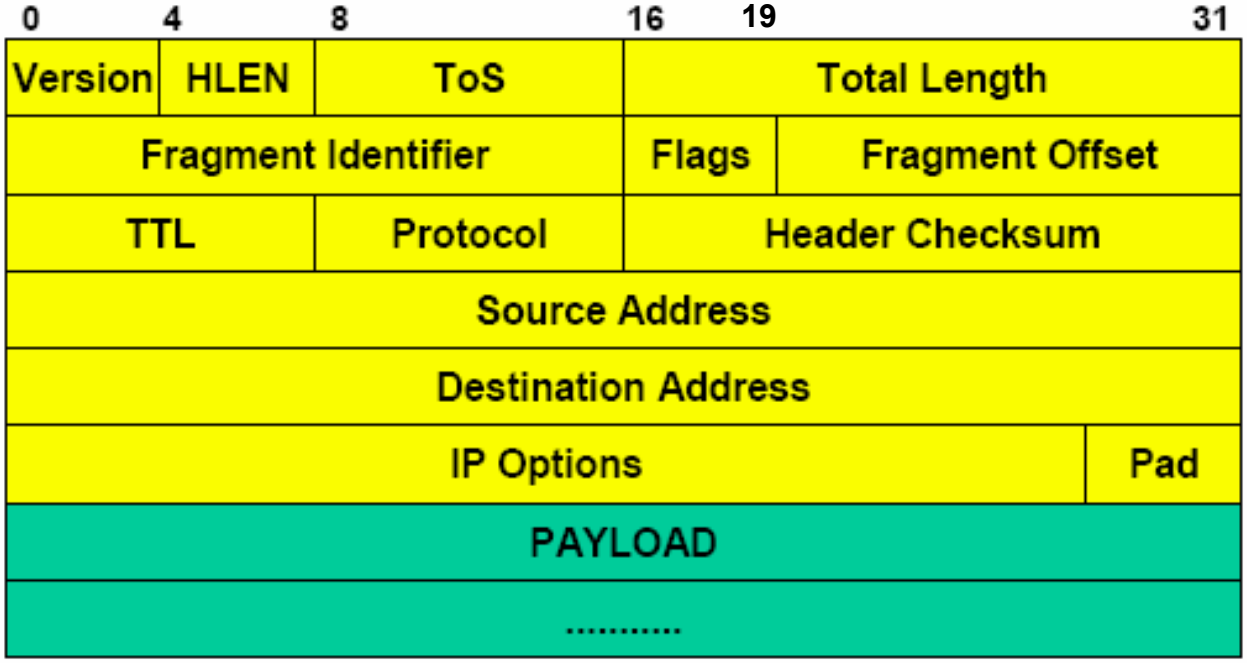
В таблице маршрутизации каждого Интернет-роутера всем IP-адресам хостов (компьютеров) в Интернет сопоставлено направление передачи (порт роутера)

IP протокол: сервис

- **Четыре основных вида межсетевого сервиса**
  - Качество обслуживания
  - Время жизни (время существования пакета в сети)
  - Дополнительные возможности (временные метки, безопасность, специальная маршрутизация)
  - Контрольная сумма заголовка (пакет отбрасывается IP-модулем и отправитель оповещается посредством протокола ICMP)

IP-заголовок

Заголовок IP-пакета



Identification – “Идентификатор” фрагмента

FLG (Flags) – “Флаг”, управляет фрагментацией

Fragment Offset –“смещение фрагмента” относительно начала, кратно 8 байтам

Head Checksum – “Контрольная сумма заголовка”

Source IP Address – “IP-адрес источника”

Destination IP Address – “IP-адрес назначения”

Vers – “версия” протокола, текущая IPv4, есть IPv6

HLEN – “длина заголовка” в 32-х разрядных словах

ToS (Type jf Service) – “тип сервиса”, качество обслуживания

Total Length – “полная длина” в байтах (заголовок + данные)

TTL(Time-to-Live) –“время жизни” датаграммы

Protocol – “протокол” верхнего уровня

Options – “опции”, дополнительные функций

PAD - “дополнение” заголовка до границы 32 бита

Поля заголовка IP-пакета

- **Vers – "версия" IP-протокола**
  - текущая версия IPv4
  - в стадии внедрения (перехода на) версия IPv6
- **TTL (Time-to-Live) –"время жизни" в сек**
  - устанавливается отправителем (15-30 сек)
  - уменьшается на 1 по мере прохождения точек маршрута
  - при достижении TTL=0, дейтаграмма уничтожается
  - назначение – не засорять сеть
- **Protocol – "протокол" верхнего уровня**
  - Например: 1(ICMP), 6(TCP), 8(EGP), 17(UDP), 89(OSPF) ...
  - Пока зарегистрировано около 100 различных типов для IP

Поля заголовка IP-пакета

- **HLEN – "длина заголовка"**
  - в 32-х разрядных словах
  - Длина заголовка различная, зависит от наличия опций
    - ✓ HLEN min = 5 (20 байт)
    - ✓ HLEN max = 15 (60 байт)
- **Total Length – "полная длина"**
  - Длина дейтаграммы в байтах (заголовок + данные)
  - Если фрагментация – длина фрагмента
  - Максимальная длина = 65535 байт
  - Длина области данных = Total Length – (HLEN x 4)
  - Каждый хост должен принять хотя бы 576 байт
    - ✓ или как законченную дейтаграмму или для последующей сборки

Поля заголовка IP-пакета

- **Source IP Address – "IP-адрес источника"**
  - IP-адрес хоста (роутера/коммутатора), сформировавшего дейтаграмму для отправки
  - Этот хост называют "источником" или "передатчиком"
  - Сформированную дейтаграмму называют "первоначальной" или "оригинальной", поскольку по мере движения через сеть она может быть преобразована, например, фрагментирована
- **Destination IP Address – "IP-адрес назначения"**
  - IP-адрес хоста (роутера/коммутатора), которому эта дейтаграмма отправлена
  - Хост, которому отправлена дейтаграмма называют "удаленным", "назначения" или "приемником"
- **Head Checksum – "Контрольная сумма заголовка"**
  - При ошибке пакет уничтожается
  - Источник извещается об этом факте по протоколу ICMP

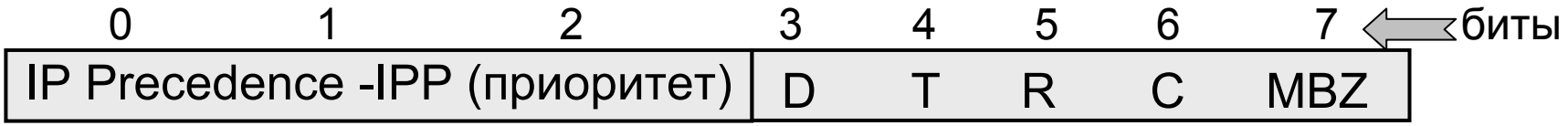
IP-приоритет (ToS)

TOS (Type of Service) – историческая справка

- **Отцы-основатели Интернет заложили в поле TOS возможность реализации качества сервиса**
- **Цитата: «байт “тип сервиса” используется для указания абстрактных параметров требуемого качества обслуживания»**
  - На основании этих параметров производится выбор реальных характеристик механизмов обслуживания при передачи дейтаграммы через заданную сеть» (RFC791, 1981 г.)
- **До конца 80-х годов Интернет в зародышевом состоянии:**
  - Низкий объем трафика, мало сетевых приложений
  - Поддержкой TOS пренебрегали и не реализовывали в IP-протоколе
  - IP-приложения не устанавливали TOS, а роутеры игнорировали его при принятии решения
- **Однако предполагалось использование поля TOS в следующем варианте**

TOS (Type of Service) – “тип сервиса”

- **Старое значение поля TOS определено в RFC791, RFC1349 и сообщает роутеру:**



8 классов приоритета (2^3)

Называется :

- IP приоритет
- IP Precedence
- IPP

предпочтительный путь в сети

4 бита – четыре варианта:

min задержка [D]

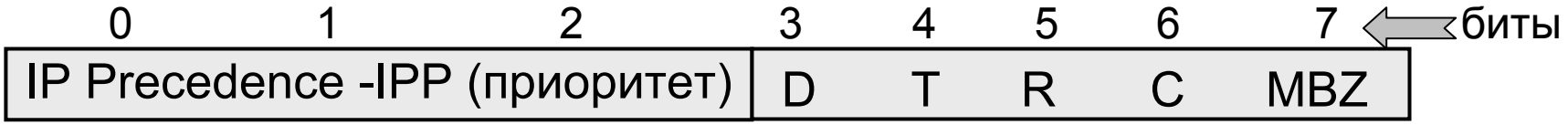
min стоимость [C]

max пропускная способность [T]

max надежность [R]

TOS (Type of Service) – “тип сервиса”

Старое значение поля TOS



111 Сетевое управление (Network control)

110 Межсетевое управление (Internetwork control)

101 Критический (ceitic/ecp) (Critical)

100 Экстренный (Flash override)

011 Срочный (Flash)

010 Немедленный (Immediate)

001 Приоритетный (Priority)

000 Обычный (Routine)

DTRC бит:

1000	D	Min delay	(min задержка)
0**1**00	T	Max throughput	(max скорость)
00**1**0	R	Max reliability	(max надежность)
000**1**	C	Min cost	(min стоимость)
0000	..	Normal service	(обычный сервис)

MBZ бит зарезервирован на будущее

Только один бит может быть равен 1

TOS (Type of Service) – “тип сервиса”

- **Биты приоритета:**
  - Определяют класс обработки пакета в пределах роутера, например, приоритет в очередях ввода/вывода.
  - Задаются только относительные уровни приоритетности (между классами), поскольку нет механизмов их задания внутри класса. Например, если telnet и SMTP внутри одного класса, то при заторе в сети нет оснований отбрасывать пакеты telnet в пользу SMTP
- **Биты D,T, R и C**
  - Могут использоваться маршрутизатором для выбора из множества путей (портов) такого, который запрашивается посредством одного из этих битов
- **TOS биты могут игнорироваться, но никогда не должны приводить к отказу от пакета, даже если запрашиваемый сервис недоступен**
- **Интернет не гарантирует запрашиваемый TOS, но многие роутеры учитывают эти запросы при выборе маршрута (OSPF и IGRP)**

TOS (Type of Service) – историческая справка

- **Популярность и коммерческое использование Интернет привело к осознаю важности внедрения качества обслуживания**
  - QoS – quality of service
- **Работоспособность TCP/IP сетей в моменты перегрузки рассмотрена Джоном Наглем -John Nagle (RFC896, 1984)**
  - Проблема заключалась в перегрузке сети TCP-сегментами приложений telnet и rlogin
- **Алгоритм Нагля решал эту проблему (RFC1122, 1989)**
  - реализован во всем программном обеспечении
  - “возвестил” о начале эпохи QoS в сетях IP

TOS (Type of Service) – историческая справка

- **В 1986 году Ван Якобсон (Van Jacobson)**
  - разработал набор функций QoS для конечных систем, являющиеся стандартом де-факто для всех современных реализаций TCP
    - ✓ “механизм медленного старта”
    - ✓ механизм предотвращения перегрузки”
- **В 1990 году для обеспечения оптимальной производительности сети в моменты перегрузки (потери пакетов) разработаны два дополнительных механизма**
  - “механизм быстрой повторной передачи и механизм быстрого восстановления” (RFC2001, 1997 г)
- **Однако это все механизмы QoS в конечных системах**
- **Сквозное QoS, реализуемое в маршрутизаторах, раньше отсутствовало**

TOS (Type of Service) – историческая справка

- **Акцент 1990-х логично переместился на реализацию функций обеспечения качечтва обслуживания в маршрутизаторах**

А именно:

- Обеспечение приложений средствами формулирования требований к ресурсам сети
- Создание механизмов управления потоками на уровне маршрутизаторов и технологий подсетей

TOS (Type of Service) – историческая справка

- **IETF разрабатывает два подхода к обеспечению сквозного QoS:**
  1. Метод интегрированных услуг (intserv)
     - ✓ (intserv - Integrated Services)
  2. Архитектура дифференцированных услуг (diffserv)
     - ✓ (diffserv - differentiated services)

Метод intserv (интегрированных услуг)

- **Требования к ресурсам сети формулируются приложениями посредством протокола RSVP (Resource Reservation Protocol – протокол резервирования ресурсов)**
- **Две услуги Intserv**
  - Гарантированное обслуживание (guaranteed service) предполагает предоставление детерминированных гарантий задержки
    - ✓ обеспечивает только максимальную, но не минимальную или среднюю задержку дейтаграмм
    - ✓ Иногда называют “гарантированная битовая скорость”
  - Регулируемая нагрузка (controlled load service) похожа на механизм негарантированной доставки трафика в слегка загруженной сети
    - ✓ Минимальное вмешательство не RSVP трафика на зарезервированный поток.
    - ✓ Более того, в реализации Cisco предусмотрена изоляция друг от друга отдельных зарезервированных потоков

Метод intserv (интегрированных услуг)

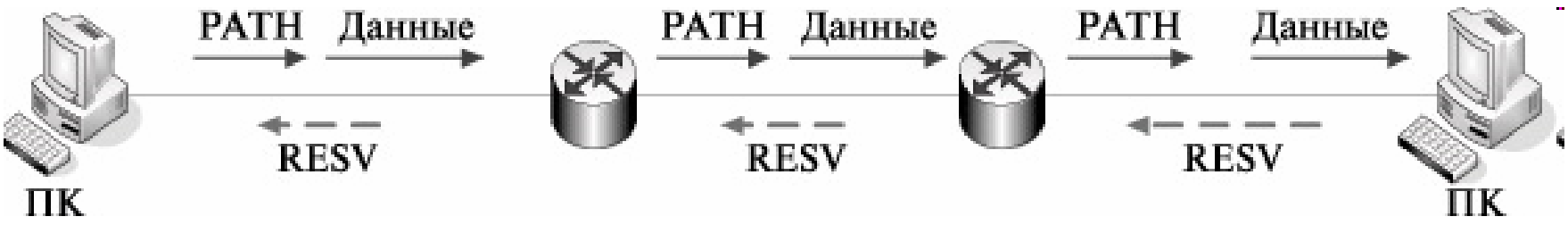
- **Оба метода используют “корзину маркеров” для описания параметров потока данных**
  - среднюю скорость (средний объем данных, который можно передать за единицу времени),
  - размер всплеска (объем данных, который можно отправить в течение заданного промежутка времени без ущерба для планирования очереди) за интервал измерения (квант времени).
- **Получатель запрашивает в RESV-сообщении определенную битовую скорость и размер всплеска**
  - Планировщик WFQ и механизм управления очередью WRED с предпочтительным весом гарантируют, что трафик достигнет получателя через строго определенное время.
- **Недостаток intserv / RSVP**
  - обслуживание каждого потока необходимо производить на всей траектории соединения, что затрудняет его использование масштабах Интернет

Протокол RSVP

- **Конечные системы используют протокол RSVP для запрашивания у сети определенного уровня QoS от имени потока данных приложения.**
  - RSVP-запросы передаются по сети при прохождении каждого узла, который применяется для передачи потока
  - Маршрут для данных и управляющего трафика RSVP определяется по применяемым в сети протоколам маршрутизации
    - ✓ Не нужен специальный протокол маршрутизации
  - Протокол RSVP пытается зарезервировать ресурсы для потока данных на каждом из этих узлов.
- **Ориентирован на использование в приложениях с групповой рассылкой, таких как приложения аудио- и видеоконференций**
- **Однако с его помощью легко можно резервировать полосу пропускания для однонаправленного трафика**
  - например для трафика сетевой файловой системы (Network File System – NFS) и управляющего трафика виртуальных частных сетей (Virtual Private Networks – VPN)

Протокол RSVP: этапы процесса резервирования

- **Отправители посылают управляющие PATH-сообщения**
  - Каждый RSVP-маршрутизатор, получивший PATH-сообщения, сохраняет IP-адрес предыдущей точки назначения, записывает вместо него свой собственный IP-адрес и отправляет обновленное сообщение
- **Получатели запрашивают с помощью RESV-сообщения ресурсы у предыдущего маршрутизатора**
  - RESV - сообщения идут от получателя к отправителю в противоположном направлении по маршруту, пройденному PATH-сообщениями
- **RSVP-маршрутизаторы, если могут, удовлетворяют эти RESV-запросы отсылая его предыдущему маршрутизатору. Если нет ресурсов, они отказывают в резервировании**
- **Отправители, получив запросы на резервирование ресурсов, считают резервирование ресурсов состоявшимся**



RSVP-компоненты

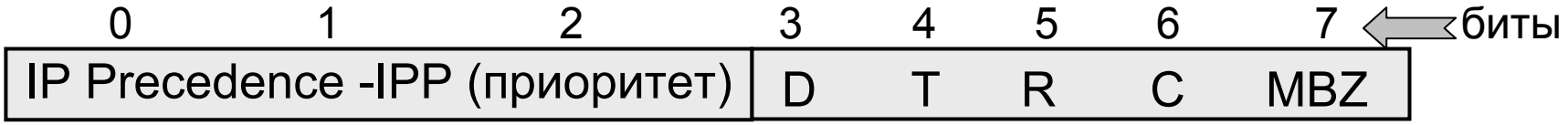
- **RSVP-отправитель** – это приложение, инициирующее отправку трафика в RSVP-сеансе
  - RSVP-отправители могут передавать по RSVP-сети:
    - ✓ **средняя скорость передачи данных;**
    - ✓ **максимальный размер всплеска.**
- **Сеть RSVP**-совместимых маршрутизаторов (RSVP-enabled router network), через которую прокладывается путь между отправителями и получателями
- **RSVP-получатель** (RSVP-receiver) – это приложение, которое получает трафик в RSVP-сеансе.
  - Во время конференций или при передаче голоса по протоколу IP (Voice over IP – VoIP) приложение может играть роль и RSVP-отправителя, и RSVP-получателя.
  - спецификации потока, который RSVP-получатели могут передавать по RSVP-сети:
    - ✓ **средняя скорость передачи данных;**
    - ✓ **максимальный размер всплеска;**
- **QoS**, включая:
  - гарантированное обслуживание – в PATH-сообщениях также описываются максимально возможные задержки в сети;
  - обслуживание с управляемой нагрузкой – маршрутизаторы гарантируют только то, что сетевые задержки будут минимальными.

Архитектура diffserv (дифференцированных услуг)

- **Основная идея – отдельная обработка потоков трафика, запросивших определенный уровень QoS**
  - Байт TOS IP-заголовка представляет собой главный механизм обеспечения diffserv
  - IETF предлагает стандартизировать байт TOS в качестве байта diffserv

TOS (Type of Service) – “тип сервиса”

Вспомним, старое значение поля TOS



111 Сетевое управление (Network control)

110 Межсетевое управление (Internetwork control)

101 Критический (ceitic/ecp) (Critical)

100 Экстренный (Flash override)

011 Срочный (Flash)

010 Немедленный (Immediate)

001 Приоритетный (Priority)

000 Обычный (Routine)

DTRC бит:

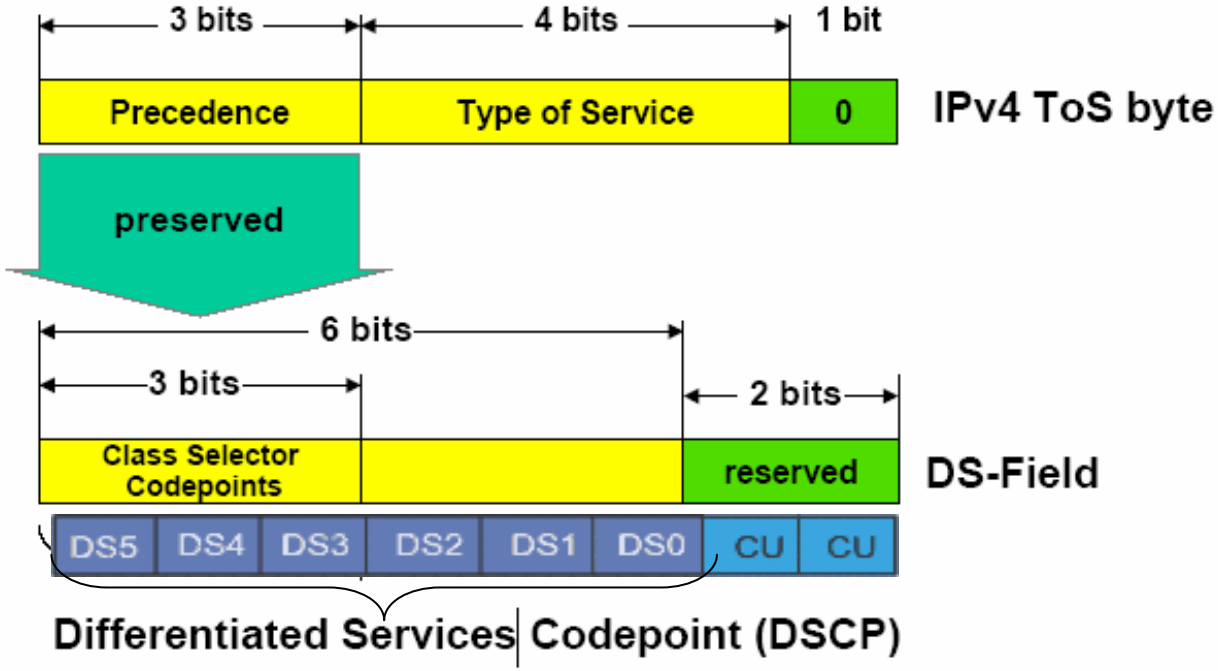
1000	D	Min delay	(min задержка)
0**1**00	T	Max throughput	(max скорость)
00**1**0	R	Max reliability	(max надежность)
000**1**	C	Min cost	(min стоимость)
0000	..	Normal service	(обычный сервис)

MBZ бит зарезервирован на будущее

Только один бит может быть равен 1

Поле DSCP - современная модель дифференцированного сервиса - Differentiated Services (RFC 2474, 2475)

- **Модель DiffServ подразделяет потоки данных на несколько классов и выделяет ресурсы для каждого отдельного класса**
- **В новейших разработках (RFC2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers) поле TOS заменено на DSCP (Differenciated Services Code Point)**
- **Младшие 6 бит выделены для кода DS (Differentiated Services), а старшие два бита пока не определены и их**



Маркируется класс трафика потока

Поток соотносят с обменом между двумя IP-хостами и определяют:

- IP-адресом источника и приемника
- Типом протокола
- Портами TCP и UDP источника и приемника

DSCP

- **Значения DSCP могут быть выражены в цифровой форме или с использованием специальных ключевых слов, называемых поведением сетевых участков (PHB - Per-Hop Behavior). Определено три класса DSCP маркировки:**
  - по возможности (BE – best effort или DSCP 000000)
  - гарантированная доставка (Assured Forwarding, AFxy)
  - срочная доставка (Expedited Forwarding – EF)
- **В дополнение к этим трем определенным классам существуют коды селектора классов (class selector code points), которые обратно совместимы с IPP (CS1-CS7 идентичны значениям 1-7 IPP). Эти PHB описаны в RFC 2547, 2597 и 3246, соответственно.**
- **Определено четыре класса гарантированной доставки, они начинаются с AF и далее две цифры.**
  - Первая цифра (x) определяет AF класс и принимает значения от 1 до 4
  - Вторая цифра (y) определяет уровень вероятности сброса пакета в пределах каждого класса и принимает значения от 1 (минимальная вероятность сброса) до 3 (максимальная вероятность сброса).
- **Значения DSCP могут быть выражены в десятичном формате или с использованием ключевых слов DSCP. Например, DSCP EF аналогично DSCP 46, а DSCP AF31 аналогично DSCP 26.**

IP-фрагментация

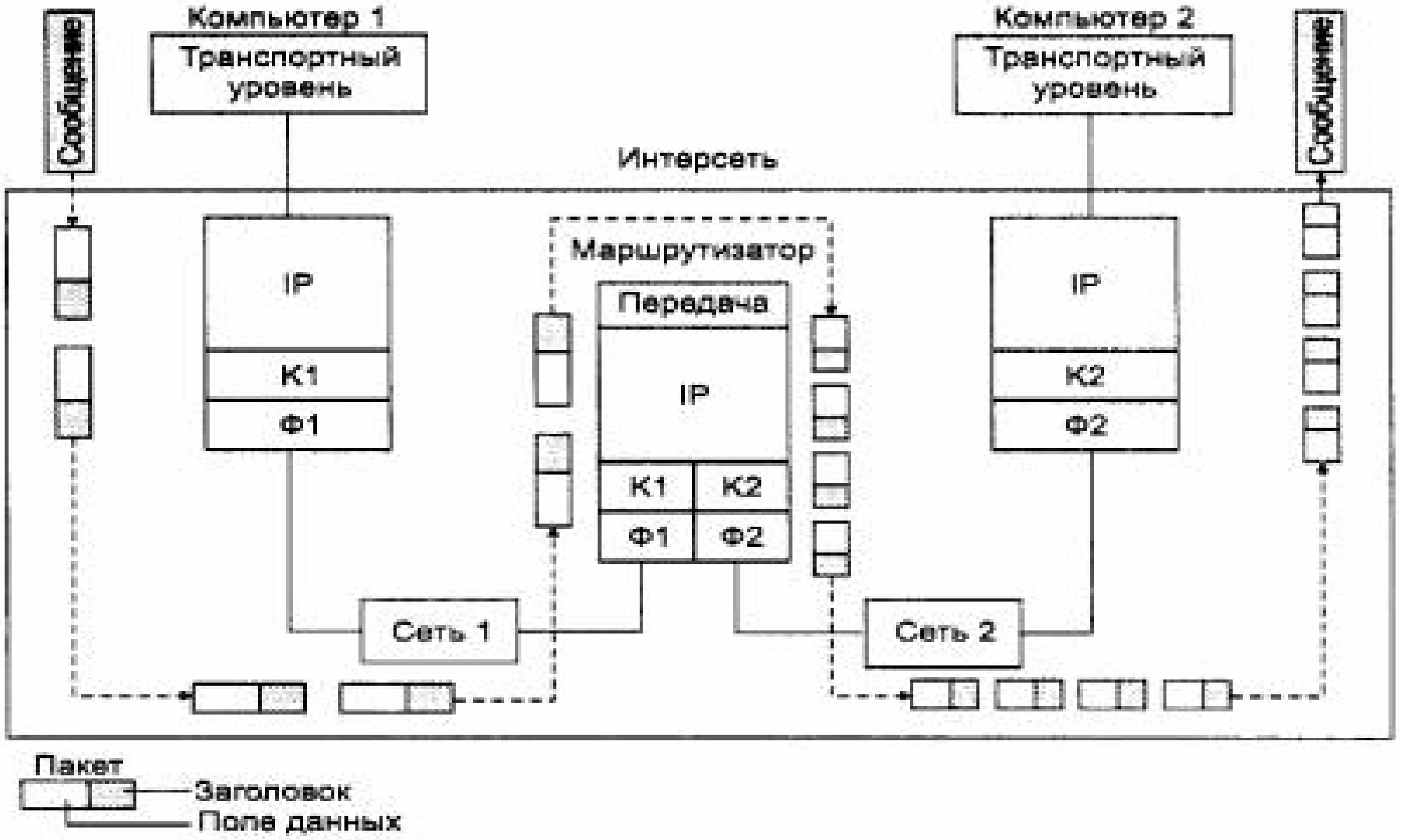
Зачем нужна вообще фрагментация?

- **Следует различать потребность в фрагментации:**
  - в конечных системах, например, в хосте отправителе
  - в маршрутизаторах, которые являются транзитными узлами
- **В хосте отправителе (в стеке TCP/IP) эту задачу решает протокол TCP (L4), который разбивает поток байтов, передаваемый ему с прикладного уровня на сообщения нужного размера для последующей инкапсуляции (с учетом IP-заголовка) в протокол канального уровня (L2). Разбивает, например, на 1460 байт для протокола Ethernet.**
  - Поэтому протокол IP в узле-отправителе (в стеке TCP/IP) не использует свои возможности по фрагментации пакетов

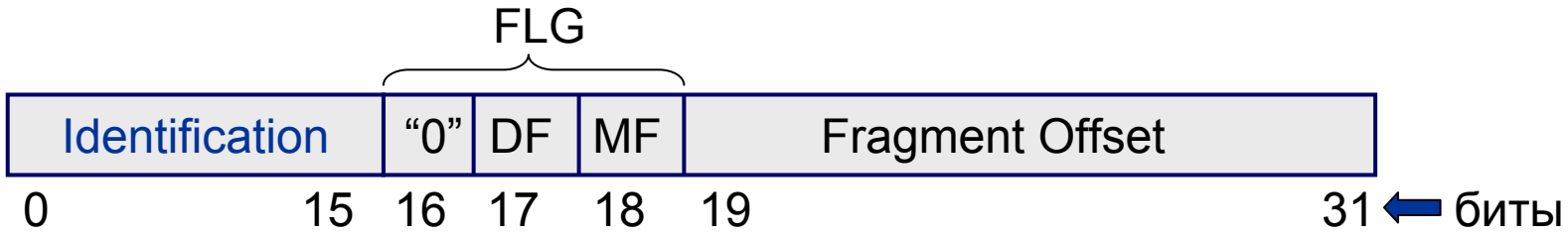
Зачем нужна вообще фрагментация?

- **Если роутер передает IP-пакет в сеть, у которой размер кадра мал для инкапсуляции этого пакета, необходима IP-фрагментация**
- **В большинстве типов локальных и глобальных сетей значения MTU, то есть максимальный размер поля данных (длина кадра), в которое должен инкапсулировать свой пакет протокол IP, значительно отличается:**
  - Сети Ethernet имеют значение MTU =1500 байт
  - сети FDDI – MTU = 4096 байт
  - Сети X.25 - MTU = 128 байт
- **IP разбивает слишком длинный для конкретного типа составляющей сети пакеты на более короткие пакеты**
  - используются поля IP-заголовка, используемые для последующей сборки фрагментов в исходное сообщение

Зачем нужна вообще фрагментация?

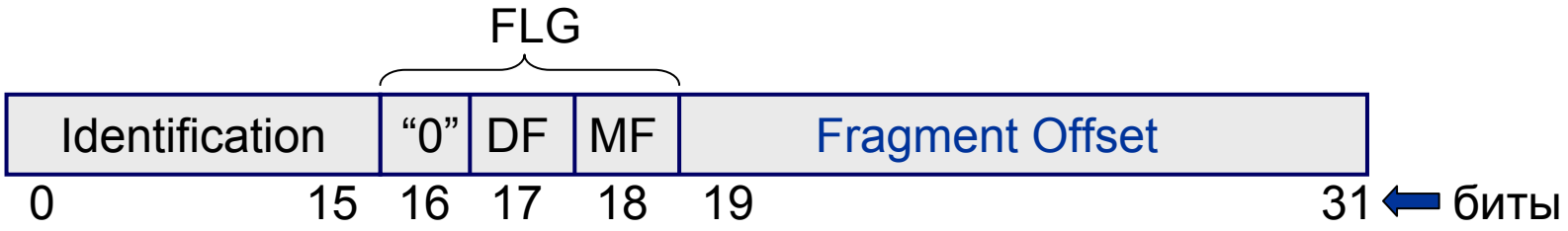


Заголовок IP-пакета (фрагментация)



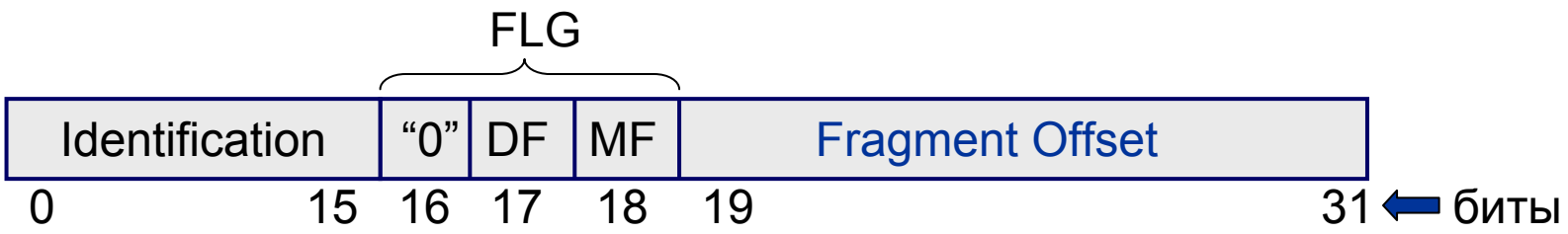
- **Identification – “Идентификатор” фрагмента**
  - используется вместе с полями “FLG” и “Fragment Offset” для правильной сборки пакета
  - код, присваиваемый каждому фрагменту пакета
  - каждый фрагмент получает один и тот же идентификатор
  - если нет фрагментации, значение поля Identification равно 0

Заголовок IP-пакета (фрагментация)



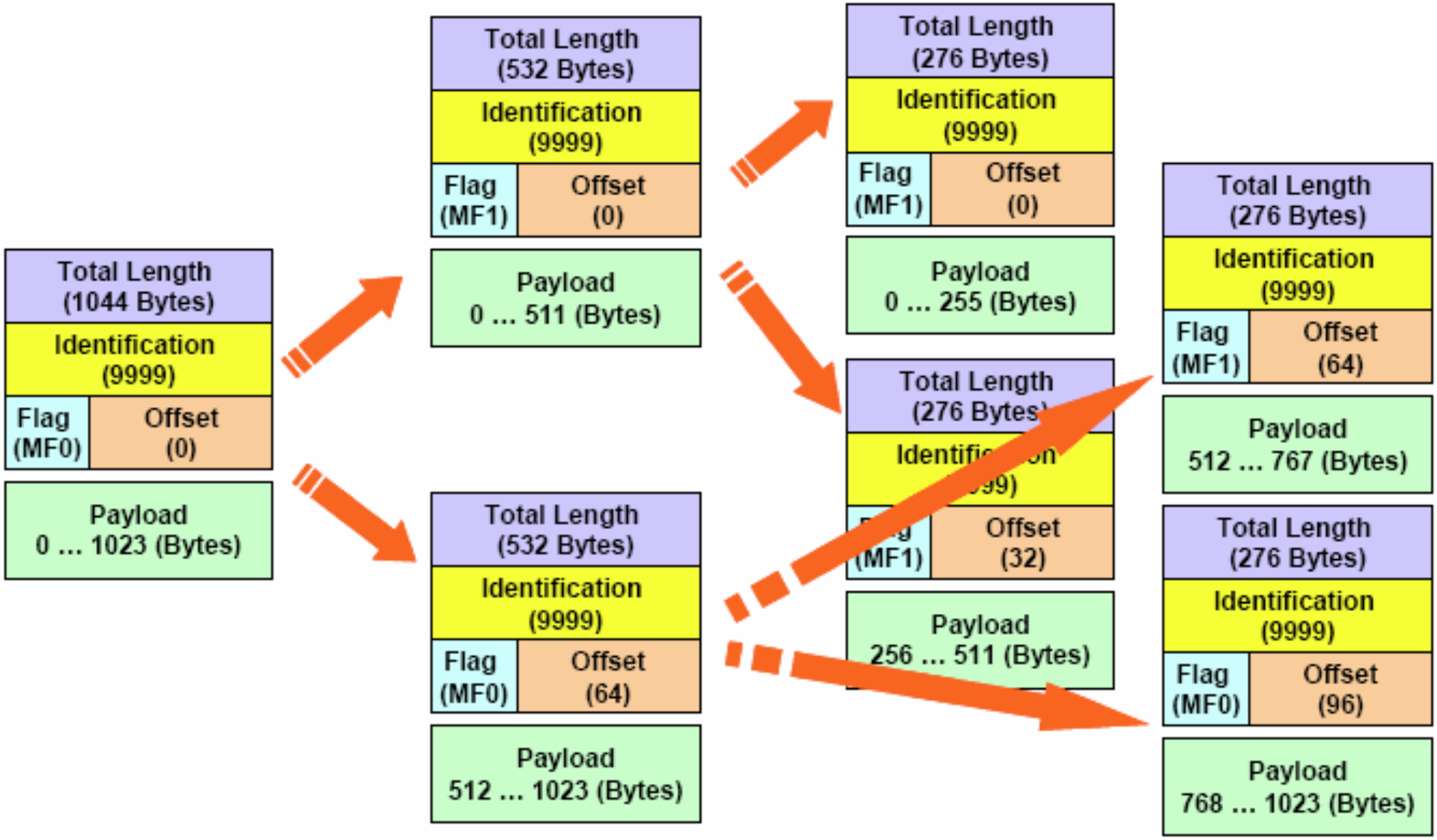
- **FLG (Flags) – “Флаг” управляет фрагментацией**
  - DF (don`t fragment)
    - ✓ если установлен (DF=1), то фрагментация запрещена
    - ✓ дейтаграмма отвергается если MTU (maximum transmission unit) следующего линка (хопа) меньше требуемой для передачи
  - MF (more fragments)
    - ✓ Если MF=1, значит промежуточный фрагмент
      - ➢ Т.е. поступят еще фрагменты, сформированные из первоначальной (оригинальной) дейтаграммы
    - ✓ Если MF=0, значит последний фрагмент
      - ➢ т.е. поступил последний фрагмент первоначальной дейтаграммы и можно попытаться выполнить сборку первоначальной дейтаграммы
      - ➢ или поступила сама первоначальная дейтаграмма, которая не подвергалась фрагментации

Заголовок IP-пакета (фрагментация)

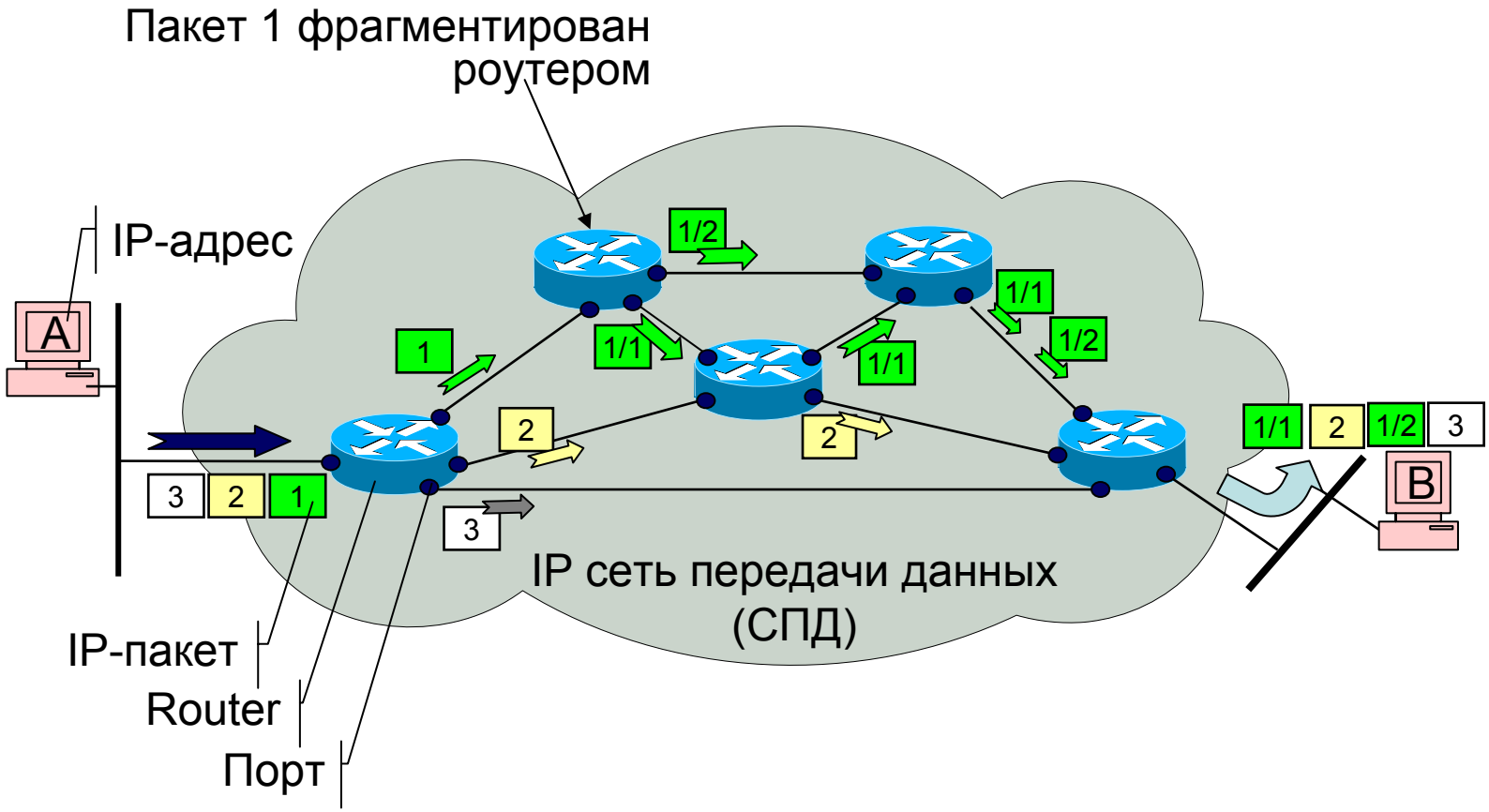


- **Fragment Offset –“смещение фрагмента”**
  - Показывает позицию фрагмента относительно начала первоначальной (оригинальной) дейтаграммы
  - Значение смещения кратно 8 байтам (64 бита)
  - Первый фрагмент и не фрагментированный пакет имеют значение “0”
  - Длина фрагмента, кроме последнего, должны быть кратны 8 байтам
  - Оригинальная дейтаграмма собирается из фрагментов с одинаковой комбинацией полей: “IP-адреса источника” / “IP-адреса приемника” / “Протокол” / “Идентификатор фрагмента”

IP – фрагментация (пример)



IP- фрагментация



IP – сборка

- **Сборка выполняется в хосте получателя**
- **Хост получателя должен:**
  - Иметь достаточное буферное пространство
  - Уметь восстанавливать последовательность фрагментов
  - Иметь механизм ограничения жизни неполной дейтаграммы:
    - ✓ Приняв первый фрагмент пакета (MF=1 и offset = 0), приемник запускает “таймер сборки”
    - ✓ Если таймер истечет раньше момента сборки оригинала, фрагменты удаляются и буфера очищаются
- **Таймер сборки ограничивает жизнь неполной дейтаграммы и позволяет эффективнее использовать буферный ресурс**

IP-опции

Формат описания опций

- **Флаг "копия"**

  1 - опция должна быть скопирована во все фрагменты дейтограммы.

  0 - опция копируется только в первый фрагмент

- **Класс опции**

  0 - Дейтограмма пользователя или сетевое управление

  1 - Зарезервировано для будущего использования

  2 - Отладка и измерения (диагностика)

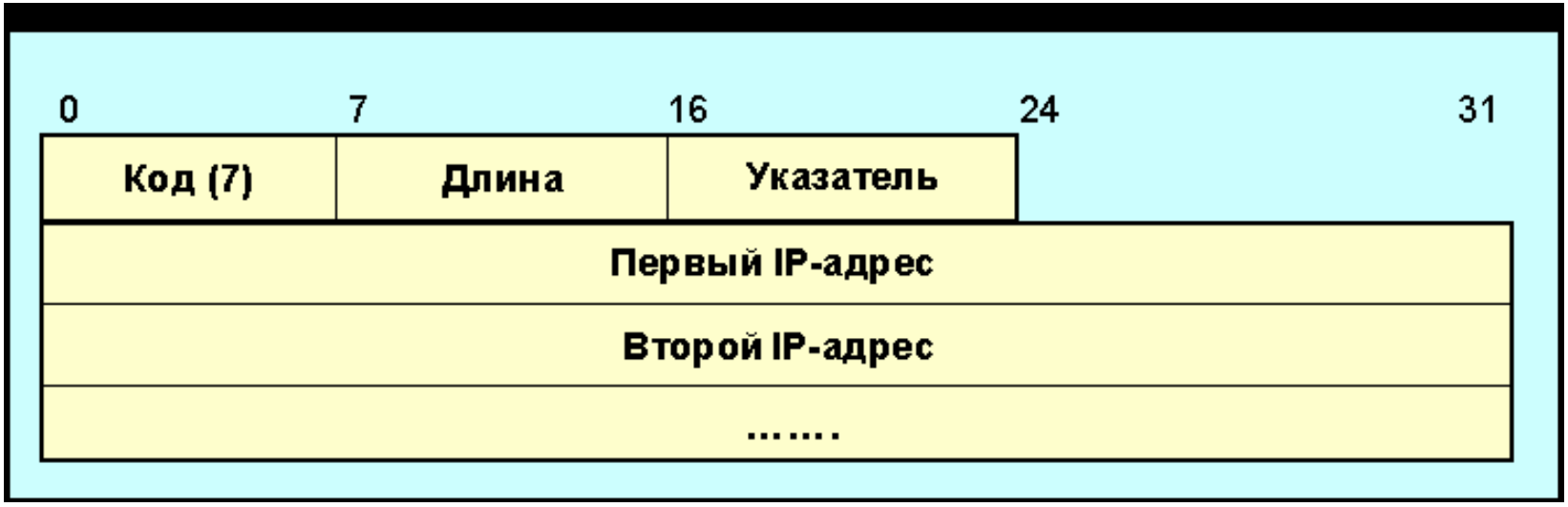
  3 - Зарезервировано для будущего использования

Номер опции

Класс опции	Номер опции	Длина описания	Назначение
0	0	-	Конец списка опций. Используется, если опции не укладываются в поле заголовка (смотри также поле "заполнитель")
0	1	-	Никаких операций (используется для выравнивания октетов в списке опций)
0	2	11	Ограничения,связанные с секретностью (для военных приложений)
0	3	*	Свободная маршрутизация. Используется для того, чтобы направить дейтограмму по заданному маршруту
0	7	*	Запись маршрута. Используется для трассировки
0	8	4	Идентификатор потока. Устарело.
0	9	*	Жесткая маршрутизация. Используется, чтобы направить дейтограмму по заданному маршруту
2	4	*	Временная метка Интернет

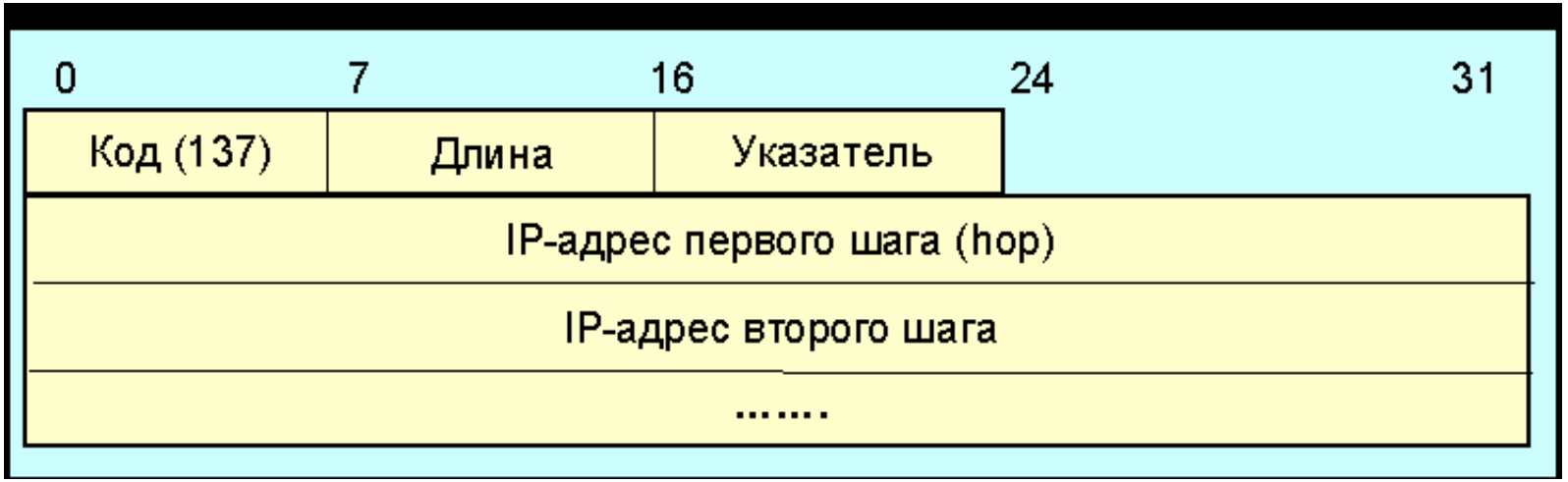
Опция ЗАПИСАТЬ МАРШРУТ

- **Длина - Длина опции, включая первые 3 байта**
- **Указатель - первая свободная позицию в списке IP-адресов, куда можно произвести запись очередного адреса)**



Опция МАРШРУТ ОТПРАВИТЕЛЯ

- **Обеспечивает возможность посылать дейтограммы по заданному отправителем маршруту.**
  - позволяет исследовать различные маршруты, в том числе те, которые недоступны через узловые маршрутизаторы.
- **Две формы такой маршрутизации:**
  - Свободная маршрутизация - возможностью прохода между двумя адресами списка более чем через одну сеть
  - Жесткая маршрутизация, означает, что адреса определяют точный маршрут дейтограммы



Опция ВРЕМЕННЫЕ МЕТКИ

- **Аналогична опции “запись маршрута”**
- **поле переполнение содержит число маршрутизаторов, которые не смогли записать временные метки из-за ограничений выделенного места в дейтограмме.**
- **поле флаги задают порядок записи временных меток маршрутизаторами:**
  - 0 - Записать только временные метки; опустить ip-адреса.
  - 1 - Записать перед каждой временной меткой ip-адрес
  - 3 - ip-адреса задаются отправителем; маршрутизатор записывает только временные метки, если очередной IP-адрес совпадает с адресом маршрутизатора
- **Временные метки - содержат время в миллисекундах, отсчитанное от начала суток**

IP-адресация

IP-адрес

- **IP-адрес**
  - 32 бита (4 байта)
    - ✓ каждый байт представляется в десятичном виде
    - ✓ байты разделяются точкой
    - ✓ Например: 152.193.44.13
  - Идентифицирует хост, порт роутера и т.д.
  - Структурирован и содержит два уровня иерархии
    - ✓ Номер сети
    - ✓ Номер хоста

Правила записи IP-адреса

Схема перевода из двоичной в десятичную систему счисления

1 байт								2 байт								3 байт								4 байт							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1

Битовое представление IP-адреса

1	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**

Десятичное представление IP-адреса

152	**193**	**44**	**13**

В результате получаем четыре десятичных числа, разделенных точкой

152.193.44.13

Классовая модель IP-адресации

Что такое - Адрес вообще?

- **Идентификатор для нахождения объекта**
  - ✓согласно некоторым правилам интерпретации
- **Обычно иерархический**
  - Каждая часть имеет более специфическую подробность
- **Например, … способ нахождения МГФ**
  - +7 342 2378376
  - www.icmm.ru/~masich
  - masich@icmm.ru
  - 195.69.156.87

- **Идентификатор Internet, информирующий о том, как достигнуть сетевой локализации**
  - через Internet маршрутизирующую систему
- **IPv4: 32 битовое число (4 байта)**
  - Байты пишутся в десятичной форме, разделяются точками
  - Например, 205.150.58.7
  - 4 миллиарда различных хост адресов (2^{32})
- **IPv6: 128 битовое число (16 байт)**
  - Пишется в Шестнадцатерично-десятичной нотации
  - Например,2001:0503:0C27:0000:0000:0000:0000:0000
  - 16 миллиардов миллиардов сетевых адресов

* bit = binary digit

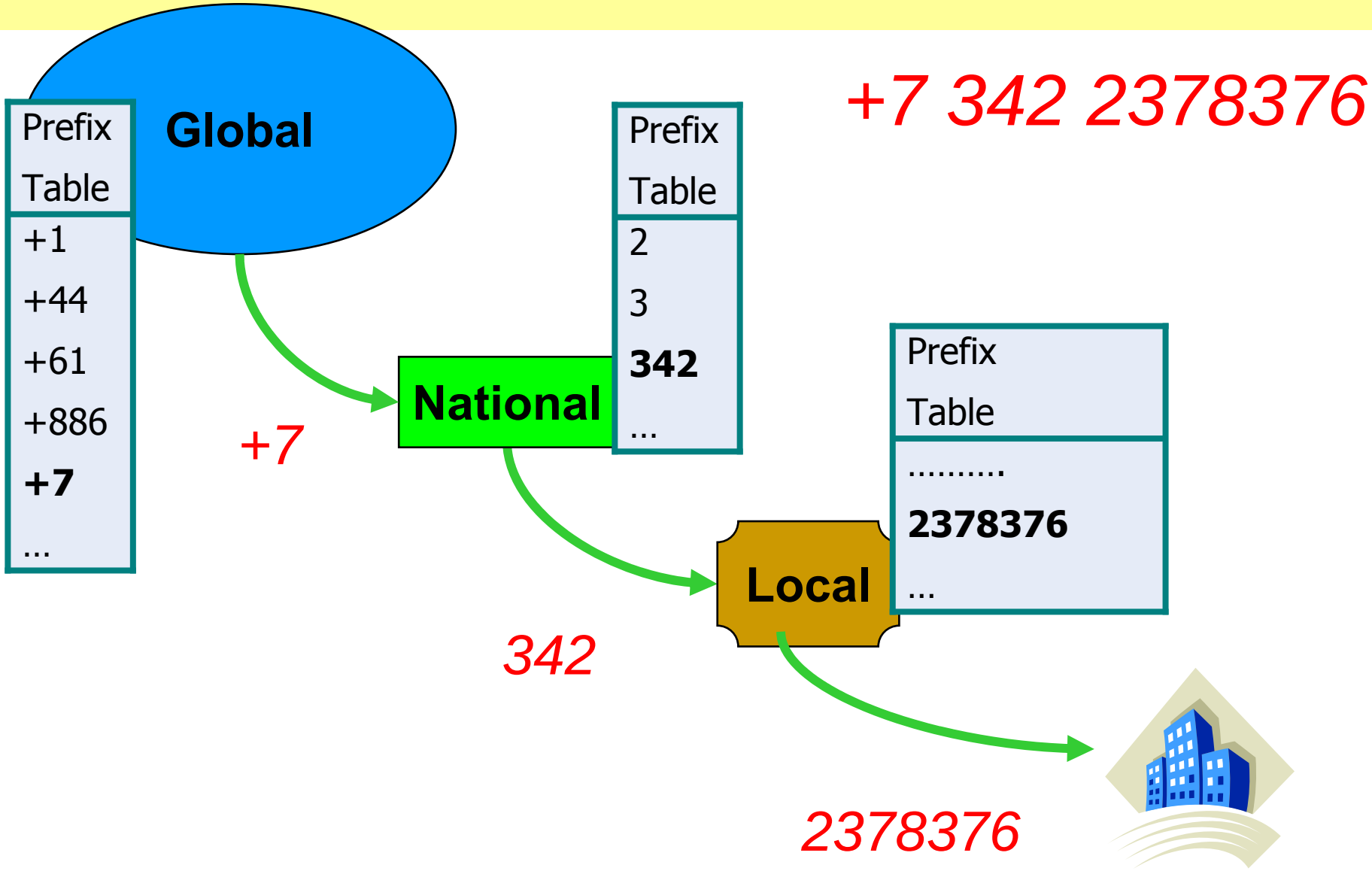
Зачем нужен IP-адрес ?

- **Необходим для Маршрутизации в Internet**
- **Конечный "Общественный Ресурс"**
- **Никогда не "находящийся в собственности" пользователя адреса**
  - не свойство
  - не может быть куплен, продан, передан …
  - предоставляется на непостоянной основе для использования
  - возвращается, когда больше не требуется
- **Не зависит от сервера домена имен (DNS)**

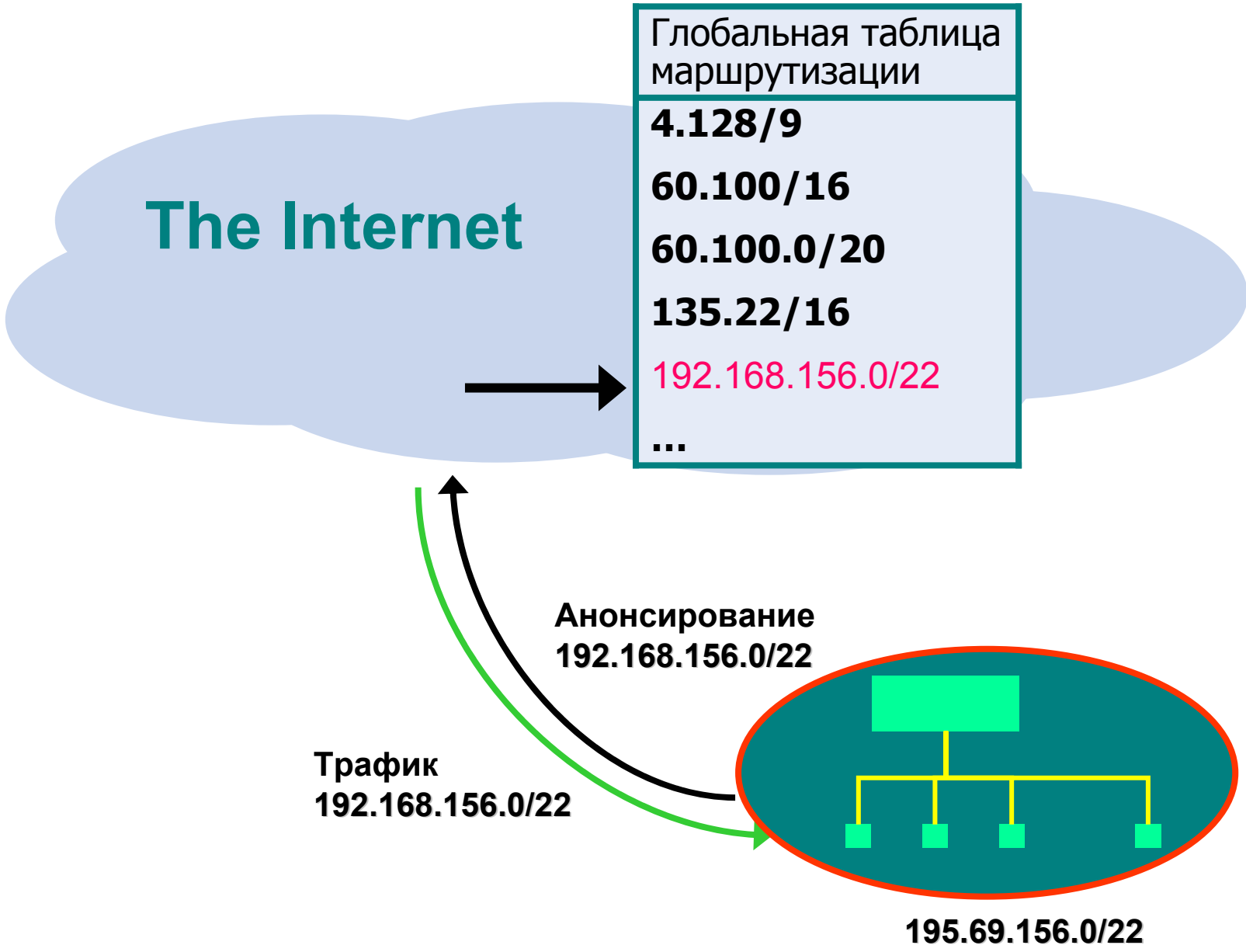
География Internet

- **"Национальные" Internet - сети**
  - «Фронтальные" – пограничные маршрутизаторы
  - "Соглашения" о пиринге устанавливают зависимости между сетями
- **Это - очень динамический мир …**
  - Новые нации формируются ежедневно
  - Новые границы устанавливаются ежечасно
  - Изменение таблиц маршрутизации каждую минуту
  - Управляемый почти полностью промышленностью
  - Не централизованное управление
- **Очень отличаются от "традиционных" сетей**
  - Телефония, например

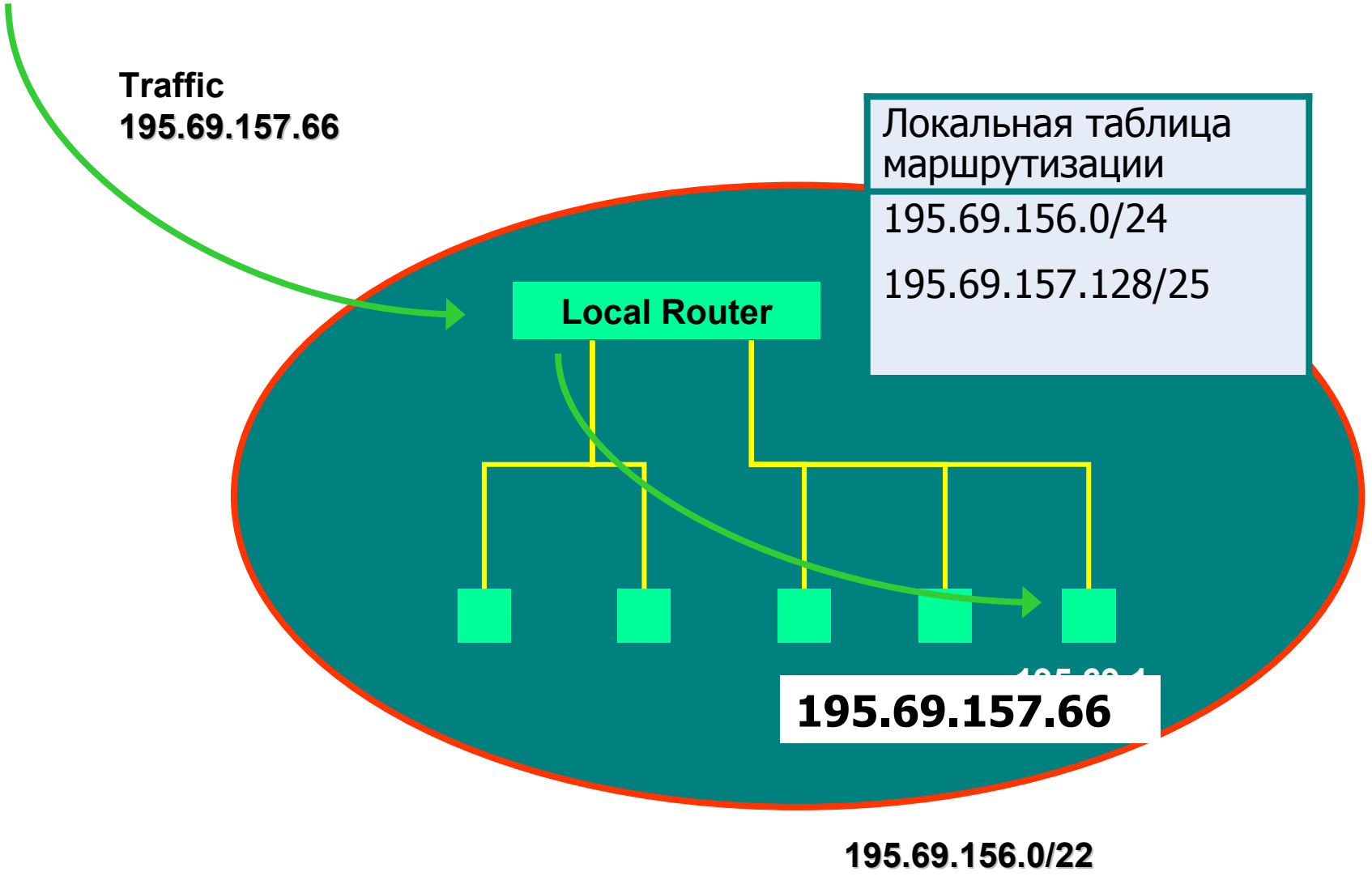
Маршрутизация в телефонных сетях



Маршрутизация в Internet



Маршрутизация в Internet



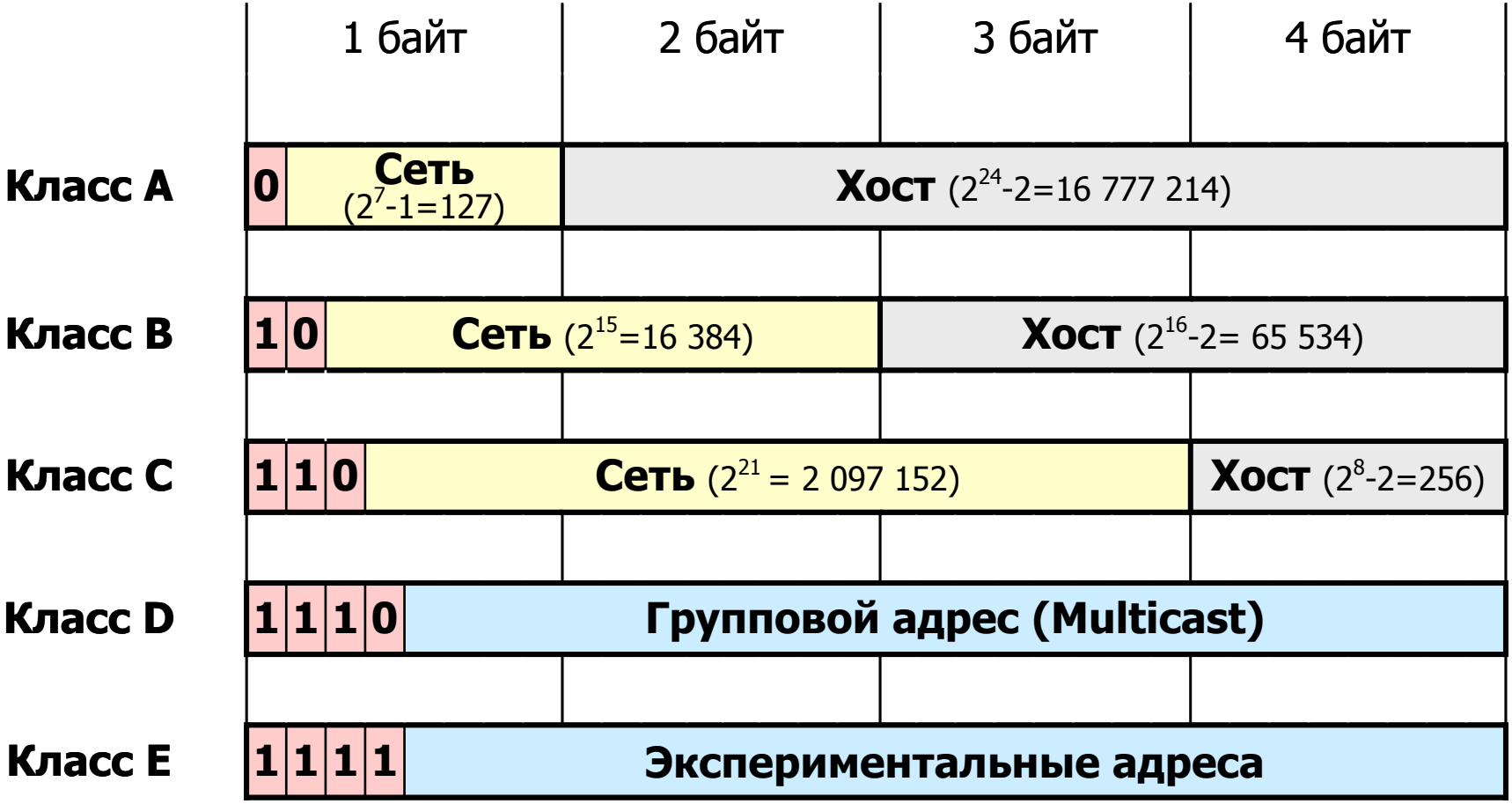
Классы IP-адресов

✓Адреса классов A , B, и C доступны для нумерации узлов /компьютеров/хостов

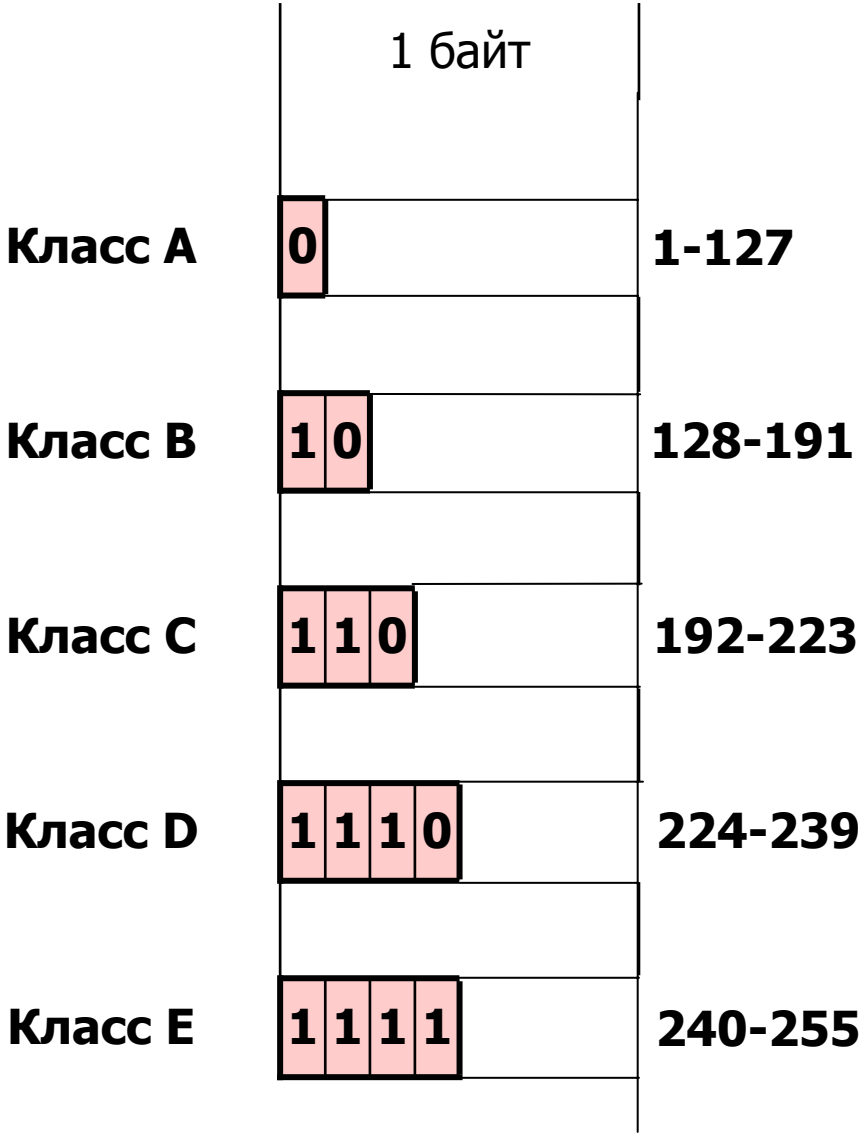
✓Некоторые адреса класса D используют протоколы маршрутизации (OSPF - 224.0.0.5, 224.0.0.6, RIPv2 - 224.0.0.9, EIGRP-224.0.0.10).

✓Другие адреса Класса D используются для видеоконференций и других приложений,

Классовая модель IP-адресации



Значение первого байта в классовой модели



IP-адрес сети/хоста, примеры

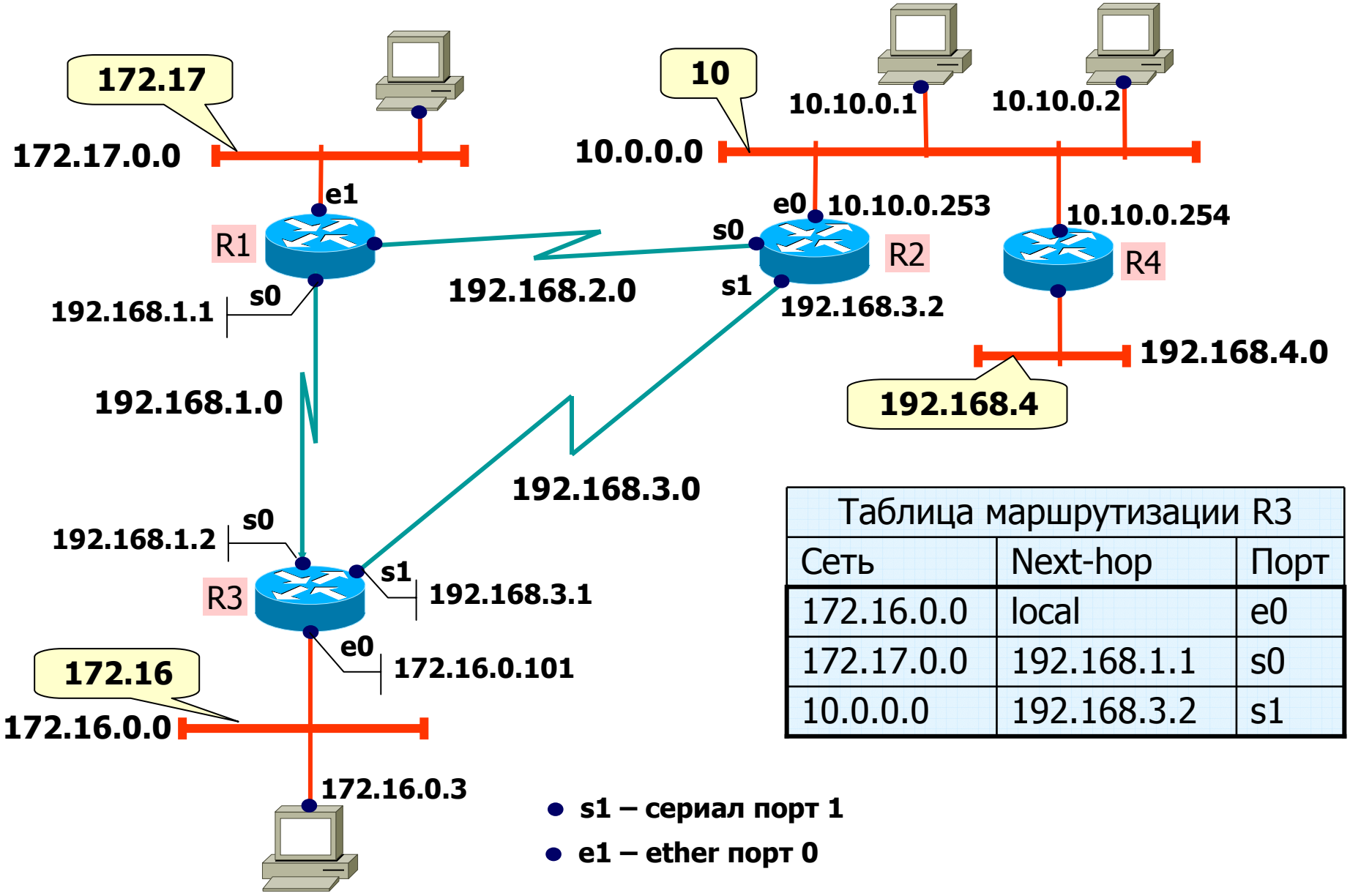


Таблица маршрутизации R3		
Сеть	Next-hop	Порт
172.16.0.0	local	e0
172.17.0.0	192.168.1.1	s0
10.0.0.0	192.168.3.2	s1

Специальные IP-адреса

- **Несколько адресов во всех классах зарезервированы для специальных целей:**

Диапазон адресов	Назначение
0.0.0.0	Неизвестная сеть, (сеть по умолчанию). Поэтому число сетей в классе А равно 2^7-1=127
10.0.0.0 – 10.255.255.255	Зарезервировано для частных сетей (RFC1918), в классе А
127.0.0.0 – 127.255.255.255	Зарезервировано для локальных адресов типа “петля”
172.16.0.0 – 172.31.255.255	Зарезервировано для частных сетей (RFC1918), в классе В
192.168.0.0 – 192.168.255.255	Зарезервировано для частных сетей (RFC1918), в классе С
255.255.255.255	Широковещательный адрес

Частный (Private) диапазон адресов

- **Три диапазона адресного пространства зарезервированы для частных сетей**
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8 prefix)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12 prefix)
  - 192.168.0.0 -192.168.255.255 (192.168.0.0/16 prefix)
    - ✓ Обратите внимание: первый блок – одна сеть класса A, второй блок – 16 подряд идущих номеров сетей класса B, третий блок – 256 подряд идущих номеров сетей класса C

- **Трансляция межу частными адресами и глобальными уникальными адресами -> NAT**

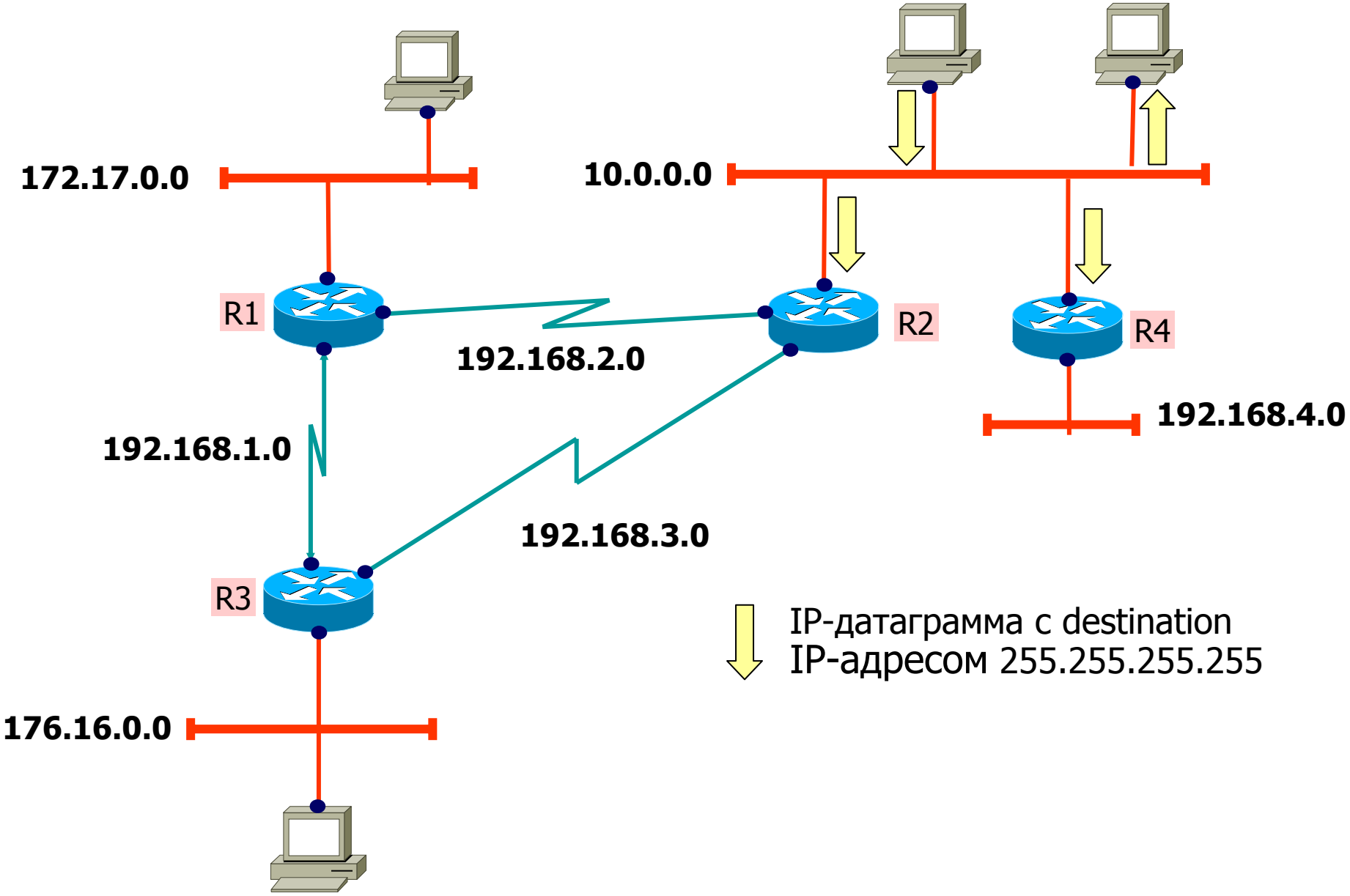
Диапазоны адресов: разъяснения

- **Основной формат IP-адреса**
  - { № сети, № хоста}
- **Пример: что означает IP-адрес 131.67.0.1 класса B ???**

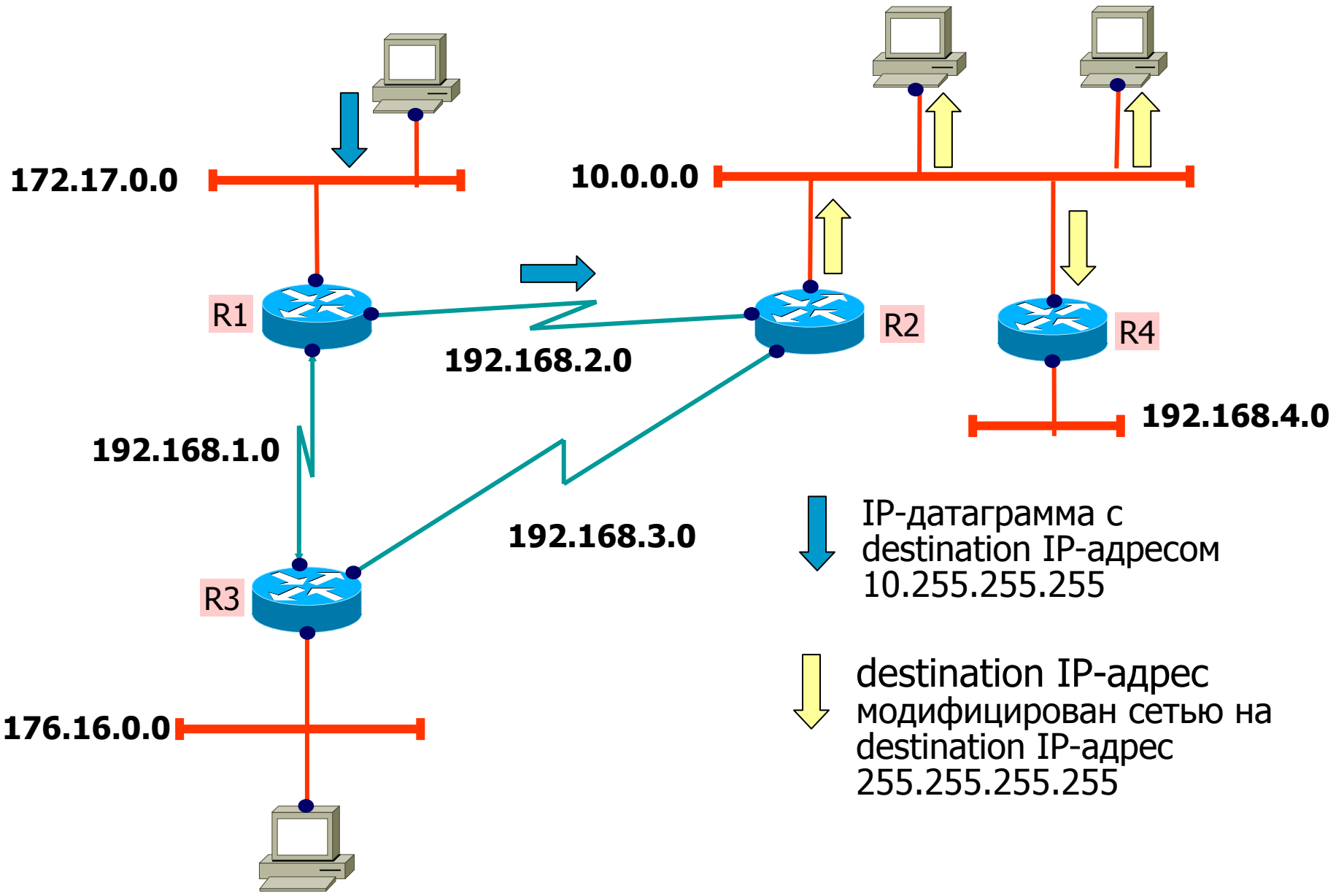
N сети	N узла	
172.16.	0.0	- IP-адрес сети (не используется для нумерации хостов)
172.16.	**0.1**	**- первый хост в этой сети (индивидуальный)**
172.16.	.....	
172.16.	255.254	- последний хост в этой сети (индивидуальный)
172.16.	255.255	- направленное широковещание для этой сети
255.255.	255.255	- ограниченное широковещание в этой сети

Поэтому максимально возможное значение числа узлов в сети уменьшено на 2

IP ограниченного широковещания (limited broadcast)



IP направленного широковещания (directed broadcast)



Бесклассовая модель IP-адресации

Исчерпание IP-адресного пространства

- **Растущий запрос IP-адресов**
  - Классовая модель напряжена
    - ✓ Класс A слишком большой (16 млн хостов)
    - ✓ Класс B истощен (к 1991 год расход приобрел угрожающие размеры) и заканчивается)
    - ✓ Класс C имеет маленький размер для большинства организаций
    - ✓ много адресов классы C, выданные некоторым организациям, ведет к (взрыву) переполнению записей таблиц маршрутизации в маршрутизаторах ядра Internet

- **Способы решения этих проблем**
  - Подсети (VLSM/CIDR)
  - Творческое (совещательное) распределение IP-адресов
  - Использование частных (private) IP-адресов и механизма преобразования сетевых адресов (NAT)
  - IPv6

Подсеть

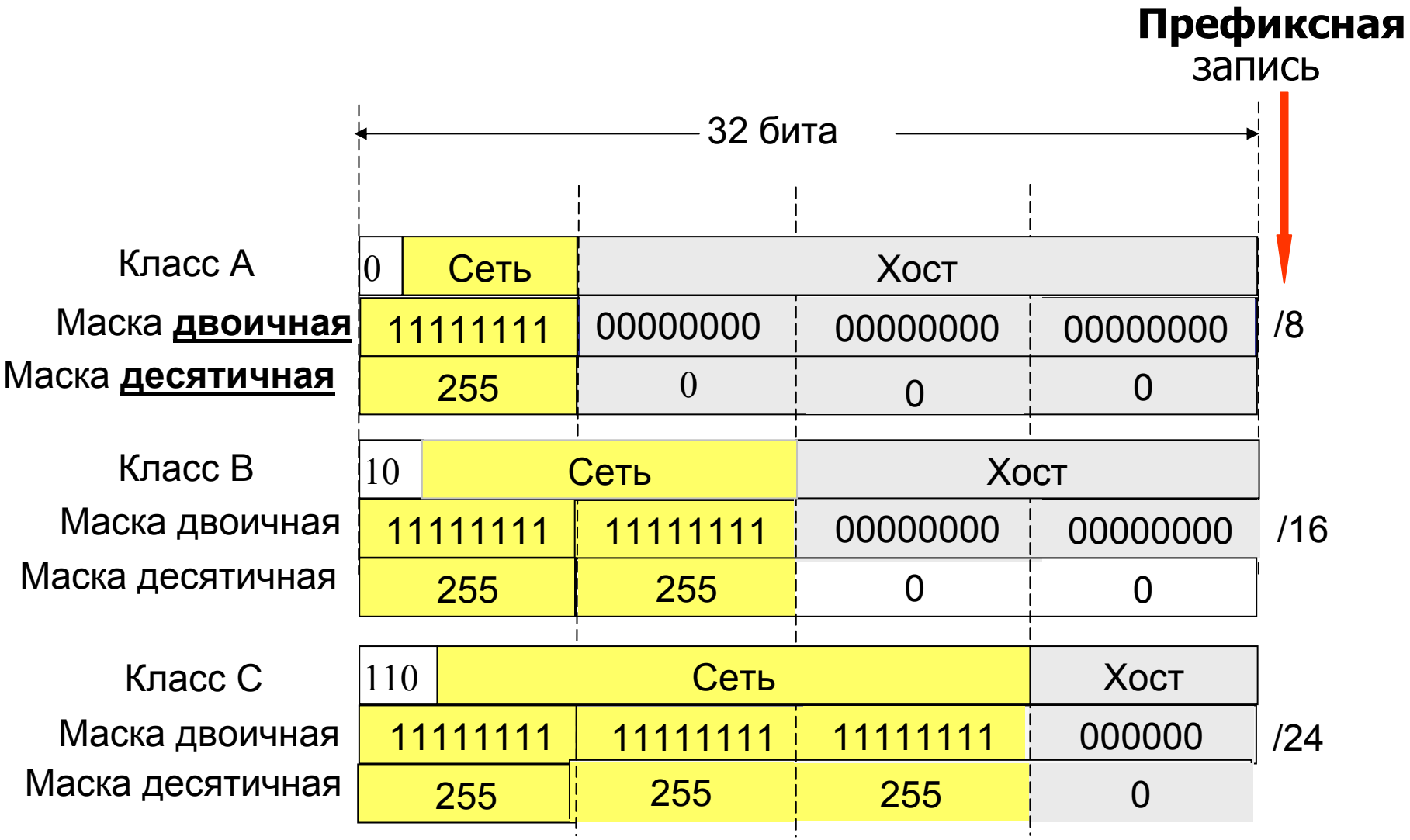
- **Двухуровневая иерархия IP- адресации была достаточна в раннем Интернет**
- **Сейчас в большинстве LAN используется три уровня иерархии, основанное на подсети**
- **Подсеть**
  - Некоторые биты нумерации хоста используются для подсети
  - Подсеть расширяет значение классового номера сети
    - ✓ Биты подсети локально интерпретируются внутри области сети
    - ✓ Биты сети все еще глобально видятся вне полученной области подсети
  - Количество бит, используемых для нумерации сети, специфицируются маской подсети, также записываемые в десятичной нотации
    - ✓ Единицы в битах маски определяют часть адреса для нумерации сети (должны быть непрерывными)
    - ✓ Нули в битах маски определяют часть адреса для нумерации хостов

Что такое «маска подсети» ?

	1 байт	2 байт	3 байт	4 байт
	Есть сеть класса B			
Класс B /16	**1 0** **Сеть**		**Хост**	
	Сформируем подсеть посредством маски подсети			
(Маска подсети)$_2$	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
(Маска подсети)$_{10}$	255	255	255	0
	Получим			
Сеть, подсеть/24	**Сеть**		**Подсеть**	**Хост**
	представлена в глобальных таблицах		используется локально	

	Пример: Разделим сеть 172.16.0.0 на подсети			
172.16.0.0/24	172	16	0	0
172.16.1.0/24	172	16	1	0
172.16.2.0/24	172	16	2	0
172.16.X.0/24	172	16	.....	
172.16.255.0/24	172	16	255	0

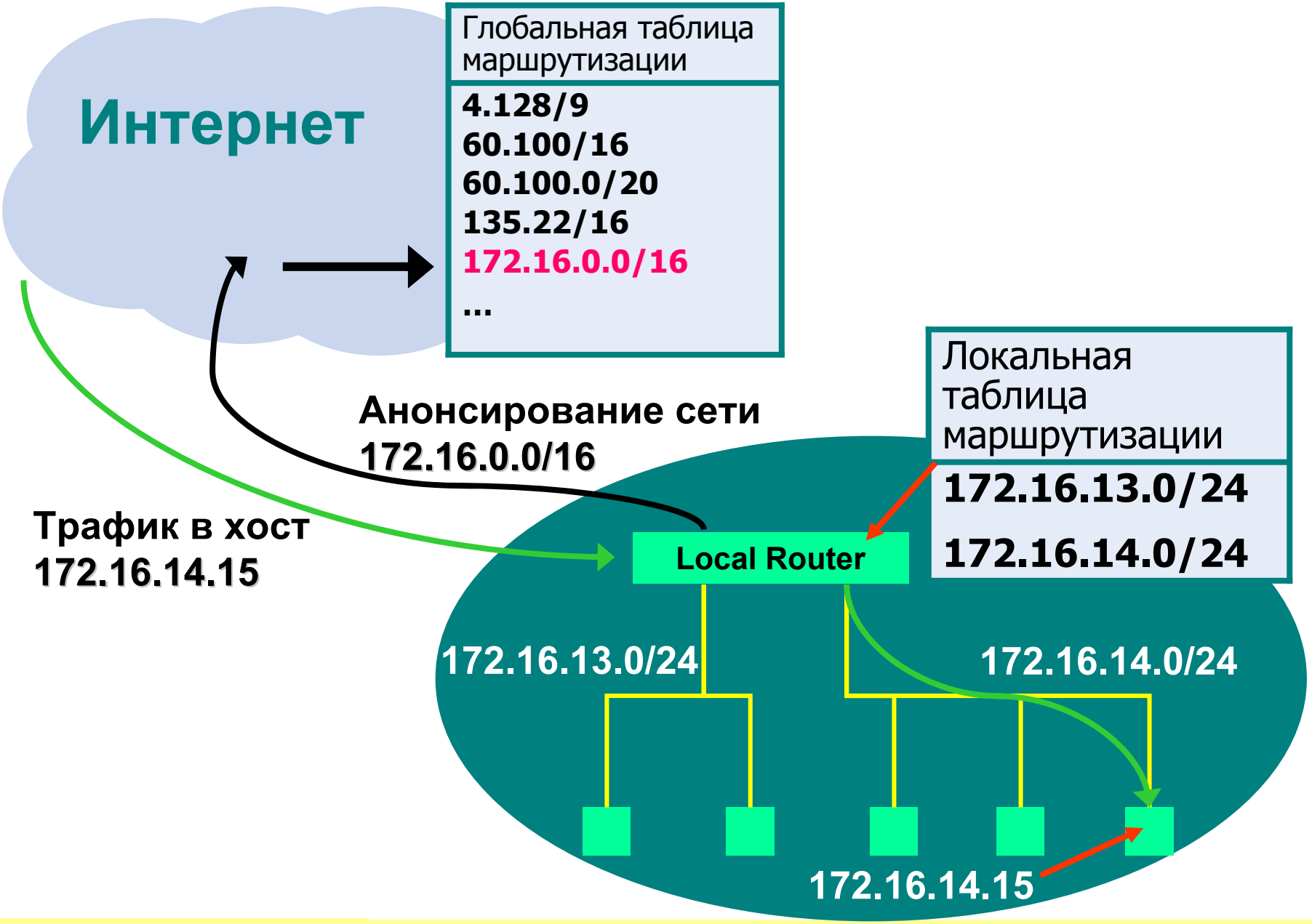
Маски классовой модели адресации



Правила записи масок

- **Маски**
  - классовых IP-сетей
    - ✓ Класс A 255.0.0.0
    - ✓ Класс B 255.255.0.0
    - ✓ Класс C 255.255.255.0
- **Старая нотация IP-адреса сети**
  - с маской
    - ✓ Класс A 10.0.0.0 255.0.0.0
    - ✓ Класс B 176.16.0.0 255.255.0.0
    - ✓ Класс C 192.12.1.0 255.255.255.0
- **Новая нотация IP-адреса сети**
  - с префикс/длина
    - ✓ Класс A 10.0.0.0/8
    - ✓ Класс B 176.16.0.0/16
    - ✓ Класс C 192.12.1.0/24

Маршрутизация в Интернет



Правила адресации подсети

- **Формат IP-адреса с подсетью**
  - «сеть, подсеть, хост»
- **Добавлена специальная цель обращения и правила**
  - «сеть, подсеть, 255»
    - ✓ Направленное широковещание в специфицированную подсеть
  - «сеть, 255, 255»
    - ✓ Направленное широковещание во все подсети сети
  - «сеть, 0, хост»
    - ✓ Нули в подсети никогда не используются для нумерации подсети в классовой модели маршрутизации (RFC 950)
  - «сеть, 255, хост»
    - ✓ Единицы в подсети (широковещание в подсеть) никогда не используются для нумерации подсети в классовой модели маршрутизации (RFC 950)

Подсеть с маской. Пример 1

- **Класс А → разделим на псевдо сети класса В**
  - 10.0.0.0 с маской 255.255.0.0 (10.0.0.0/16)
  - Подсети
    - ✓ 10.0.0.0 нулевая подсеть (не используется для нумерации)
    - ✓ 10.1.0.0 первая подсеть
      - ➢ 10.1.0.0 адрес подсети
      - ➢ 10.1.0.1 первый хост в подсети 10.1.0.0
      - ➢ 10.1.255.254 последний хост в подсети 10.1.0.0
      - ➢ 10.1.255.255 направленное широковещание в подсеть 10.1.0.0
    - ✓ 10.2.0.0 вторая подсеть
    - ✓ 10.3.0.0 третья подсеть
    - ✓ .....
    - ✓ 10.254.0.0 последняя подсеть
    - ✓ 10.255.0.0 направленное широковещание в подсети (не используется для нумерации подсети)
  - 254 подсети / 65534 хоста

Нули в подсети / широковещание (все единицы) в подсети

- **записи 10.0.0.0 для идентификации сети мало**
  - Это сеть 10

  или
  - подсеть 10.0
- **записи 10.255.255.255 недостаточно для направленного широковещания**
  - для сети 10

  или
  - подсети 10.255
- **subnet zero и subnet broadcast двусмысленны**

Примеры IP адресации посредством подсетей

Сеть 10.0.0.0 (класс A) с маской подсети 255.255.0.0

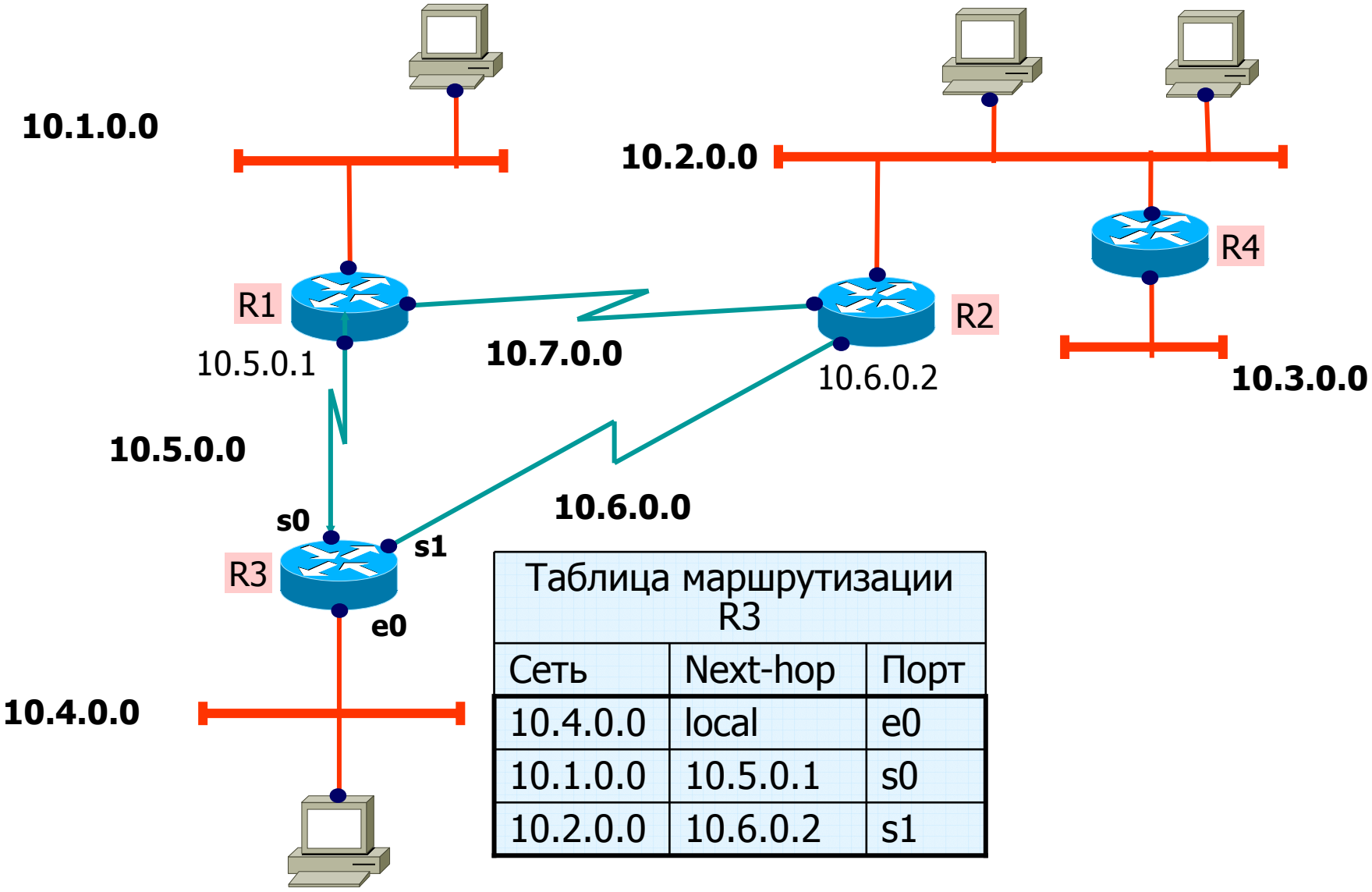


Таблица маршрутизации R3		
Сеть	Next-hop	Порт
10.4.0.0	local	e0
10.1.0.0	10.5.0.1	s0
10.2.0.0	10.6.0.2	s1

Классовая маршрутизация

Сеть 10.0.0.0 (класс A) с маской подсети 255.255.0.0

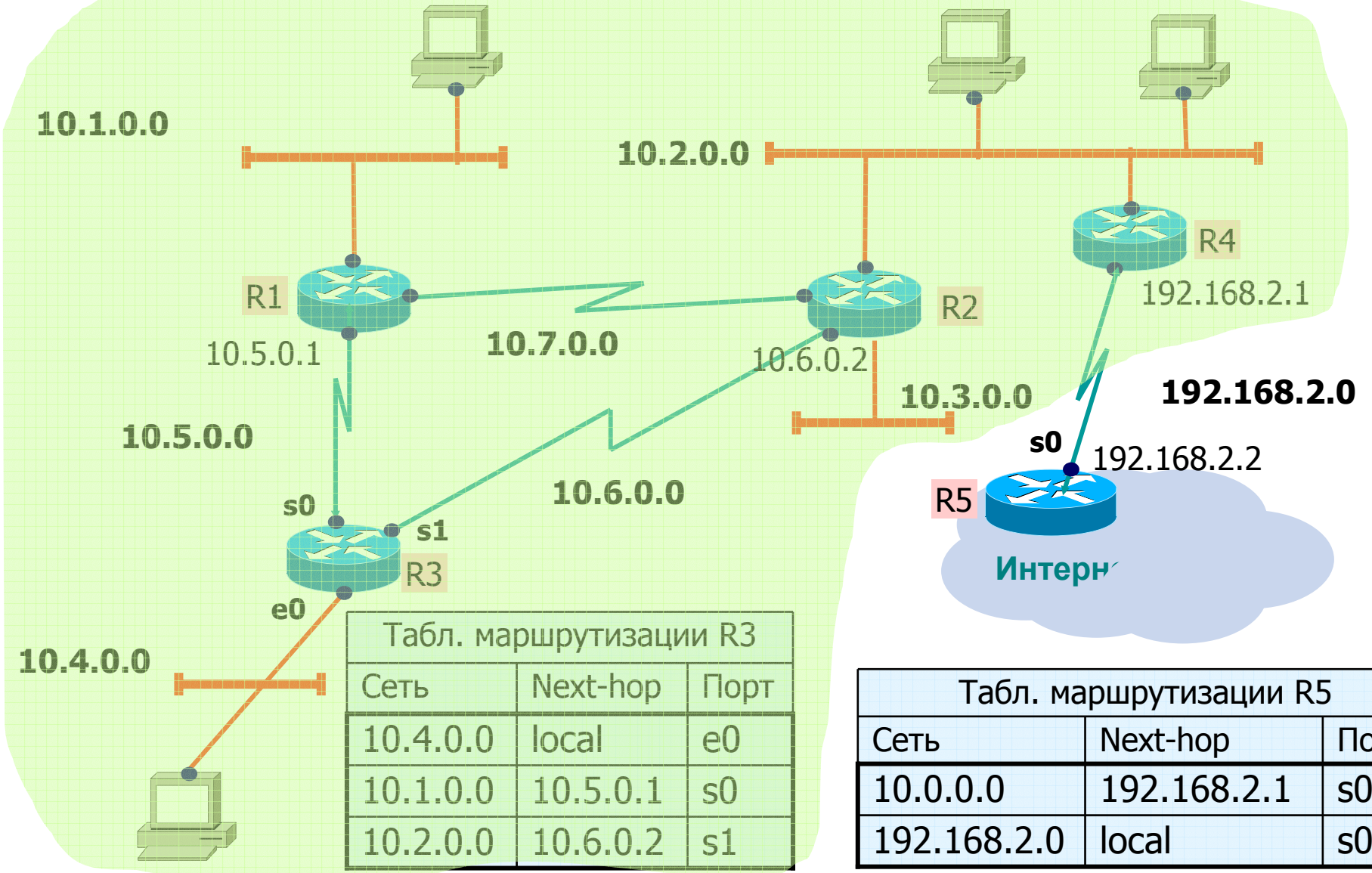


Табл. маршрутизации R3		
Сеть	Next-hop	Порт
10.4.0.0	local	e0
10.1.0.0	10.5.0.1	s0
10.2.0.0	10.6.0.2	s1

Табл. маршрутизации R5		
Сеть	Next-hop	Порт
10.0.0.0	192.168.2.1	s0
192.168.2.0	local	s0

Бесклассовая модель IP-адресации

VLSM

CIDR (Classless InterDomain Routing)

Принципы VLSM-маскирования

- **VLSM-маскирование обеспечивает**
  - возможность создания более одной маски подсети в пределах одной главной сети
  - возможность разбивать на подсети уже разбитые на подсети IP-адреса.
- **Преимущества VLSM-маскирования**
  - Более эффективное использование адресного пространства
    - ✓ Без VLSM-маскирования для всего адресного пространства сетей класса A, B или C можно применять только одну маску подсети
  - Возможность суммирования маршрутов.
    - ✓ Возможно большое количество иерархических уровней в рамках одного плана адресации
    - ✓ Это позволяет производить оптимальное суммирование в таблицах маршрутизации

Пример маски подсети не на границе байта

	1 байт								2 байт								3 байт								4 байт							
Вес разряда →	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Сеть класса B																																
140.97.0.0/16	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Разобьем маской 255.255.192.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
Подсети	**Сеть**																**Подсеть**								**Хост**							
140.97.0.0/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
140.97.0.64/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
140.97.0.128/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
140.97.0.192/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
140.97.1.0/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
140.97.1.64/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0
…																																
140.97.255.128/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
140.97.255.192/26	1	0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

Определение, к какой подсети относится адрес

- **Пусть имеем конкретный IP-адрес (класса B)**
  - IP-адрес 140.97.113.205
  - Маска подсети 255.255.192.0
  - Какая сеть?, какой хост в сети?

двоичный IP-адрес 10001100 . 01100001 . 01110001 . 11001101

Двоичная маска 11111111 . 11111111 . 11111111 . 11000000

Выполняем логическую операцию “И”

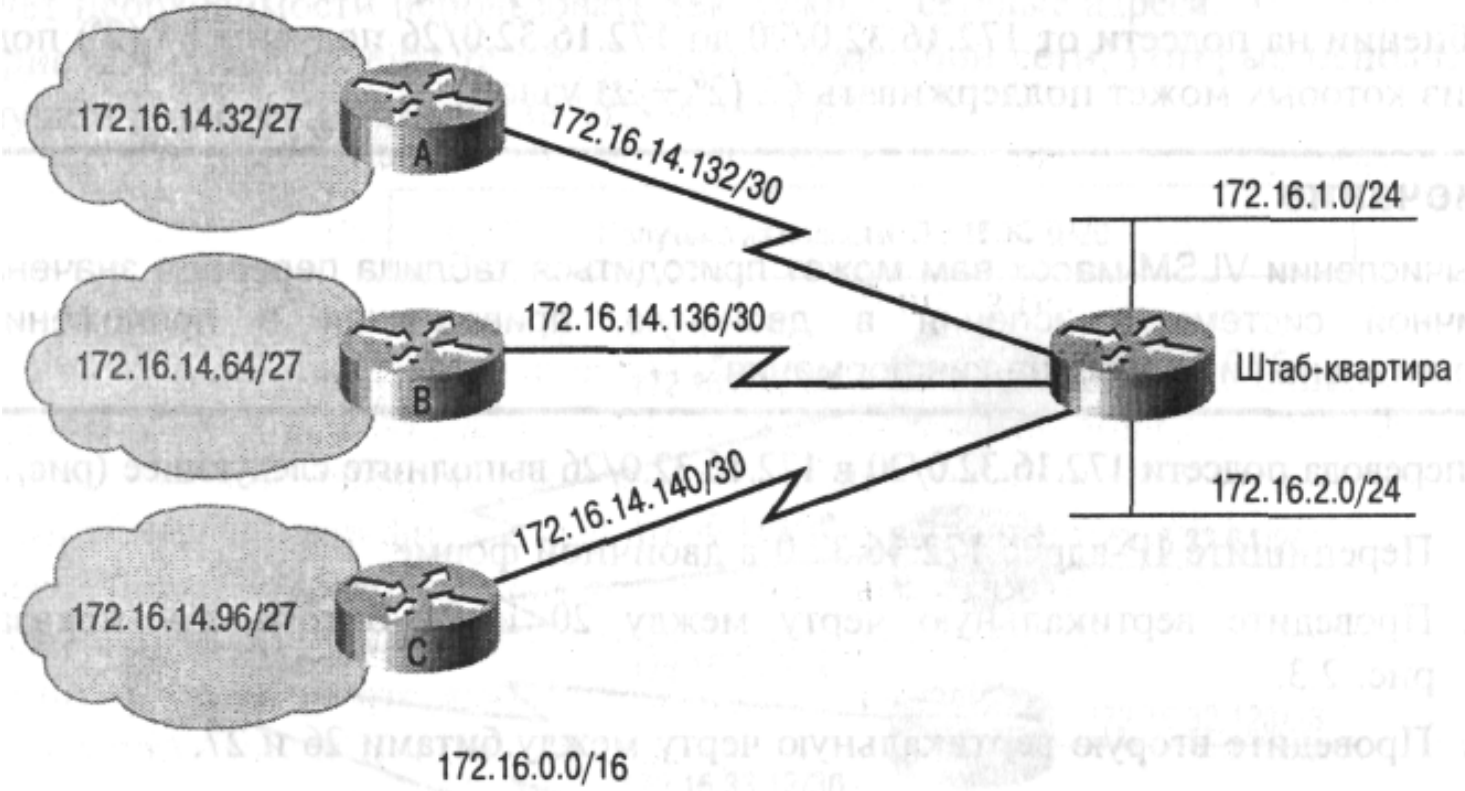
Сеть 10001100 . 01100001 . 01110001 . 11000000

Получаем в десятичном виде:

Сеть = 140.97.113.192

Хост = 0.0.0.13 (эту запись обычно не приводят)

Например, IP-адрес 172.16.14.0/24 может суммировать все подсети, входящие в подсеть 172.16.14.0, включая такие подсети более глубокого уровня вложения, как 172.16.14.0/27 и 172.16.14.128/30.



Лабы делать так

IP-маршрутизация

Прямая и косвенная маршрутизация

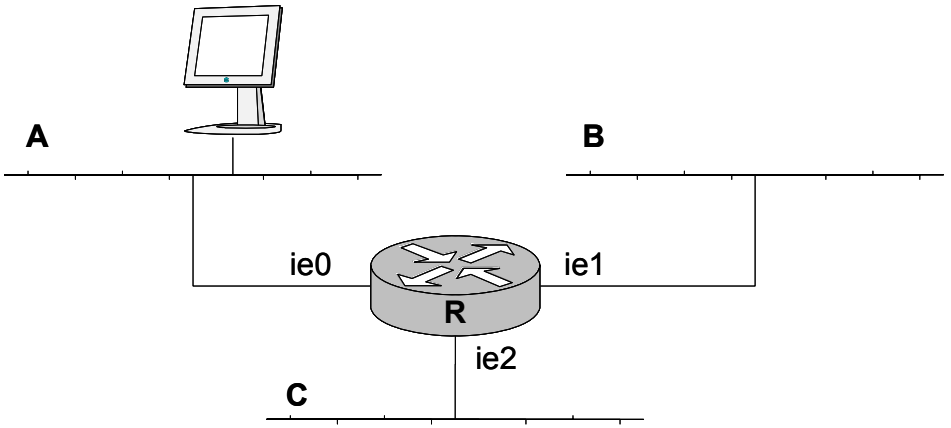


Таблица маршрутов для компутеров в сети A

имя сети (сеть/маска)	флаг вида маршр-ии	шлюз	номер адаптера	метрика
a	прямо	-	1	0
b	косвенно	IP R(ie0)	1	1
c	косвенно	IP R(ie0)	1	1

Таблица маршрутов роутера R				
a	прямо	-	ie0	0
b	прямо	-	ie1	0
c	прямо	-	ie2	0

- **Порядок прямой маршрутизации**
  - Имя преобразуется в IP адрес (посредством DNS);
  - IP модуль (посредством маски) выделяет сеть и ищет соответствие с сетью в таблице маршрутов;
  - В случае прямой маршрутизации стоит флаг прямо и посредством ARP таблицы ставится в соответствие IP адресу MAC адрес;
  - Формируется кадр и передается через указанный в таблице маршрутизации interface.
- **Порядок косвенной маршрутизации**
  - Имя преобразуется в IP адрес (посредством DNS);
  - IP модуль (посредством маски) выделяет сеть и ищет соответствие с сетью в таблице маршрутов;
  - Выделяем IP адрес шлюза;
  - По ARP таблице определяем MAC адрес шлюза;
  - Формируется кадр и передается через указанный в таблице маршрутизации interface.

Установка маршрутов в Unix хосте

- **ifconfig**
  - включение и выключение сетевого интерфейса, обмена по протоколу ARP, режима отладки, задание маски, задание метода маршрутизации

ifconfig ie0 128.6.4.4 netmask 255.255.255.0

ifconfig ie1 128.6.5.35 netmask 255.255.255.0

- **route**
  - выводит и удаляет маршруты в таблице маршрутизации

route add 128.6.2.0 128.6.4.1 1

route add 128.6.6.0 128.6.5.35 1

route add default 128.6.4.27 1

Установка маршрутов в Unix хосте

- ifconfig ie0 128.6.4.4 netmask 255.255.255.0
- ifconfig ie1 128.6.5.35 netmask 255.255.255.0
- route add 128.6.2.0 128.6.4.1 1
- route add 128.6.6.0 128.6.5.35 1
- route add default 128.6.4.27 1

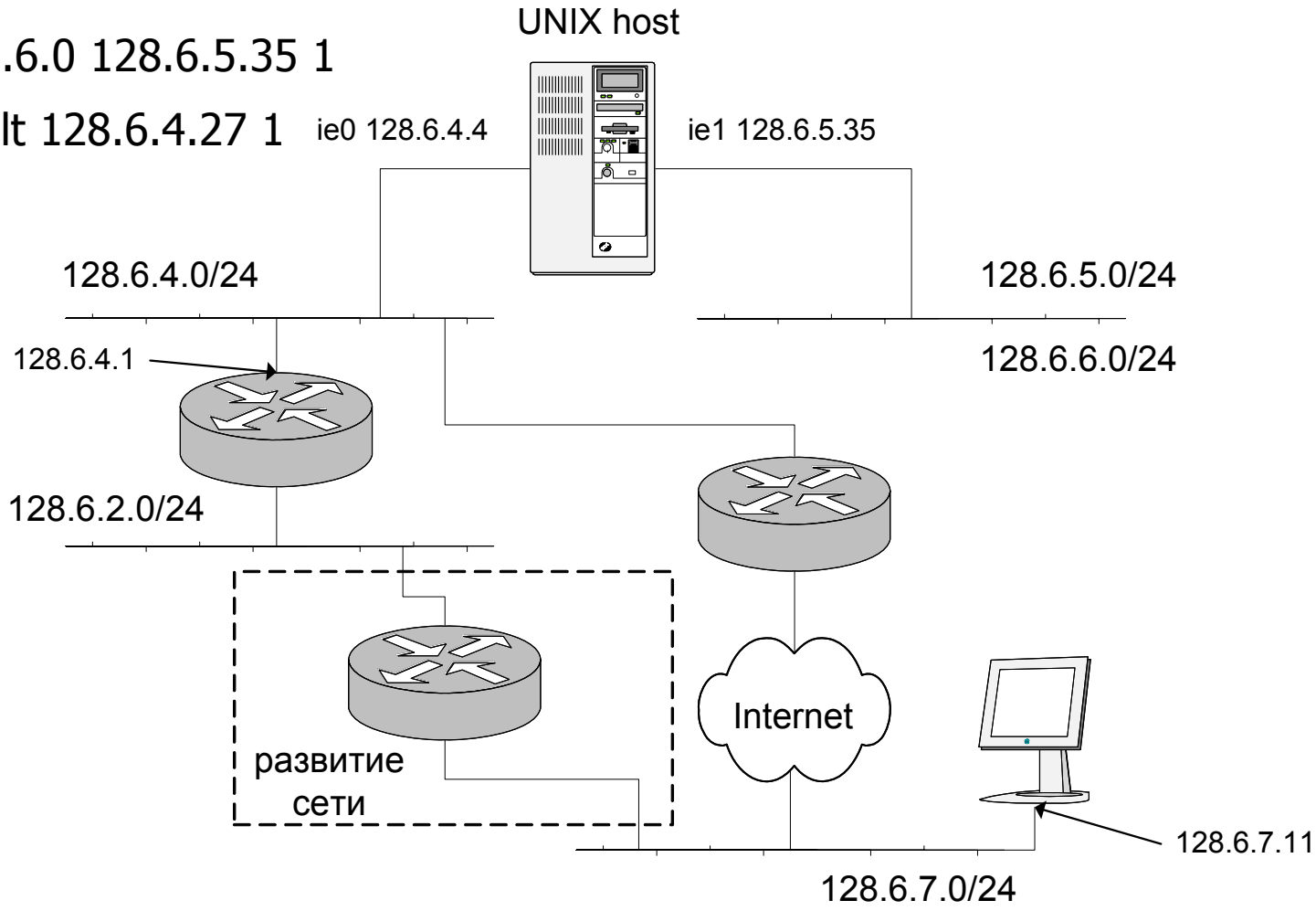


Таблица маршрутизации (UNIX host)

Destination	Flag	Gateway	Interface	Metric
128.6.4.0/24	прямая	-	ie0	0
128.6.5.0/24	прямая	-	ie1	0
128.6.2.0/24	косвенная	128.6.4.1	ie0	1
128.6.6.0/24	прямая	-	ie1	0
default	косвенная	128.6.4.27	ie0	-

Destination	Flag	Gateway	Interface	Metric
128.6.7.0/24	косвенная	128.6.4.1	ie0	2

- Данная строчка добавится, когда придет ICMP сообщение о перенаправлении (для 128.6.7.11 есть лучший маршрут через 128.6.4.1)
- Сообщения о переадресации (перенаправлении) не могут использовать сами шлюзы

Если в IP сети несколько путей достижение адресата, а в таблице маршрутов одна запись, то шлюзы выполняют перенаправление пакетов, для которых есть более выгодные маршруты.

ARP протокол

- **Протокол ARP (address resolution protocol - протокол разрешения адресов, RFC-826) – находит по сетевому адресу (L3) канальный адрес (L2)**
- **В нашем случае находит по IP-адресу соответствующий MAC-адрес**
- **Порядок преобразования**

1. Требуется отправить пакет по известному IP-адресу, MAC-адрес которого неизвестен. Исходящий пакет ставится в очередь.
2. Всем машинам в сети посылается широковещательный Ethernet кадр с ARP-запросом по искомому IP-адресу (MAC-адрес назначения все единицы)
3. Каждая машина, принявшая ARP-запрос, в своем ARP-модуле сравнивает собственный IP-адрес с IP-адресом в запросе. Если IP-адрес совпал, то по Ethernet-адресу отправителя запроса посылается ответ, содержащий как IP-адрес ответившей машины, так и ее Ethernet-адрес
4. После получения ответа на свой ARP-запрос машина имеет требуемую информацию о соответствии IP и Ethernet-адресов, формирует соответствующий элемент ARP-таблицы и отправляет IP-пакет, ранее поставленный в очередь
5. Если же в сети нет машины с искомым IP-адресом, то ARP-ответа не будет и не будет записи в ARP-таблицу. Протокол IP будет уничтожать IP-пакеты, предназначенные для отправки по этому адресу

ARP кадр

- HA-Len - длина аппаратного адреса;
- PA-Len – длина протокольного адреса (длина в байтах, например, для IP-адреса PA-Len=4).
- Тип оборудования - это тип интерфейса, для которого отправитель ищет адрес; код содержит 1 для Ethernet

ARP кадр

- **Тип оборудования**

Код типа оборудования	Описание
1	Ethernet (10 Мбит/с)
2	Экспериментальный Ethernet (3 Мбит/с)
3	Радиолюбительская связь через X.25
4	Proteon ProNET маркерная кольцевая сеть (Token Ring)
5	Chaos
6	Сети IEEE 802
7	ARCNET

ARP: Тип протокола

Код типа протокола		Описание
Десятичное значение	Hex	
512	0200	XEROX PUP
513	0201	PUP трансляция адреса
1536	0600	XEROX NS IDP
2048	0800	**DOD Internet протокол (IP)**
2049	0801	X.75 Internet
2050	0802	NBS Internet
2051	0803	ECMA Internet
2052	0804	Chaosnet
2053	0805	**X.25 уровень 3**
2054	0806	**Протокол трансляции адреса (ARP)**
2055	0807	XNS совместимость
2560	0A00	Xerox IEEE-802.3 PUP
4096	1000	Bercley Trailer
21000	5208	BBN Simnet
24577	6001	DEC MOP Dump/Load
24578	6002	DEC MOP удаленный терминал
24579	6003	DEC DECnet фаза IV
24580	6004	DEC LAT
24582	6005	DEC
24583	6006	DEC
32773	8005	HP Probe
32784	8010	Excelan
32821	8035	**Реверсивный протокол ARP (RARP)**
32824	8038	DEC LANbridge
32923	8098	Appletalk
33100	814C	SNMP

ARP код операции

- **Поле код операции определяет**
  - 1 - ARP-запрос
  - 2 - ARP-отклик
  - 3 - RARP-запрос
  - 4 - RARP-отклик
  - 5 - запрос Dynamic RARP.
  - 6 - отклик Dynamic RARP.
  - 7 - ошибка Dynamic RARP.
  - 8 - запрос InARP.
  - 9 - отклик InARP..
- **Это поле необходимо, как поле тип кадра в Ethernet идентичны для ARP-запроса и отклика.**

ARP таблица

- **ARP-таблицы строятся согласно документу RFC-1213**
- **Для каждого IP-адреса содержит четыре кода:**

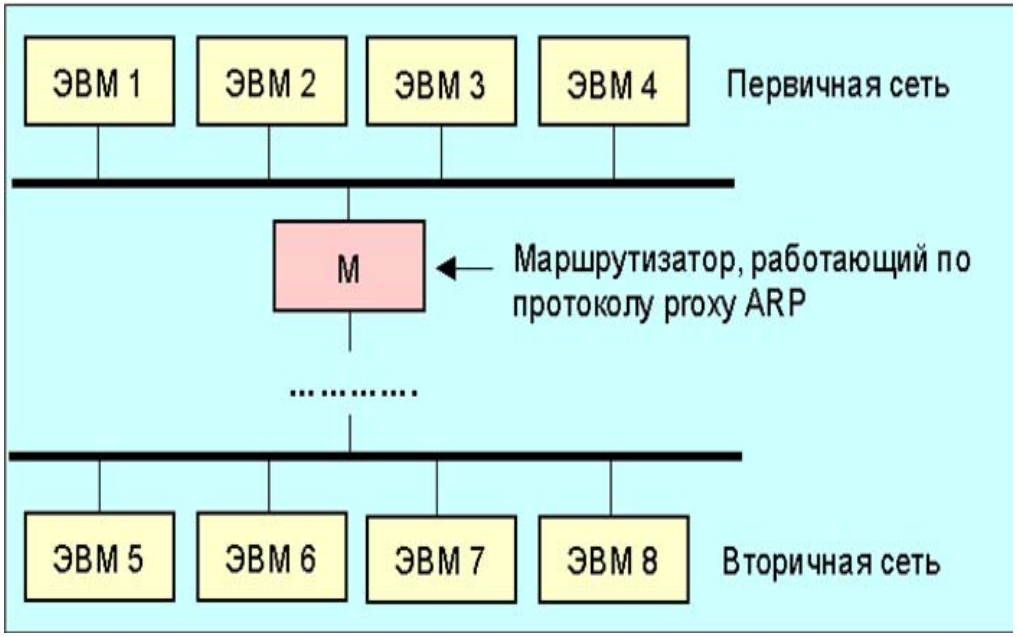
ifindex	Физический порт (интерфейс), соответствующий данному адресу;
Физический адрес	MAC-адрес, например Ethernet-адрес;
IP-адрес	IP-адрес, соответствующий физическому адресу;
тип адресного соответствия	это поле может принимать 4 значения: 1 - вариант не стандартный и не подходит ни к одному из описанных ниже типов; 2 - данная запись уже не соответствует действительности; 3 - постоянная привязка; 4 - динамическая привязка;

Proxy-ARP

Чтобы один и тот же сетевой IP-префикс адреса можно было использовать для двух сетей.

Надо соединить сети через маршрутизатор М, работающий в соответствии со смешанным протоколом ARP (функционально это IP-мост). Маршрутизатор знает, какая из машин принадлежит какой физической сети. Он перехватывает широковещательные ARP-запросы из сети 1, относящиеся к сети 2, и наоборот. Во всех случаях в качестве физического адреса маршрутизатор возвращает свой адрес. В дальнейшем, получая дейтограммы, он маршрутизирует их на физические адреса по их IP-адресам

Вывод: нескольким IP-адресам ставится в соответствие один и тот же физический адрес



Системы, где предусмотрен контроль за соответствием физических и IP-адресов, не могут работать со смешанным протоколом ARP

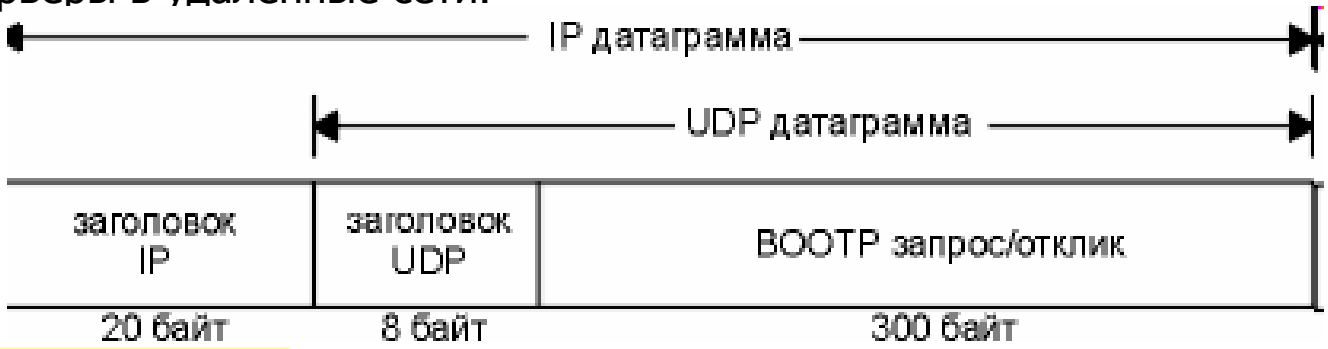
Главным преимуществом этого протокола является то, что он позволяет путем добавления одного маршрутизатора (Gateway) подключить к Интернет еще одну сеть, не изменяя таблиц маршрутизации в других узлах. Этот протокол удобен для сети, где есть ЭВМ, не способная работать с субсетями

Протокол RARP

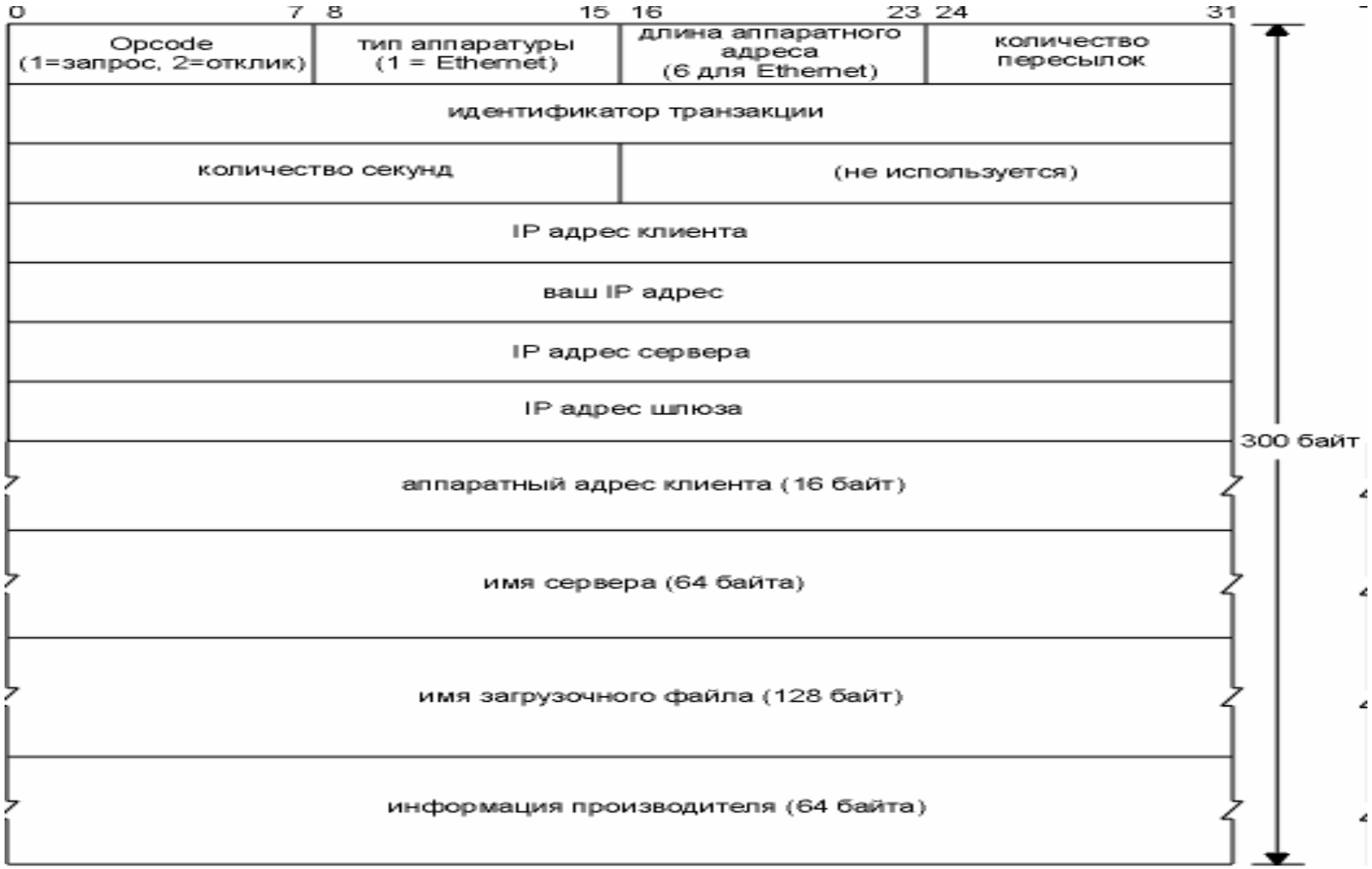
- **Обычно IP-адреса хранятся на диске, откуда они считываются при загрузке системы**
- **Проблема: а если бездисковый хост**
  - который использует TFTP для переноса из сервера в память образа операционной системы,
  - а это нельзя сделать, не зная IP-адресов сервера и хоста.
  - Записывать эти адреса в ПЗУ не представляется целесообразным, так как их значения зависят от точки подключения хоста и могут меняться
- **Решение проблемы: использование протокола обратной трансляции адресов (RARP – Reverse Address Resolution Protocol, RFC-0903) или использование протокола BOOTP.**
  - Форматы сообщений RARP сходны с ARP, хотя сами протоколы принципиально различны
- **Протокол RARP**
  - предполагает наличие специального сервера, обслуживающего широковещательные RARP-запросы и хранящего базу данных о соответствии аппаратных адресов протокольным
  - Два кода операций:
    - ✓ Код операции = 3 для RARP-запросов
    - ✓ Код операции = 4 для RARP-откликов
- **RARP проблемы: RARP сервер должен находиться в каждом широковещательном дмене**

Протокол BOOTP

- **BOOTP - Bootstrap Protocol**
  - RFC 951 [Croft and Gilmore 1985], пояснения даются в RFC 1542 [Wimer 1993]
  - альтернативы RARP для загрузки бездисковых систем, которым необходимо определить свой IP адрес
- **Использует UDP и обычно совместно с TFTP**
  - Для BOOTP выделено два заранее известных порта: 67 для сервера и 68 для клиента
- **BOOTP также может вернуть дополнительную информацию**
  - IP адрес маршрутизатора, маску подсети клиента и IP адрес DNS сервера.
- **Бездисковые системы должны иметь следующие протоколы в своей постоянной памяти: BOOTP, TFTP, UDP, IP и драйвер устройства для локальной сети.**
  - Маршрутизаторы могут также выступать в роли уполномоченных агентов для реальных BOOTP серверов, перенаправляя запросы клиентов на реальные серверы в удаленные сети.



Протокол BOOTP



где,
Opcode – код операции

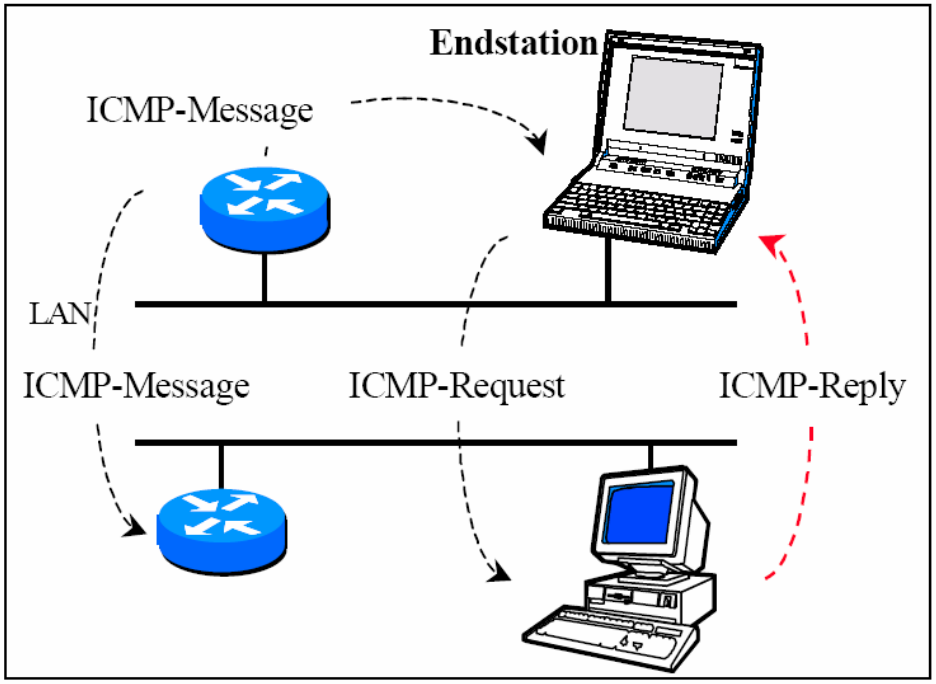
Протокол ICMP

ICMP

- **Протокол передачи команд и сообщений об ошибках (ICMP - internet control message protocol, RFC-792, - 1256) выполняет многие и не только диагностические функции**
- **ICMP-протокол сообщает об ошибках в IP-дейтограммах, но не дает информации об ошибках в самих ICMP-сообщениях.**
- **ICMP использует IP, а IP-протокол должен использовать ICMP. В случае ICMP-фрагментации сообщение об ошибке будет выдано только один раз на дейтограмму, даже если ошибки были в нескольких фрагментах**

ICMP

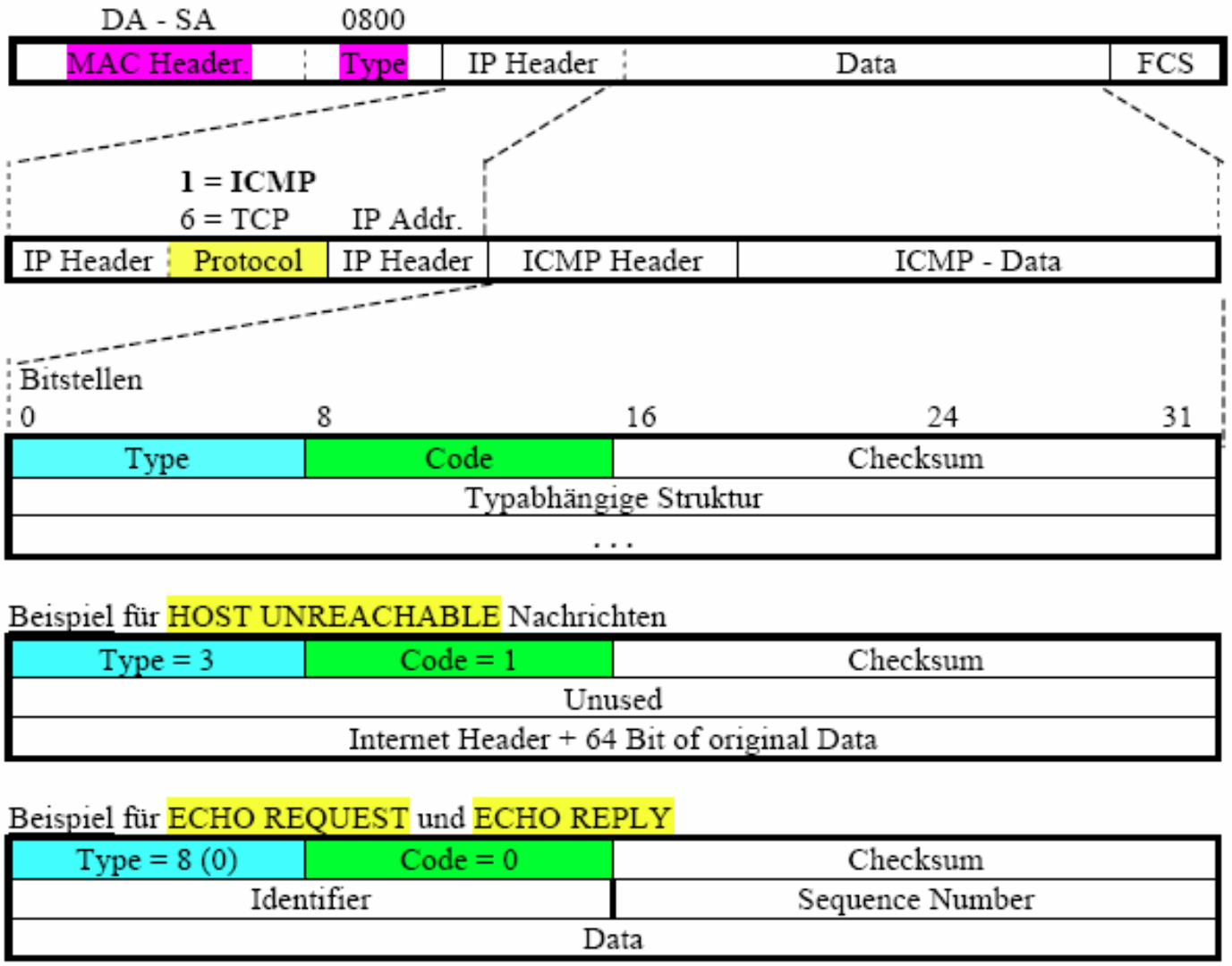
- **ICMP-протокол осуществляет:**
  - передачу отклика на пакет или эхо на отклик;
  - контроль времени жизни дейтограмм в системе;
  - реализует переадресацию пакета;
  - выдает сообщения о недостижимости адресата или о некорректности параметров;
  - формирует и пересылает временные метки;
  - выдает запросы и отклики для адресных масок и другой информации


Endstation
ICMP-Message
LAN
ICMP-Message
ICMP-Request
ICMP-Reply

ICMP

- **ICMP-сообщения об ошибках никогда не выдаются в ответ на:**
  - ICMP-сообщение об ошибке.
  - При мультикастинг или широковещательной адресации.
  - Для фрагмента дейтограммы (кроме первого).
  - Для дейтограмм, чей адрес отправителя является нулевым, широковещательным или мультикастинговым
- **Все ICMP пакеты начинаются с 8-битного поля типа ICMP и его кода (15 значений). Код уточняет функцию ICMP-сообщения. Таблица этих кодов приведена ниже (символом * помечены сообщения об ошибках, остальные - являются запросами):**

Формат ICMP [netze1.pdf]



Примеры

Beispiel für ECHO REQUEST und ECHO REPLY

Type = 8 (0)	Code = 0	Checksum
Identifier		Sequence Number
Data		

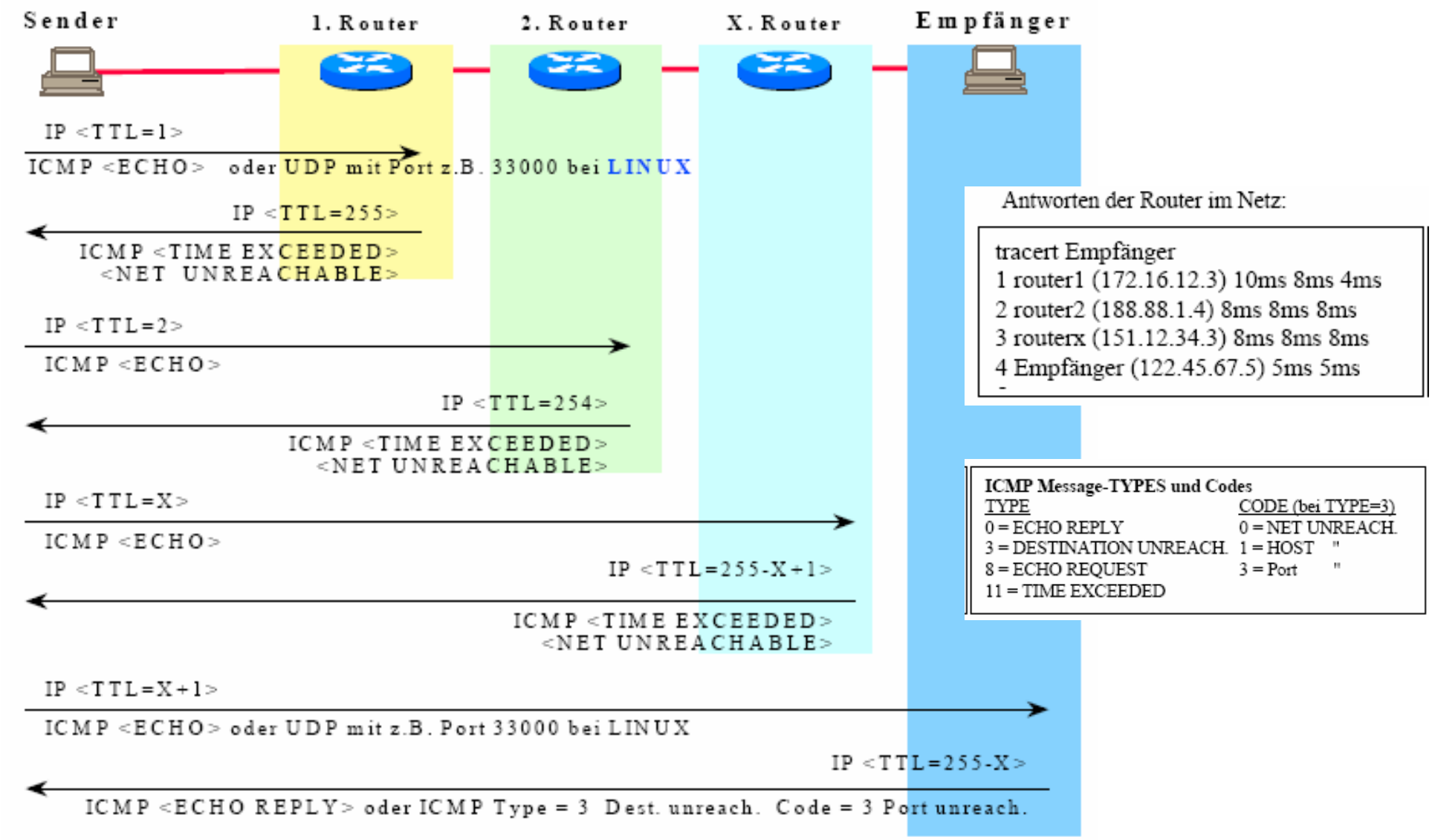
Type	Nachricht
0	Echo Reply
3	Destination unreachable
4	Source quench (Aussenderate drosseln)
5	Redirect Message
.	. ...
8	Echo Request
11	Time exceeded for datagram
	usw

Wenn **Type = 5**

Code	Meaning
0	Redirect for the network
1	Redirect for the Host
.	u.s.w

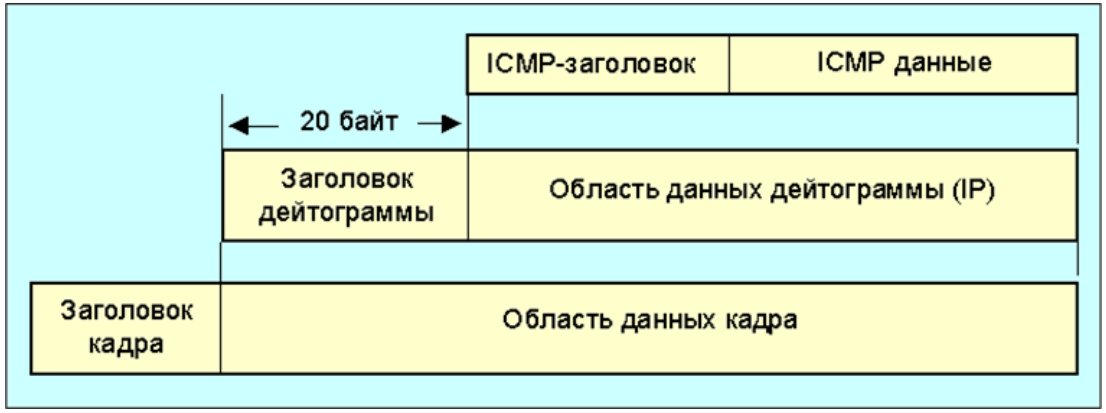
tracert

Beispiel: Trace A

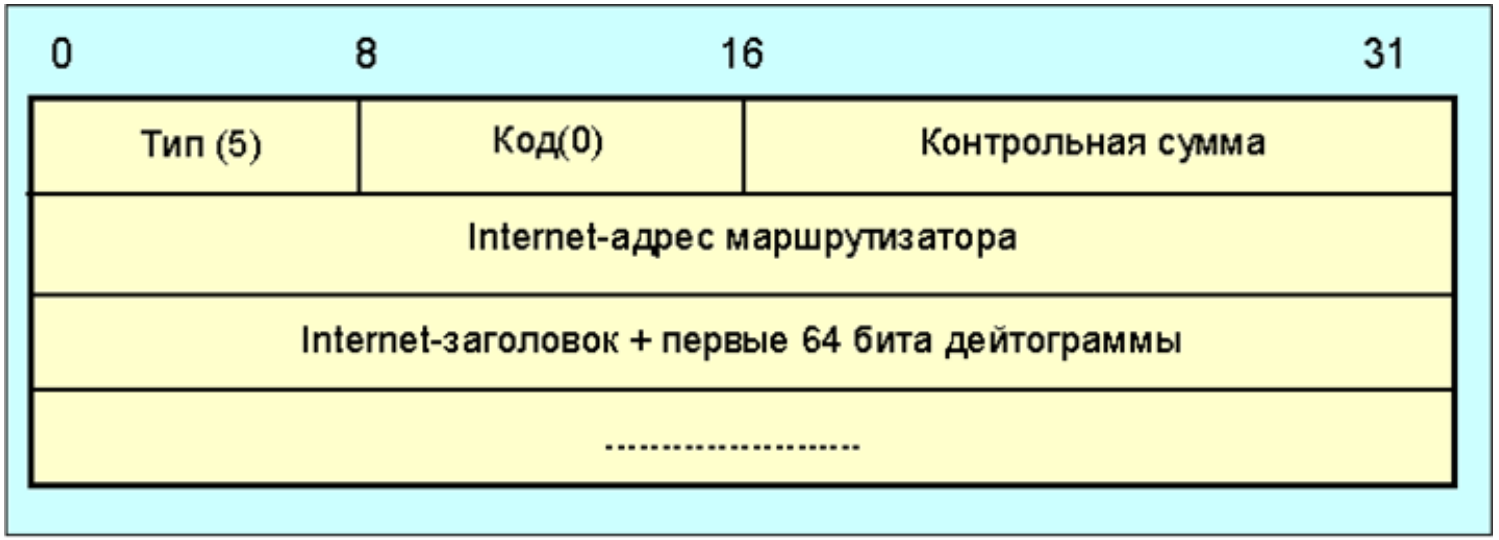


ICMP формат

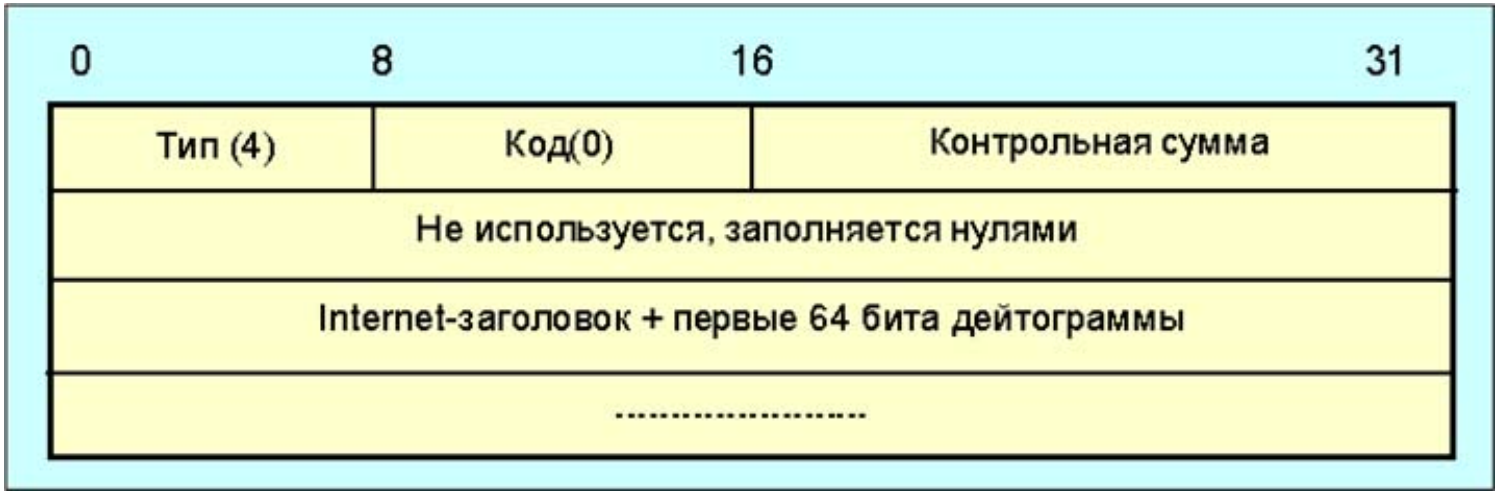
- **Код уточняет функцию ICMP-сообщения**
- **Поля идентификатор и номер по порядку служат для того, чтобы отправитель мог связать в пары запросы и отклики**



Формат ICMP-запроса переадресации

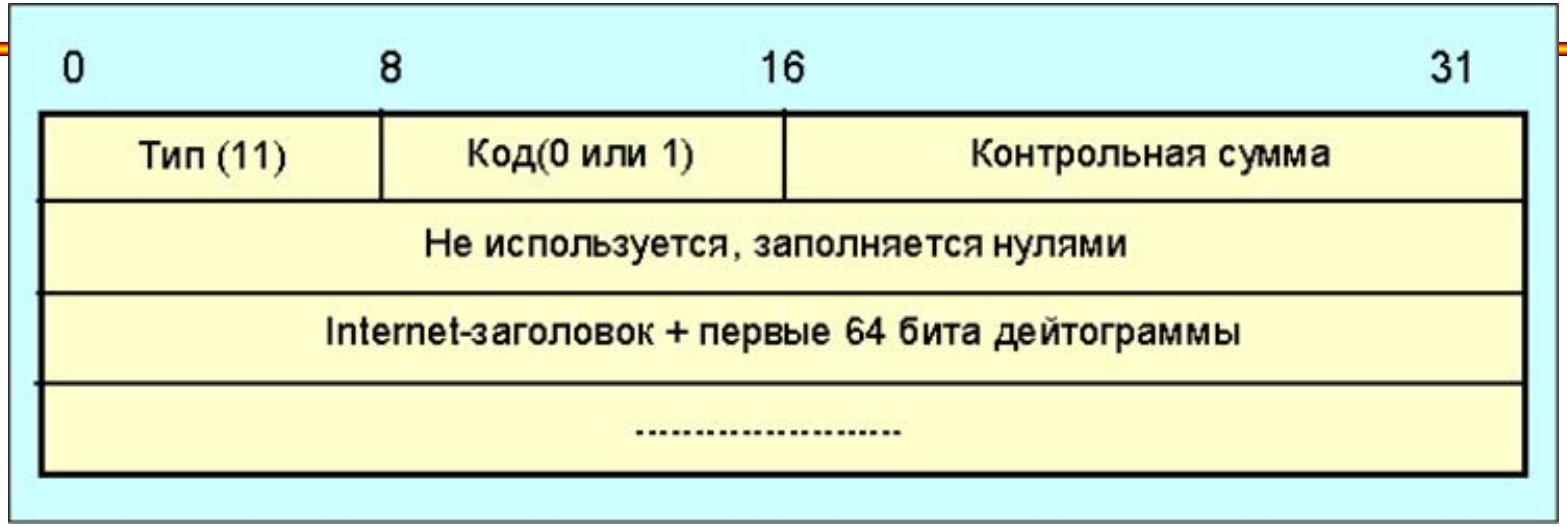


Формат ICMP-запроса снижения нагрузки

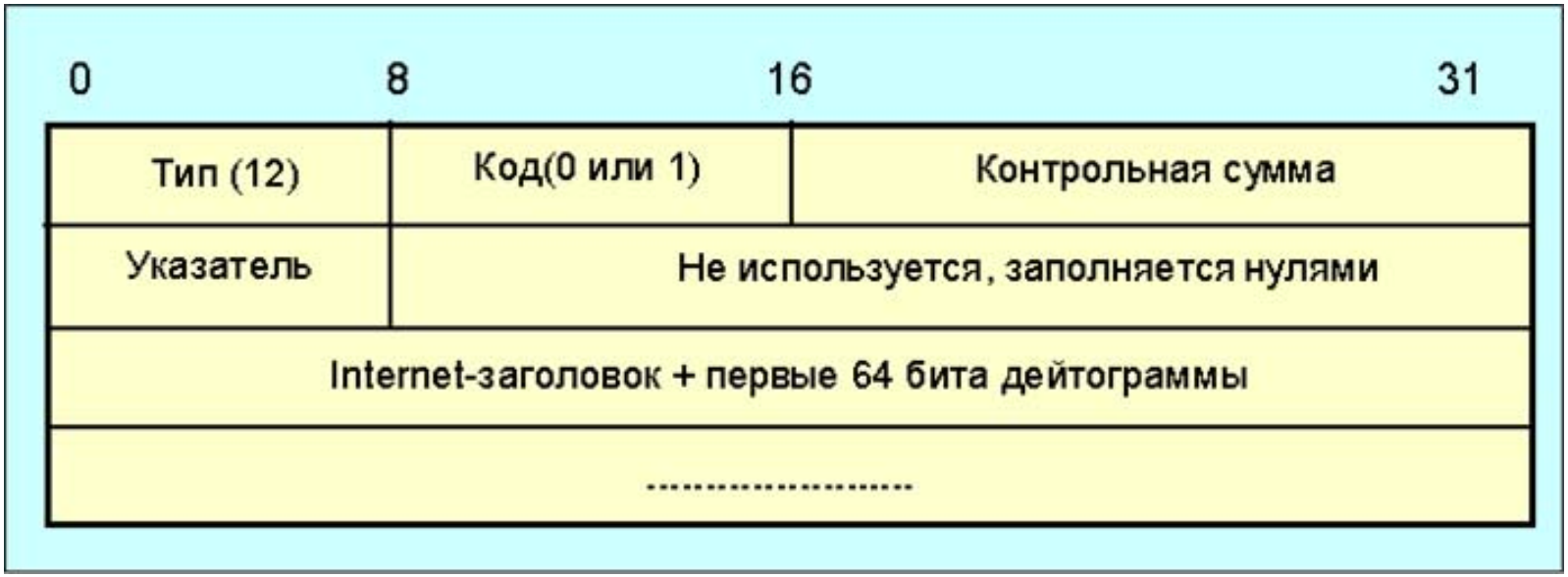


Формат эхо-запроса и отклика ICMP

Формат ICMP-сообщений об имеющихся маршрутах



Формат сообщения "время (ttl) истекло"



Формат сообщения типа "конфликт параметров"

Формат ICMP-запроса временной метки