IP-протокол

Общие сведения

Сервис

Формат пакета (дейтаграммы)

Поля заголовка, ToS, Фрагментация, Опции

СОДЕРЖАНИЕ

1. **Общие сведения**
2. **IP-сервис**
3. **Формат пакета (дейтаграммы)**
   - Поля заголовка
   - ToS (Type of Service)
   - Фрагментация
   - Опции

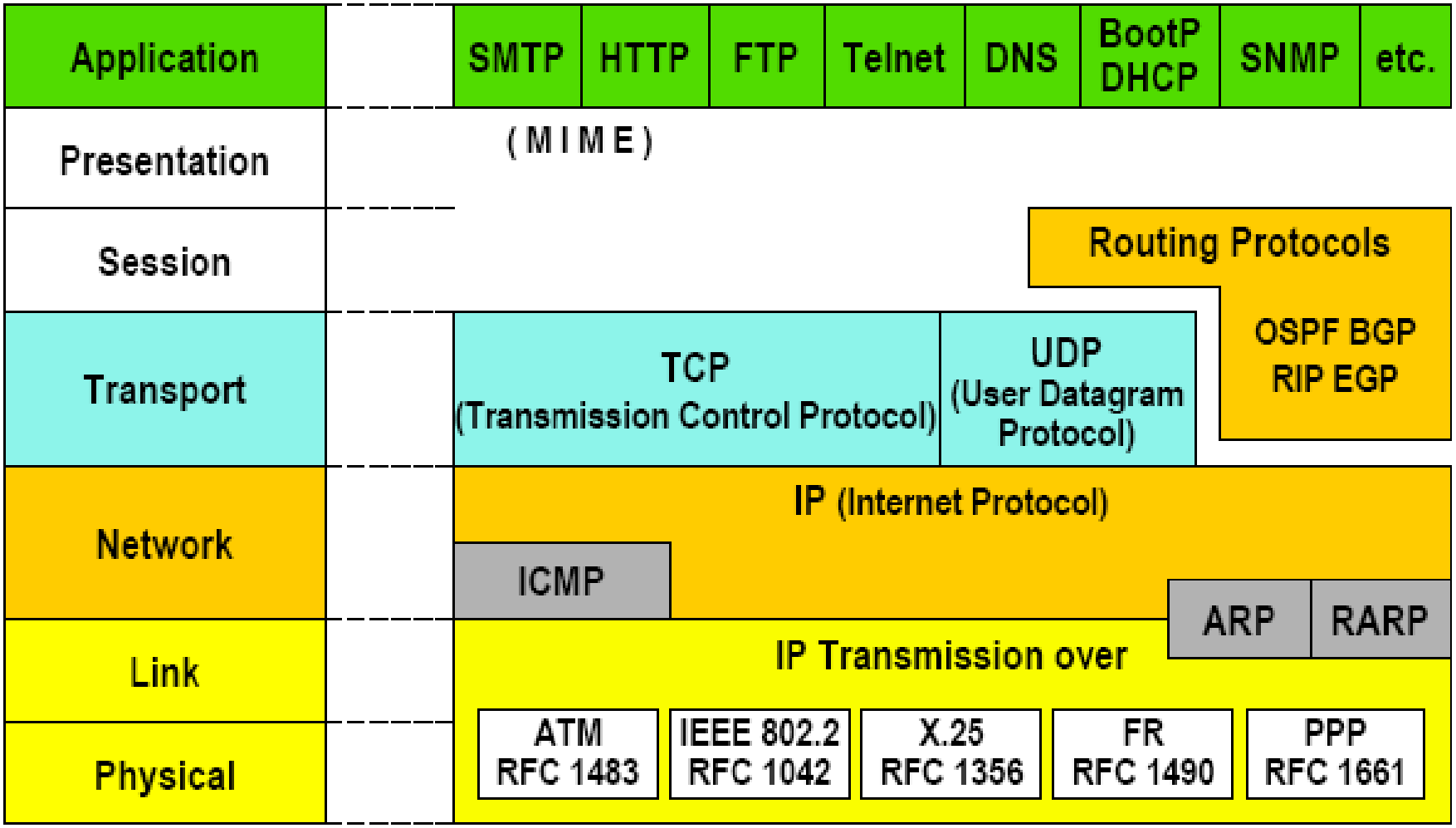
IP – технология (L3 OSI RM)

- **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

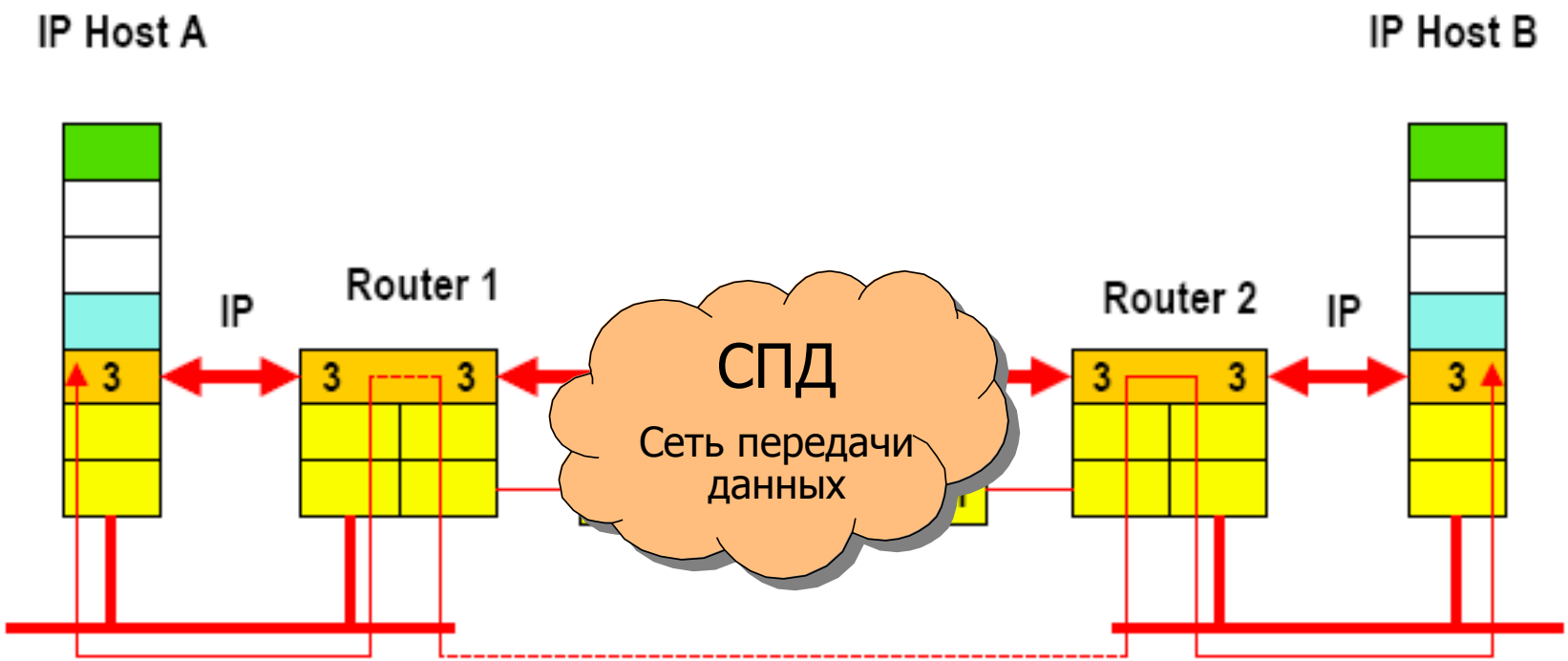
- **Протокол сетевого уровня (L3 OSI RM)**
  - Совместно с протоколом ICMP (Internet Control Message Protocol) образует сетевой уровень
- **IP PDU называется пакетом или дейтаграммой**
  - Пакет, поскольку коммутация пакетов
  - Дейтаграмма, поскольку:
    - ✓ независимость их следования друг от друга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

Назначение IP

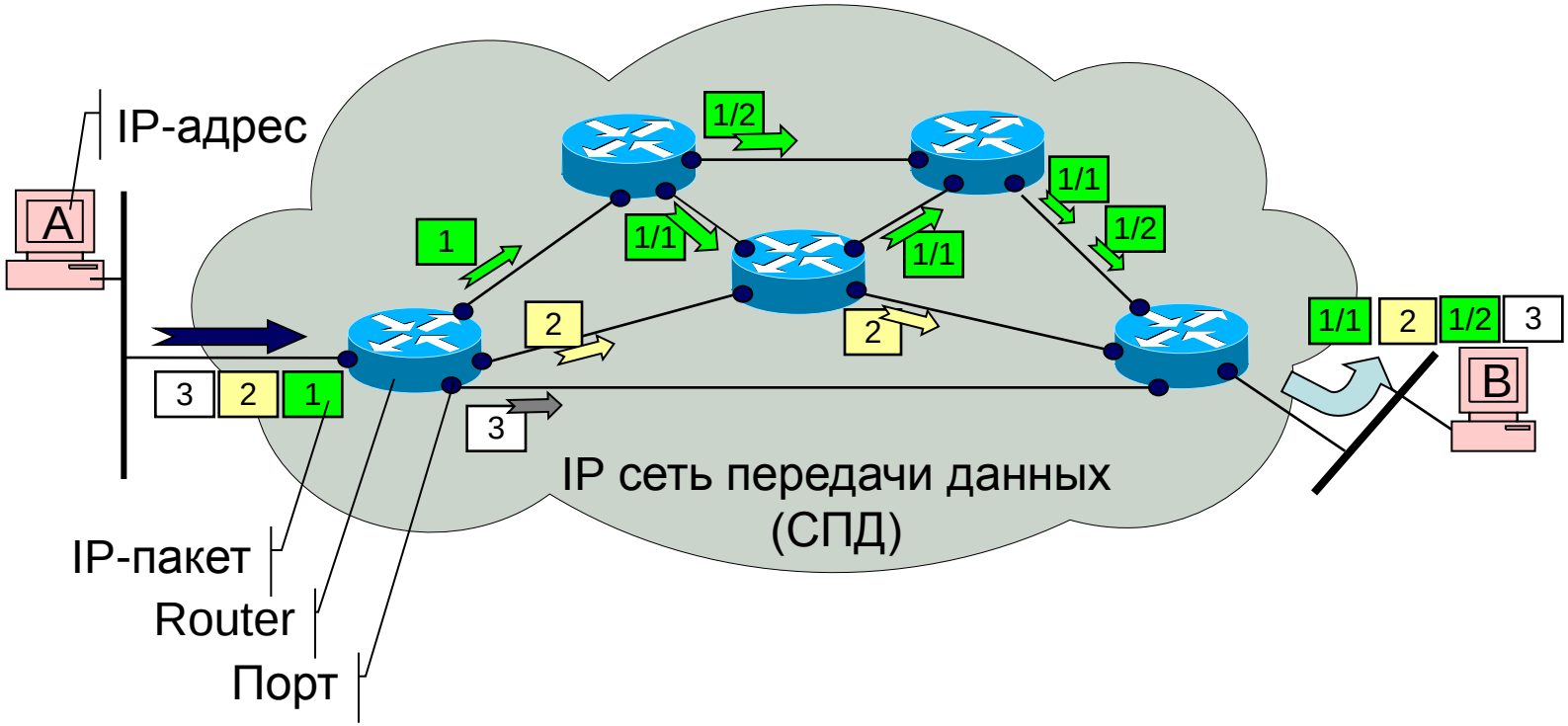
- **Доставка пакетов получателю (end-to-end)**
- **Характеристики доставки**
  - Ненадежная, пакет удаляется роутером
    - ✓ если в заголовке пакета ошибка
    - ✓ если роутер перегружен
    - ✓ если истекло время жизни пакета
  - Неупорядоченная (пакеты могут доставляться не в порядке передачи)
  - 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

0	4	8	16	19	31
Version	HLEN	ToS	Total Length		
Fragment Identifier			Flags	Fragment Offset	
TTL		Protocol	Header Checksum		
Source Address					
Destination Address					
IP Options					Pad
PAYLOAD					
.....					

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:**

0	1	2	3	4	5	6	7	биты
IP Precedence -IPP (приоритет)			D	T	R	C	MBZ	

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

0	1	2	3	4	5	6	7
IP Precedence -IPP (приоритет)			D	T	R	C	MBZ

биты

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 качества 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)

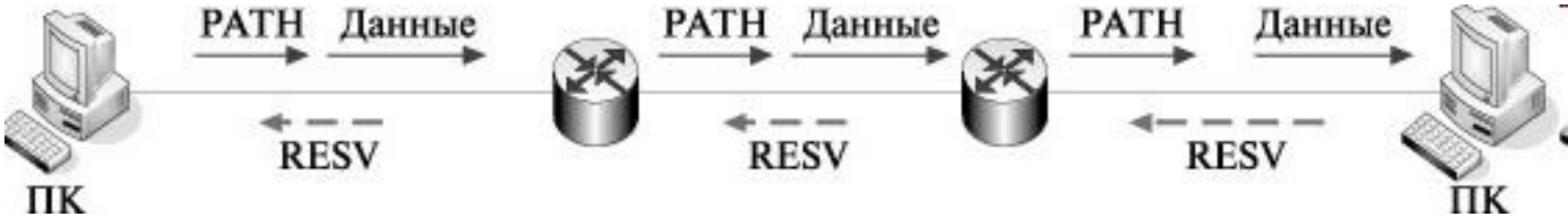
- **Оба метода используют “корзину маркеров” для описания параметров потока данных**
  - среднюю скорость (средний объем данных, который можно передать за единицу времени),
  - размер всплеска (объем данных, который можно отправить в течение заданного промежутка времени без ущерба для планирования очереди) 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
- **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

- **<u>Отправители</u> <u>посылают</u> управляющие <u>PATH-сообщения</u>**
  - Каждый RSVP-маршрутизатор, получивший PATH-сообщения, сохраняет IP-адрес предыдущей точки назначения, записывает вместо него свой собственный IP-адрес и отправляет обновленное сообщение
- **<u>Получатели запрашивают с помощью RESV-сообщения</u> 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 diffserv – 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

0	1	2	3	4	5	6	7
IP Precedence -IPP (приоритет)			D	T	R	C	MBZ

биты

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:

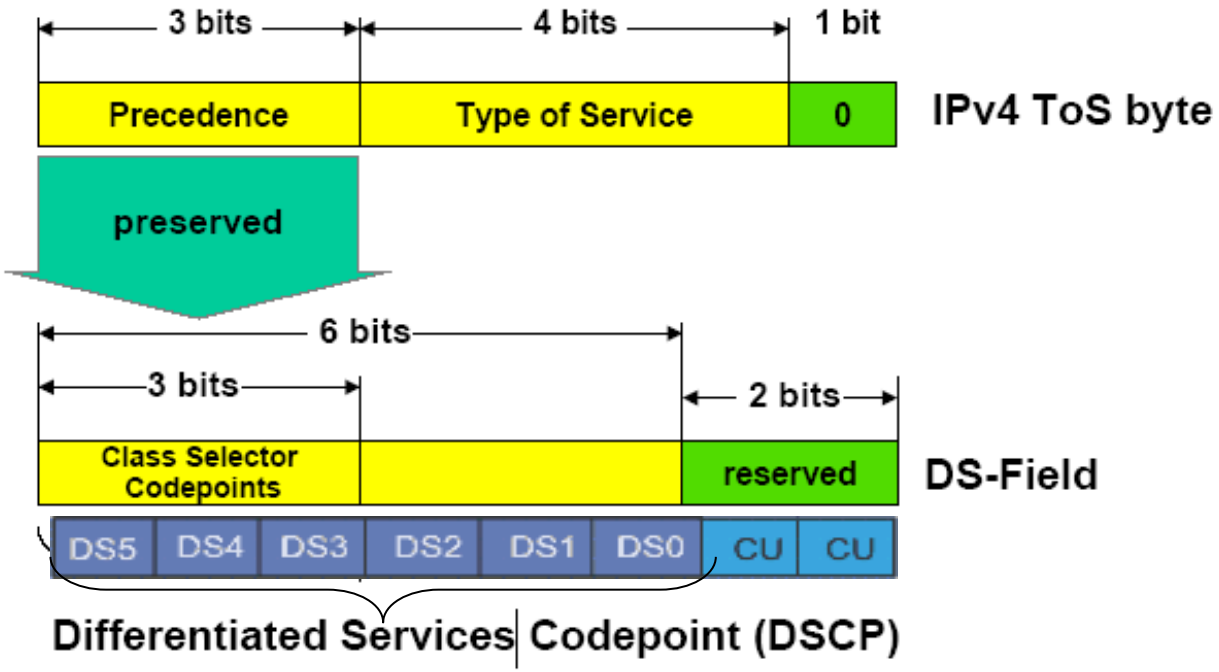
1000	D	Min delay	(min задержка)
0**1**00	T	Max throughput	(max скорость)
00**1**0	R	Max reliability	(max надежность)
000**1**	C	Min cost	(min стоимость)
0000	..	Normal service	(обычный сервис)

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

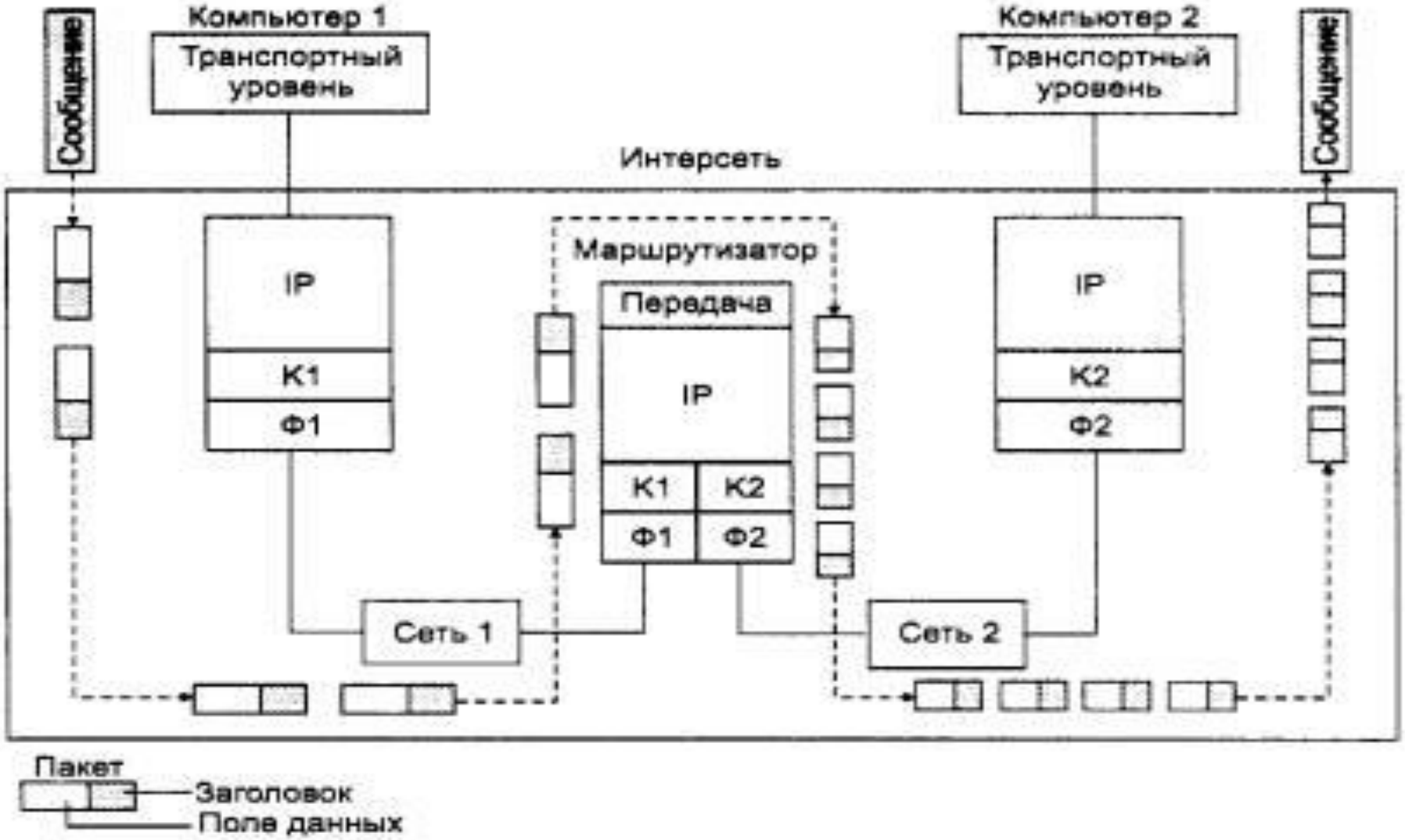
Зачем нужна вообще фрагментация?

- **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

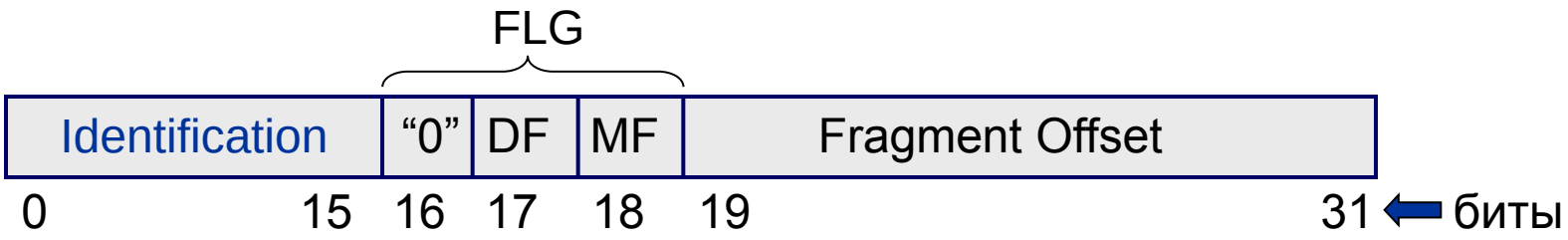
Зачем нужна вообще фрагментация?

- **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?

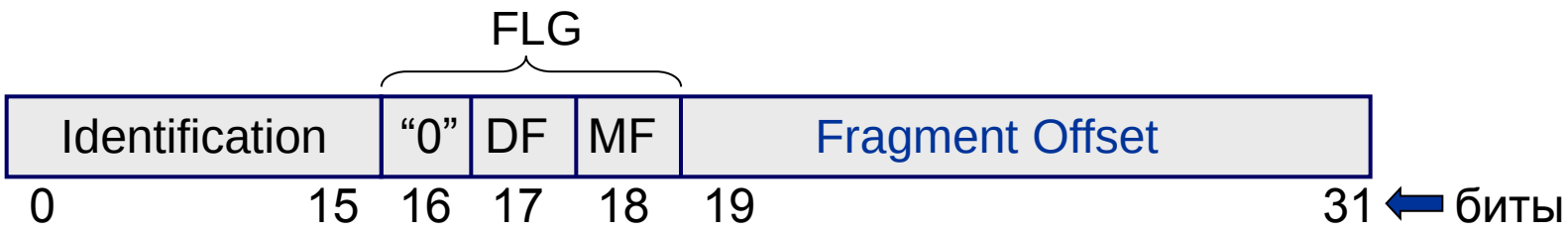


Заголовок IP-пакета (фрагментация)



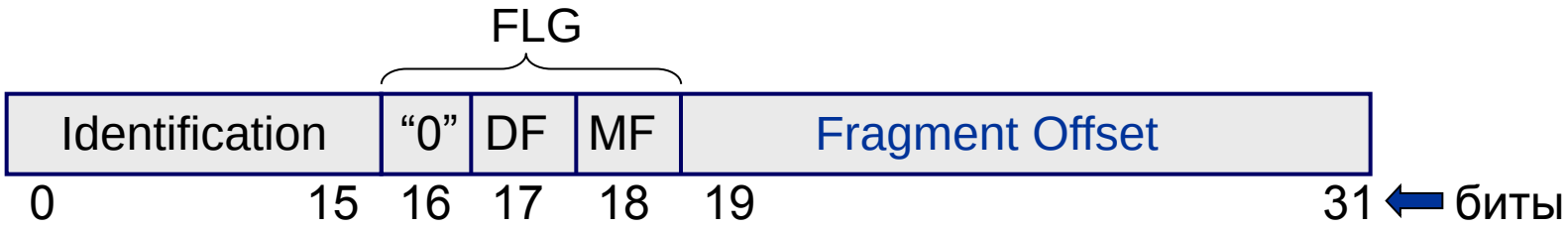
- **Identification – “Идентификатор” фрагмента**
  - используется вместе с полями “FLG” и “Fragment Offset” для правильной сборки пакета
  - код, присваиваемый каждому фрагменту пакета
  - каждый фрагмент получает один и тот же идентификатор
  - если нет фрагментации, значение поля Identification равно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

Заголовок IP-пакета (фрагментация)



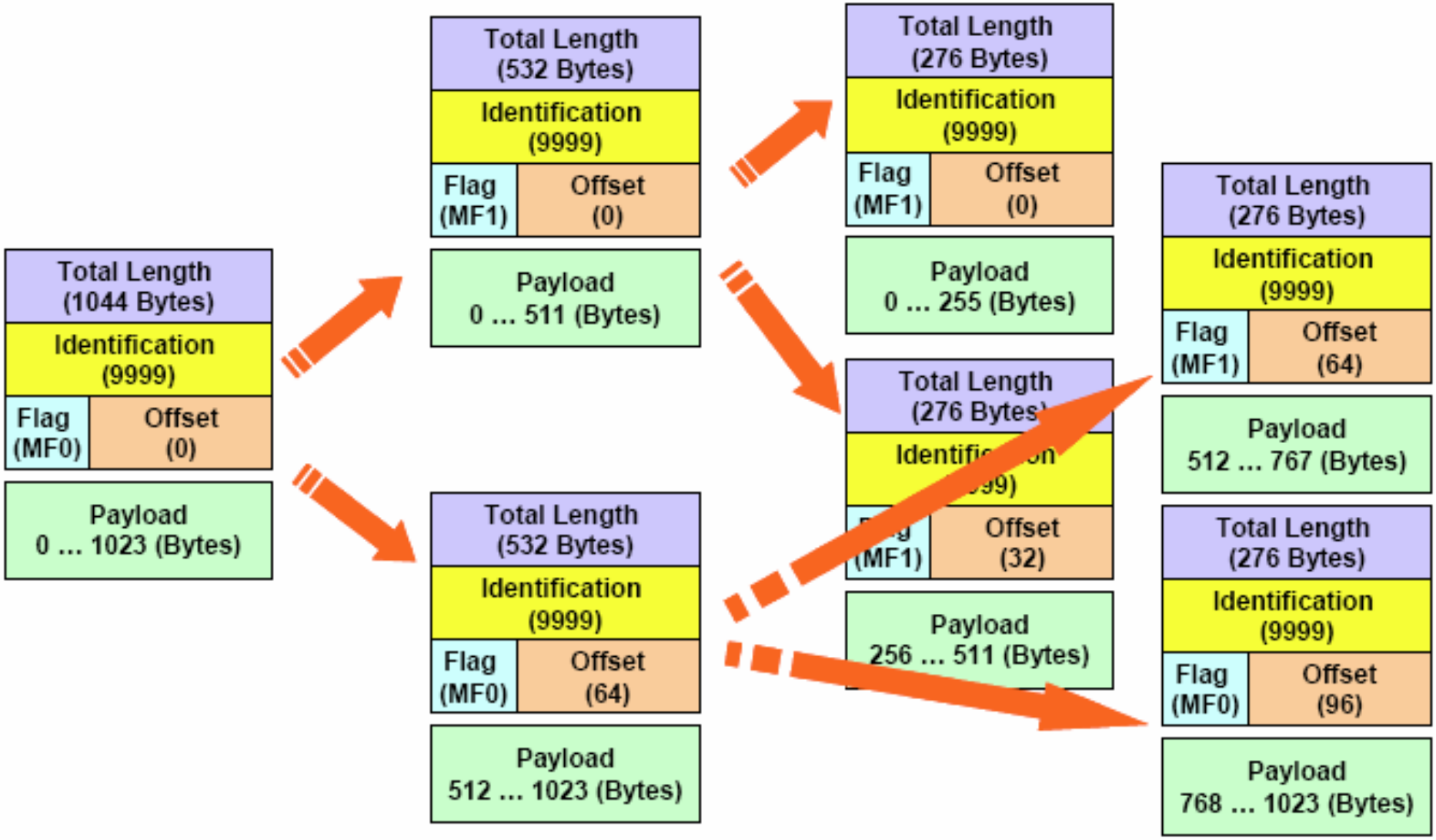
- **FLG (Flags) – “Флаг” управляет фрагментацией**
  - DF (don`t fragment)
    - ✓ если установлен (DF=1), то фрагментация запрещена
    - ✓ дейтаграмма отвергается если MTU (maximum transmission unit) следующего линка (хопа) меньше требуемой для передачи
  - MF (more fragments)
    - ✓ Если MF=1, значит 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)

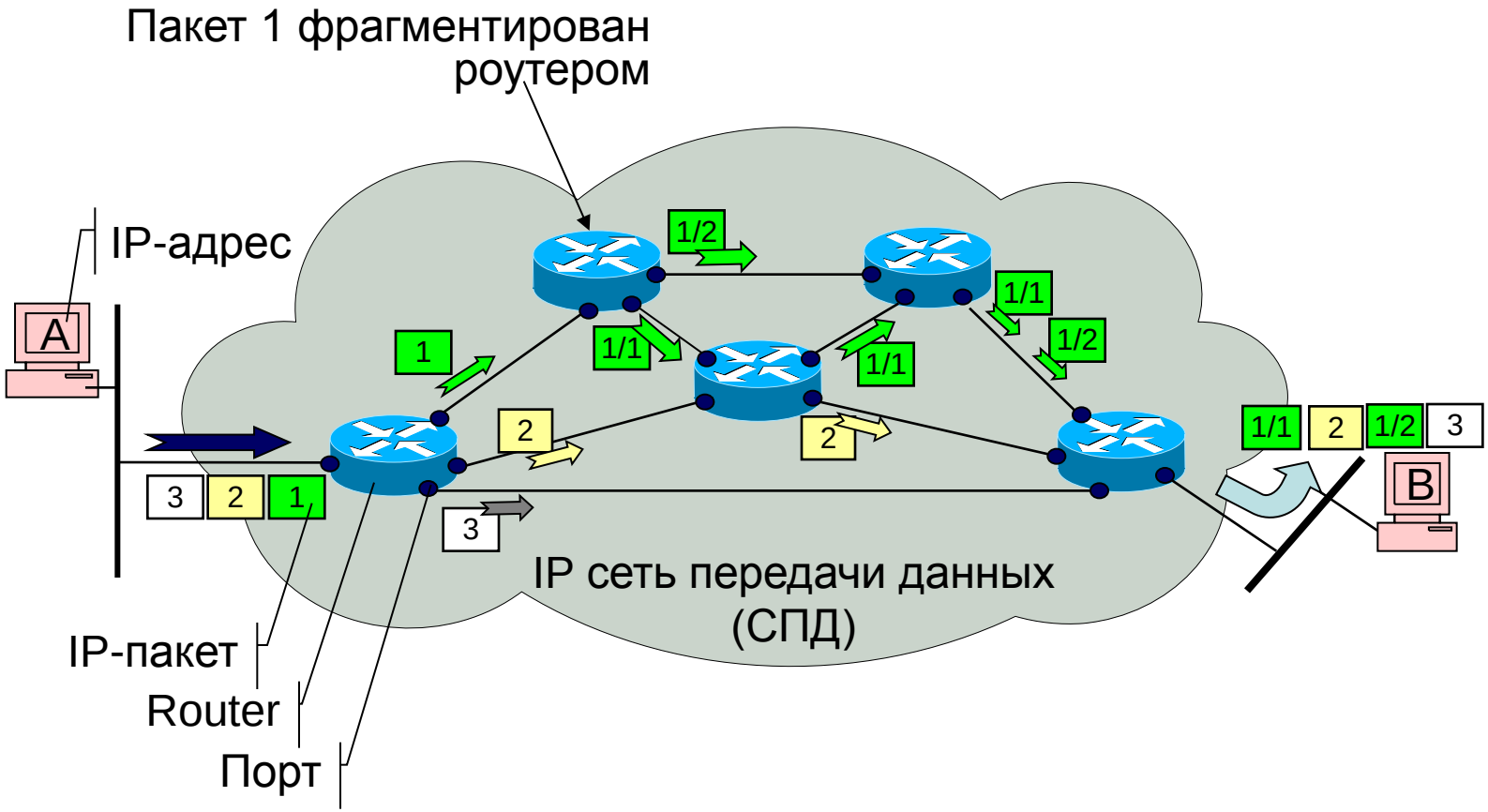


- **Fragment Offset –“смещение фрагмента”**
  - Показывает позицию фрагмента относительно начала первоначальной (оригинальной) дейтаграммы
  - Значение смещения кратно 8 байтам (64 бита)
  - Первый фрагмент и не фрагментированный пакет имеют значение “0”
  - Длина фрагмента, кроме последнего, должны 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)

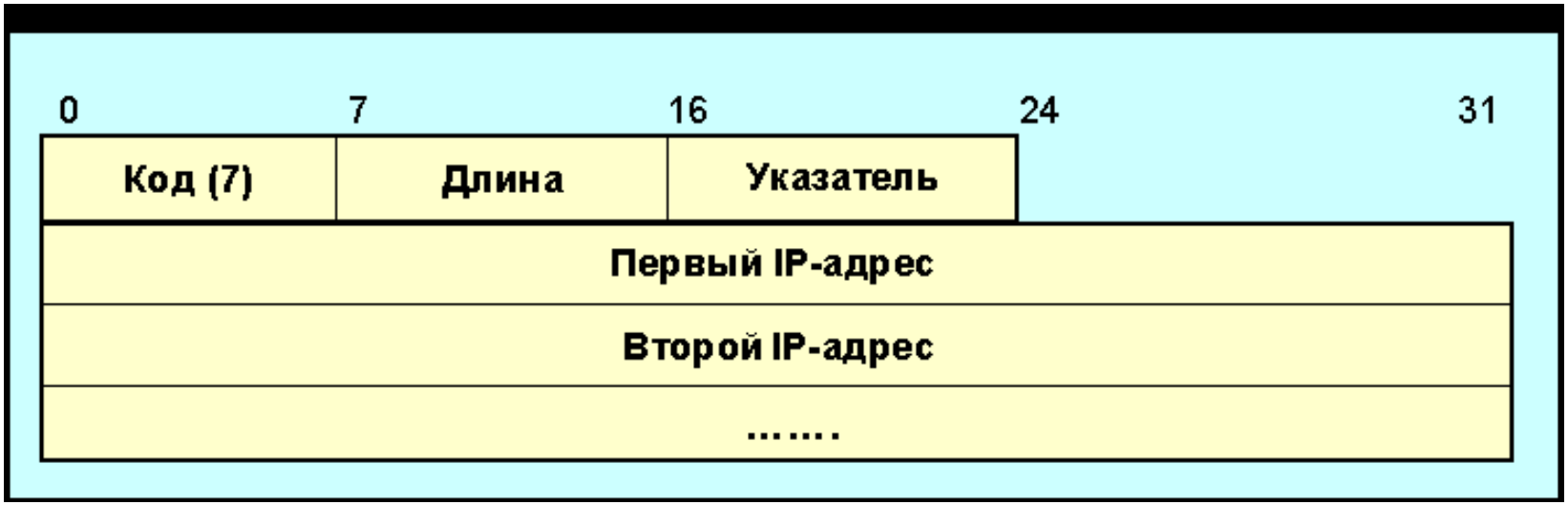
  3 - Зарезервировано для будущего использования

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

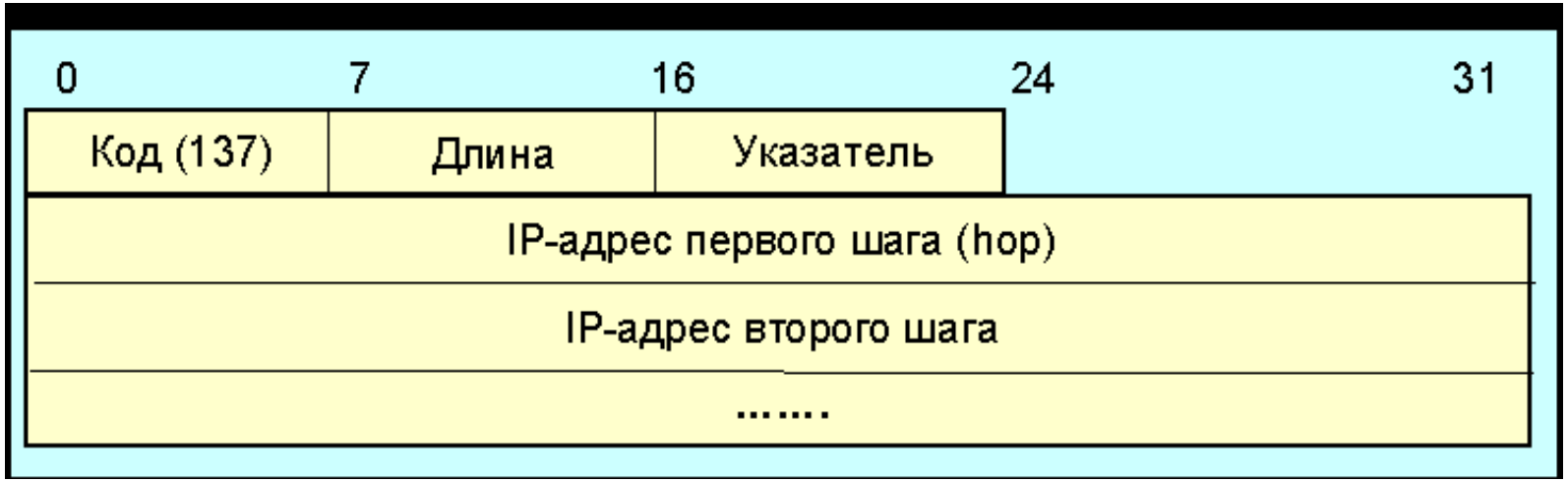
Опция ЗАПИСАТЬ МАРШРУТ

- **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**

0	7	16	24	31
Код (68)	Длина	Указатель	Переполнение	Флаги
Первый IP-адрес				
Первая временная метка				
…….				