ИТМО УНИВЕРСИТЕТ ИТМО

«Компьютерные сети»

Лектор: **АЛИЕВ Тауфик Измайлович, *д.т.н., профессор***

Национальный исследовательский университет ИТМО (НИУ ИТМО)

Факультет программной инженерии и компьютерной техники

Разделы дисциплины

Раздел 1. Принципы организации компьютерных сетей
Раздел 2. Глобальная сеть Интернет
Раздел 3. Технологии локальных сетей
Раздел 4. Транспортные технологии глобальных сетей
Раздел 5. Заключительный раздел

Раздел 2
Глобальная сеть Internet

2.1. Введение в Internet
2.2. Адресация в IP-сетях
2.3. Фрагментация IP-пакетов
2.4. Транспортные протоколы TCP/IP: UDP, TCP
2.5. Коммуникационный протокол IPv4
2.6. Протоколы маршрутизации: RIP, OSPF
2.7. Протокол межсетевых управляющих сообщений ICMP
2.8. Коммуникационный протокол IPv6
2.9. Протоколы канального уровня для выделенных линий

2.1. Введение в Internet

Специфические особенности глобальной сети Internet

1. *Неограниченный* территориальный охват.
2. Сеть объединяет *подсети (в том числе локальные сети) разных технологий* и *компьютеры разных классов* (от персональных до суперкомпьютеров).
3. Для передачи данных на большие расстояния используется *аппаратура передачи данных* (модемы, приемопередатчики) и активное сетевое оборудование (маршрутизаторы, коммутаторы).
4. Топология глобальных сетей, в общем случае, *произвольная многосвязная*.
5. Одна из важнейших задач – *организация эффективной маршрутизации* передаваемых данных.
6. Глобальная сеть содержит *каналы связи разных типов* с пропускными способностями до сотен Гбит/с: кабельные оптические и электрические, в том числе телефонные, беспроводные наземные и спутниковые каналы.

Достоинства сети Internet

1. *Неограниченный доступ* к любым вычислительным и информационным ресурсам, а также множеству специфических услуг (электронная почта, голосовая связь, конференцсвязь, телевидение по запросу и т.д.).
2. Возможность доступа к ресурсам сети практически *из любой точки Земного шара*.
3. Возможность передачи *любых видов данных*, в том числе мультимедийных (аудио, видео).

1969	***1972***	***1983***	***1983***	***1984***	***1989***	***1990***
ARPANET 4 узла	***ARPANET 30 узлов***	***TCP/IP***	***Internet/NSFNet***	***DNS***	***WWW, HTTP***	***INTERNET***

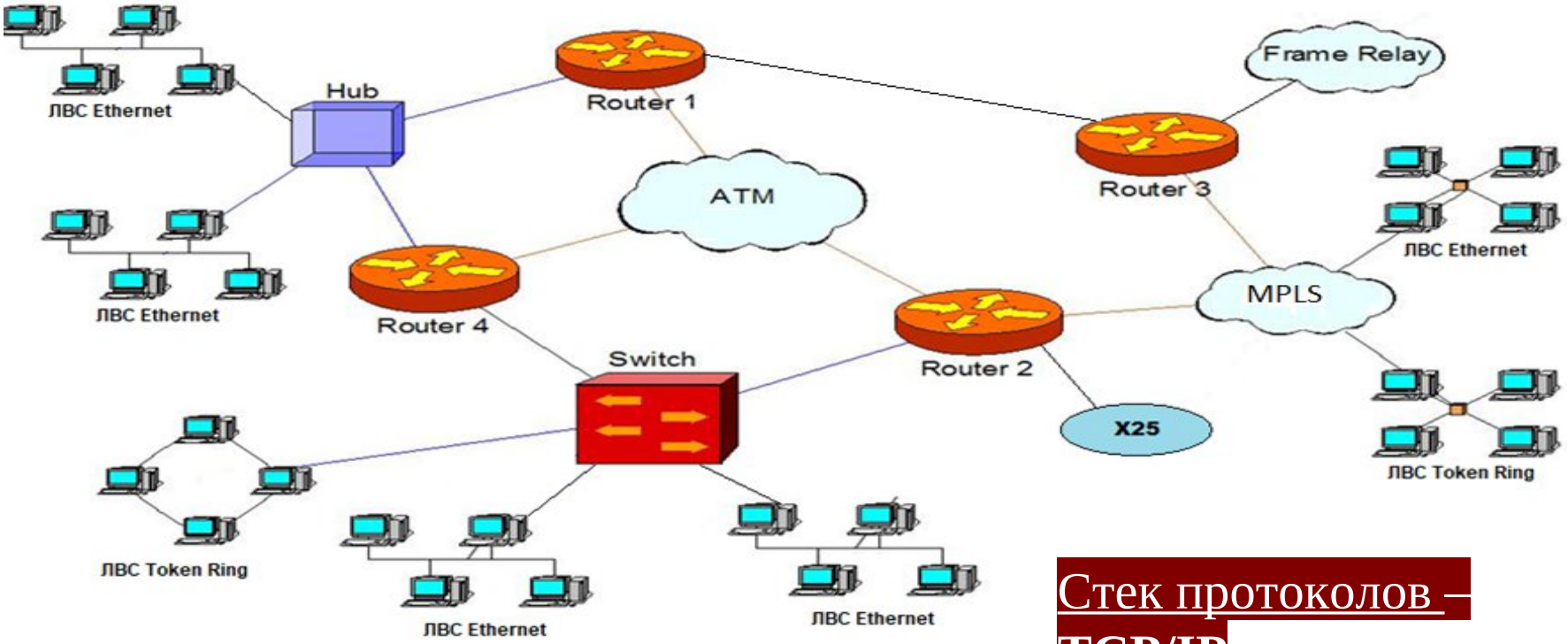
2.1. Введение в Internet

Архитектурная концепция

Физические сети (подсети)

Локальные сети (Ethernet, Token Ring)

Коммуникационные системы (модемные коммутируемые или выделенные линии, сети X.25, Frame Relay, FDDI, ATM и др.)



Стек протоколов – **TCP/IP**

Сеть Internet - множество компьютеров (***хосты***), подключенных к единой интерсети, представляющей собой совокупность ***физических сетей (подсетей)***, объединенных каналами связи с **маршрутизаторами** и **коммутаторами**.

Стек протоколов TCP/IP

Особенность стека протоколов TCP/IP – независимость от среды передачи данных.

Протокол IP (Internet Protocol) обеспечивает:

- дейтаграммную доставку без установления соединения;
- негарантированную доставку информации;
- максимально возможную доставку пакетов.

TCP (Transmission Control Protocol) – протокол управления передачей данных

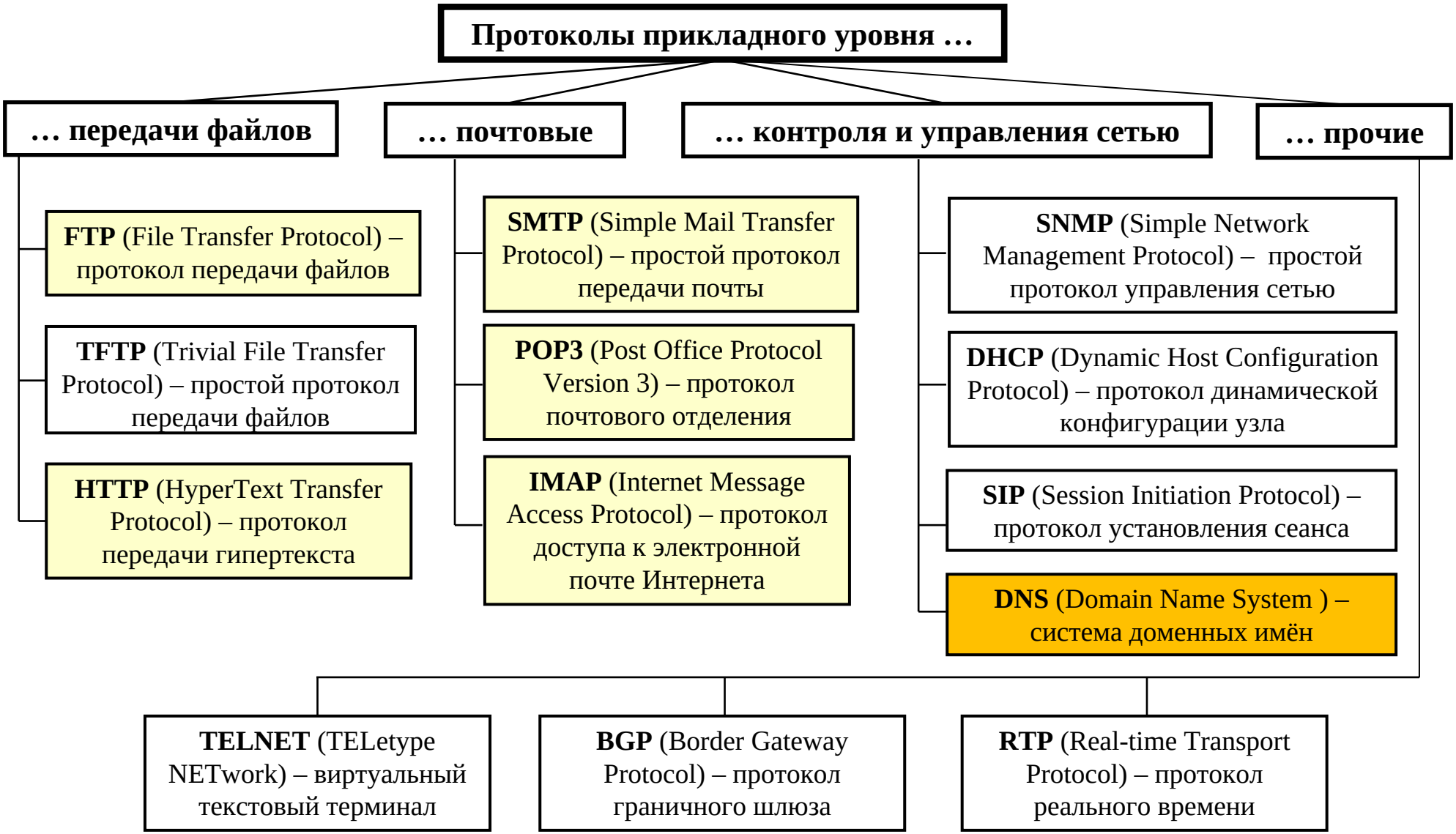
UDP (User Datagram Protocol) – протокол пользовательских дейтаграмм

Протоколы TCP и UDP обеспечивают доставку из конца в конец (end to end):

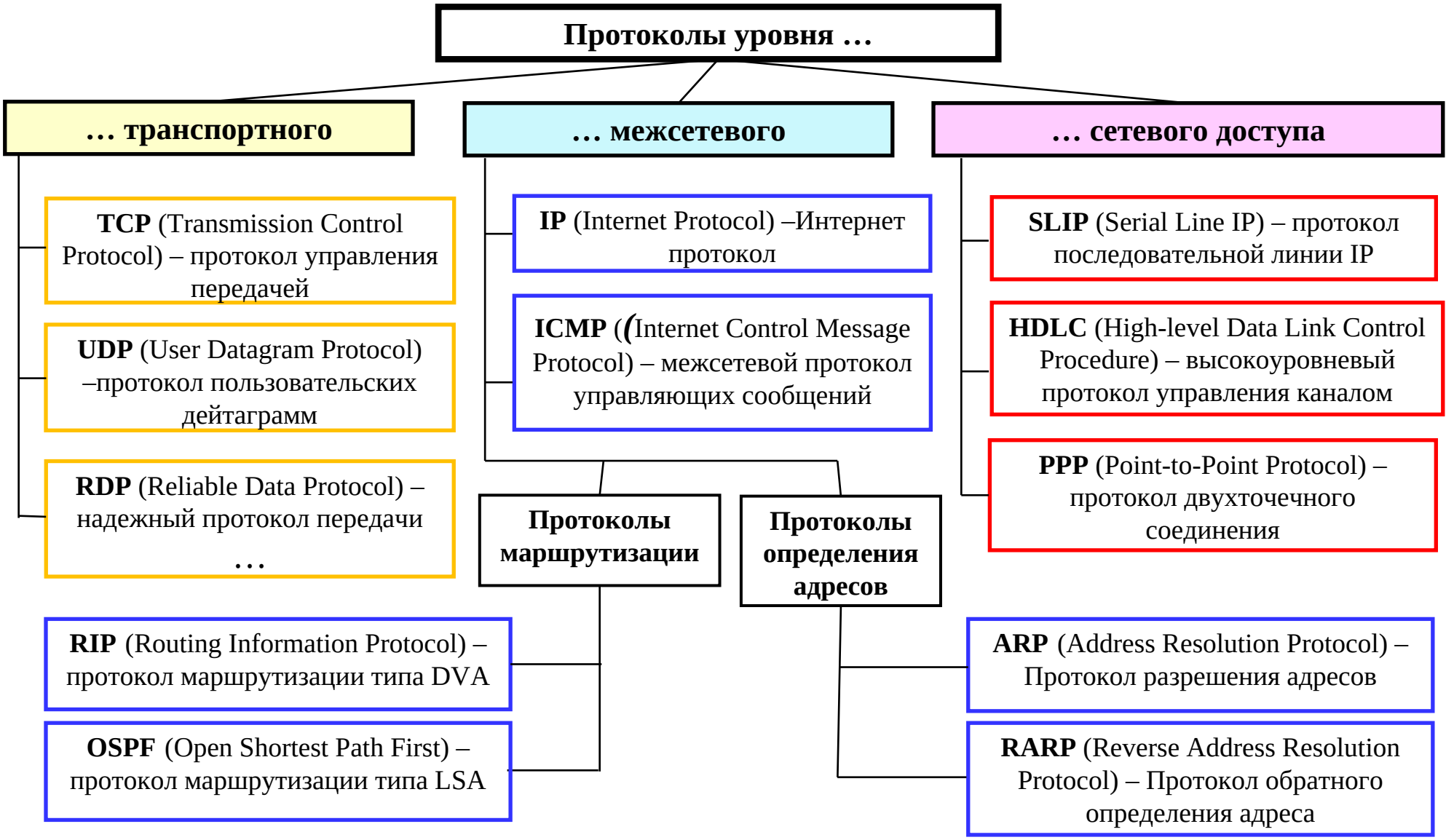
- с установлением соединения (TCP);
- без установления соединения (UDP).

Уровни OSI	Уровни TCP/IP	Протокол	Блок данных
5 – 7	Application (прикладной)	FTP, BGP, HTTP, DNS, *DHCP,* SNMP, SMTP, POP3, IMAP, RTP	Сообщение
4	Transport (транспортный)	**TCP**, UDP	Сегмент, дейтаграмма
3	Internet (межсетевой)	**IP**, RIP, OSPF, ICMP, IGMP, *ARP, RARP*	Пакет
1 – 2	Network Access Layer (уровень сетевого доступа)	SLIP, HDLC, PPP	Кадр

Протоколы прикладного уровня 4

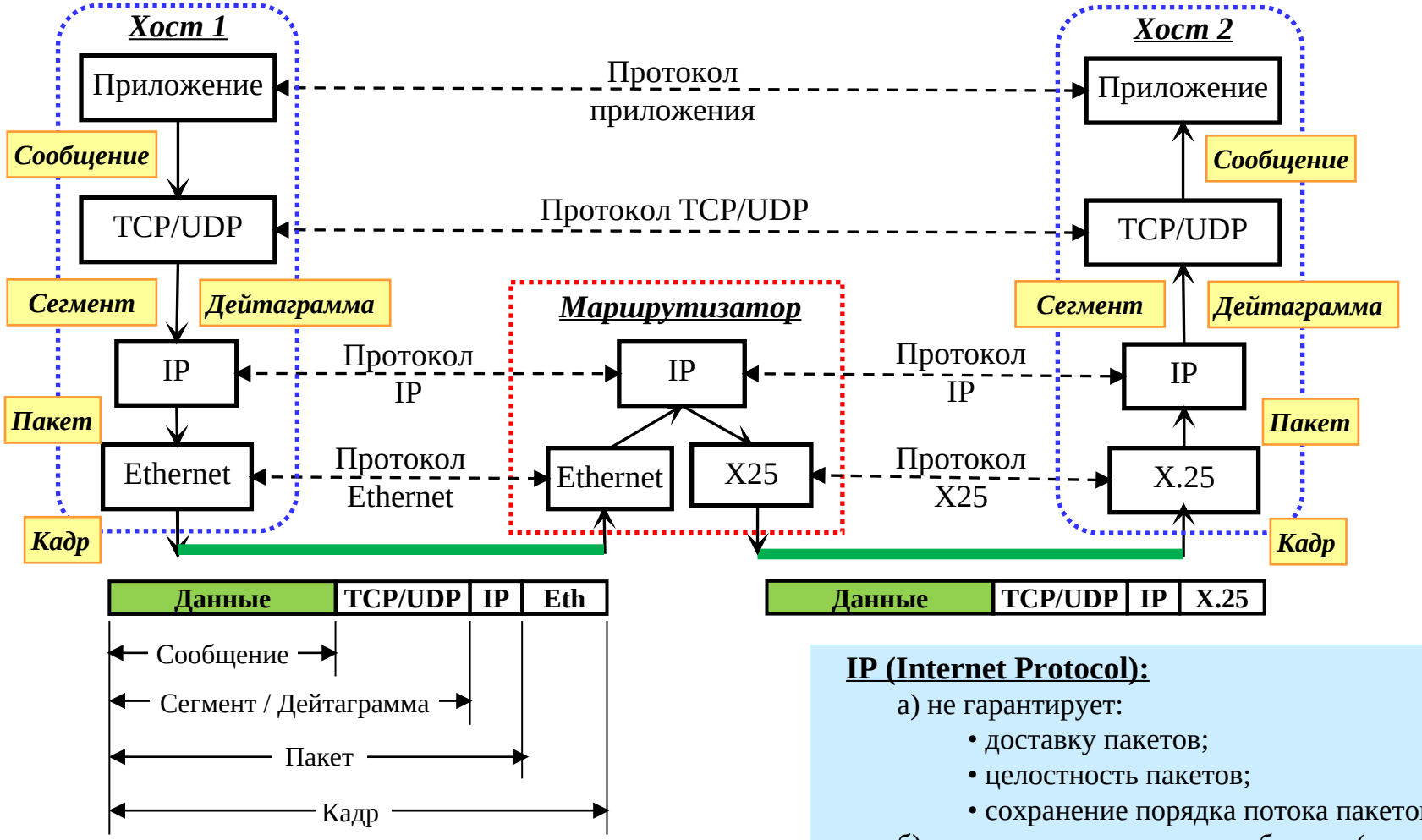


Протоколы уровней 1-3



Концептуальная модель передачи данных в сетях TCP/IP

Функции протокола IP возлагаются на *хосты и маршрутизаторы*, называемые ***узлами*** сети.



IP (Internet Protocol):

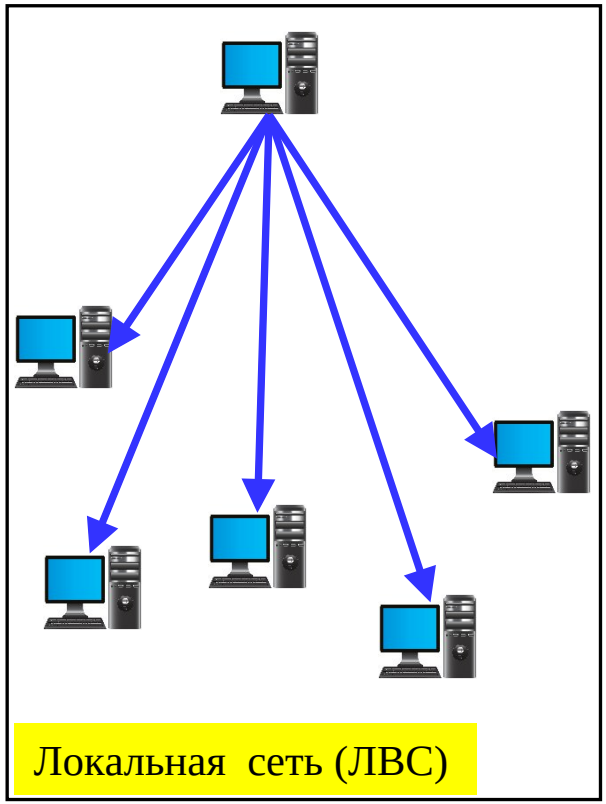
а) не гарантирует:
- доставку пакетов;
- целостность пакетов;
- сохранение порядка потока пакетов;

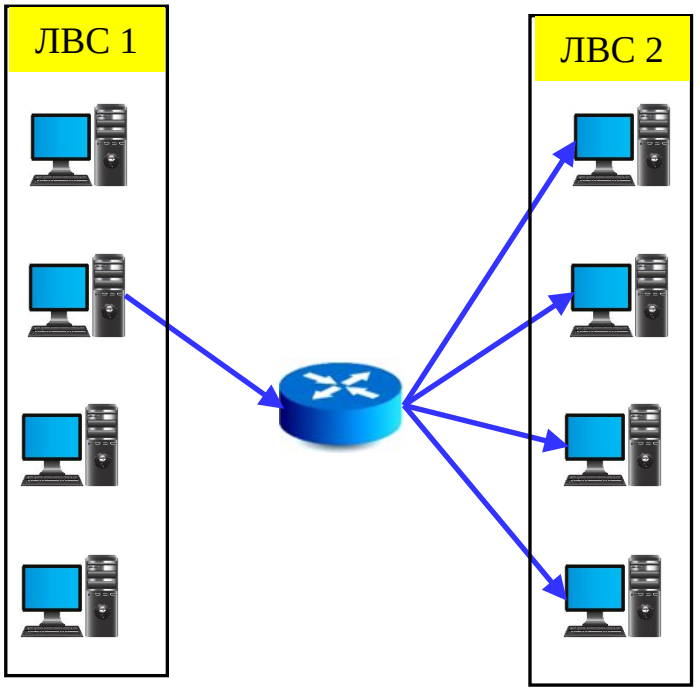
б) не различает логические объекты (процессы), порождающие поток данных.

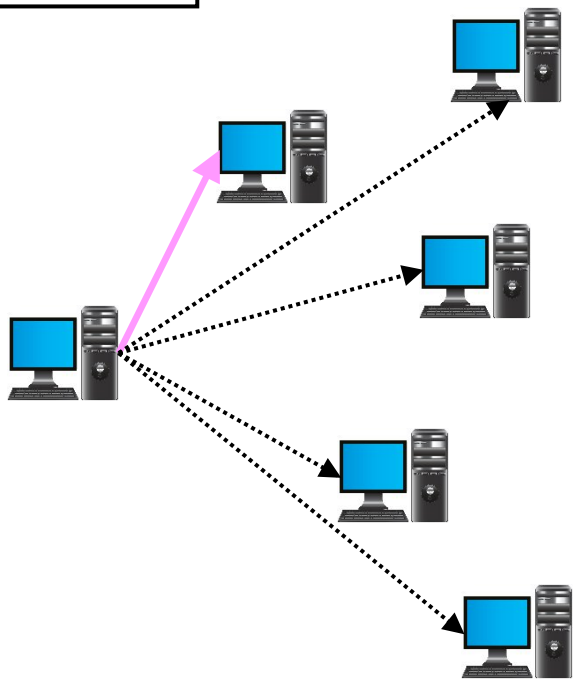
2.1. Введение в Internet

Виды трафика в сети Internet

- **Unicast** (индивидуальный)
- **Multicast** (групповой)
- **Broadcast**
  - **ограниченный** (внутри ЛВС)
  - **направленный** (в другую ЛВС)
- **Anycast** (любой)







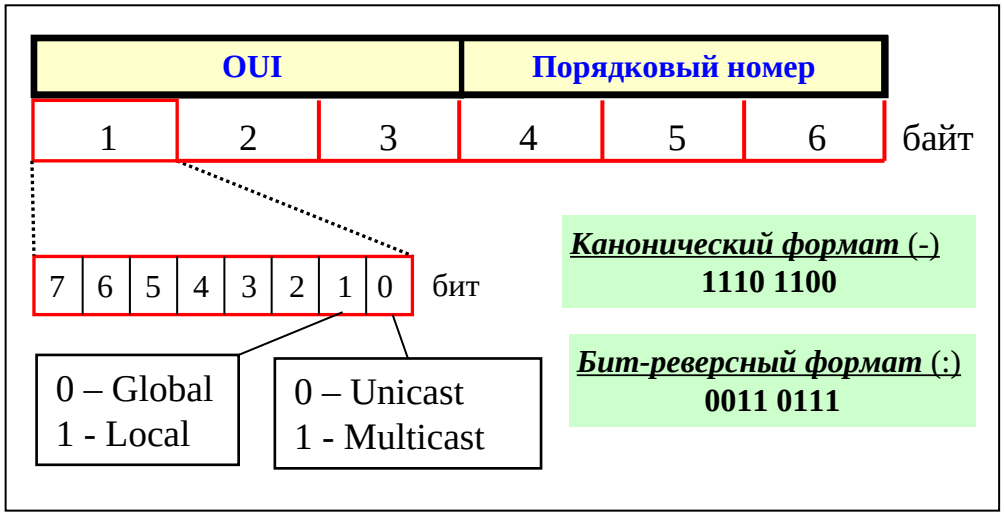
2.2. Адресация в IP-сетях

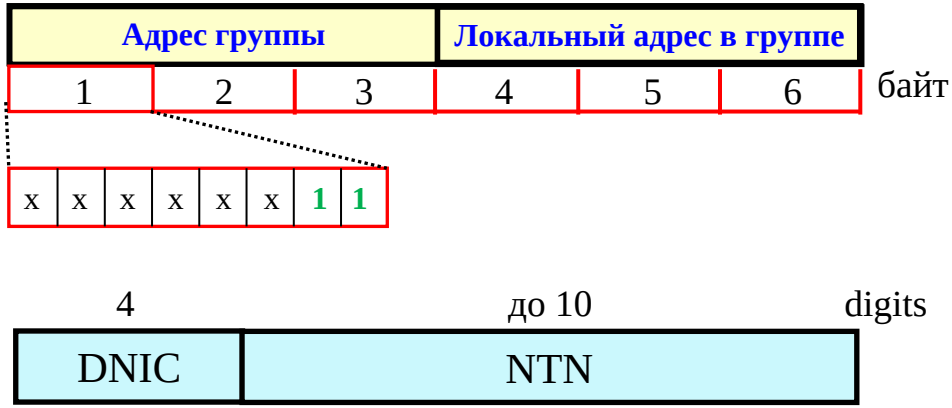
Типы адресов

Типы адресов в IP - сетях

- **Локальные** (физические, аппаратные) адреса
  - MAC-адреса (**EUI**-48)
  - X.25 – адреса (X.121)
  - прочие
- **Сетевые** адреса (IP-адреса)
  - 12.65.2.51
  - 192.168.43.1
- Доменные имена
  - ifmo.ru
  - mail.yandex.ru
  - norton.com
  - edu.dov.ru

EUI (*Extended Unique Identifier)* - расширенный уникальный идентификатор





DNIC – Data Network Identification Code: Country (3)+PSN (1)
PSN – Packet-Switched Network
NTN - National Terminal Number

01-00-5e-00-02-1b – групповой MAC-адрес
2a-00-f3-16-cd-01 – локальный MAC-адрес
fc-5a-02-ab-f4-08 – уникальный глобальный

Классовая адресация

Типы адресов в IP - сетях

Локальные адреса | **Сетевые** адреса (**IPv4**-адреса) | Доменные имена

Классы IPv4-адресов (32 бит = 4 байт): **190.171.153.15**

Биты	**0**	**1**	**2**	**3**	**4**	…	**8**	…	**16**	…	**24**	…	**31**
Класс A	0	Номер сети					Номер узла						
Класс B	1	0	Номер сети						Номер узла				
Класс C	1	1	0	Номер сети							Номер узла		
Класс D	1	1	1	0	Групповой адрес								
Класс E	1	1	1	1	0	Зарезервирован							

Адреса сети (подсети):
- **A. 45.**0.0.0
- **B. 170.25.**0.0
- **C. 219.121.43.**0

Адреса хостов / интерфейсов:
- A. 45**.0.1.234**
- B. 170.25**.252.1**
- C. 219.121.43**.158**

IP-адреса для автономного использования:
- **A. 10.0.0.0** (1 сеть);
- **B. 172.16.0.0 – 172.31.0.0** (16);
- **C. 192.168.0.0 – 192.168.255.0** (256)

Класс		**A**	**B**	**C**	**D**
Размер сети		Большая	Средняя	Малая	Групповой адр.
Номер (адрес) сети	*наименьший*	1.0.0.0	128.0.0.0	192.0.0.0	224.0.0.0
	наибольший	126.0.0.0	191.255.0.0	223.255.255.0	239.255.255.255
Максим. число узлов		16777214	65534	254	
Длина поля, в битах	*NetID*	7	14	21	
	HostID	24	16	8	

IP1= **205.2.3.10**
IP2= **195.78.1.5**

Специальные адреса и маскирование

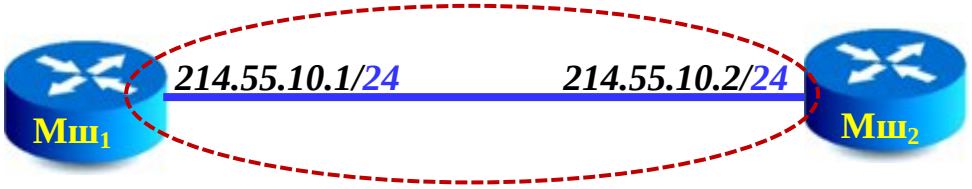
Специальные адреса IPv4

- Групповые (multicast)
  - Постоянные (well-known addresses)
  - Временные (transient multicast groups)
- Широковещательные (broadcast) **192.168.141.255**/24

Протокол IGMP (Internet Group Management Protocol)

Тип	Номер сети	Номер узла
Адрес 1	0 0 0 … 0	0 0 0 … 0
Адрес 2	0 0 0 … 0	x x x … x
Адрес 3	x x x … x	0 0 0 … 0
Адрес 4	*1 1 1 … 1*	*1 1 1 … 1*
Адрес 5	x x x … x	1 1 1 … 1
Адрес 6	**01111111**	

127 – ***адрес обратной петли (тестовый адрес) – loopback address***



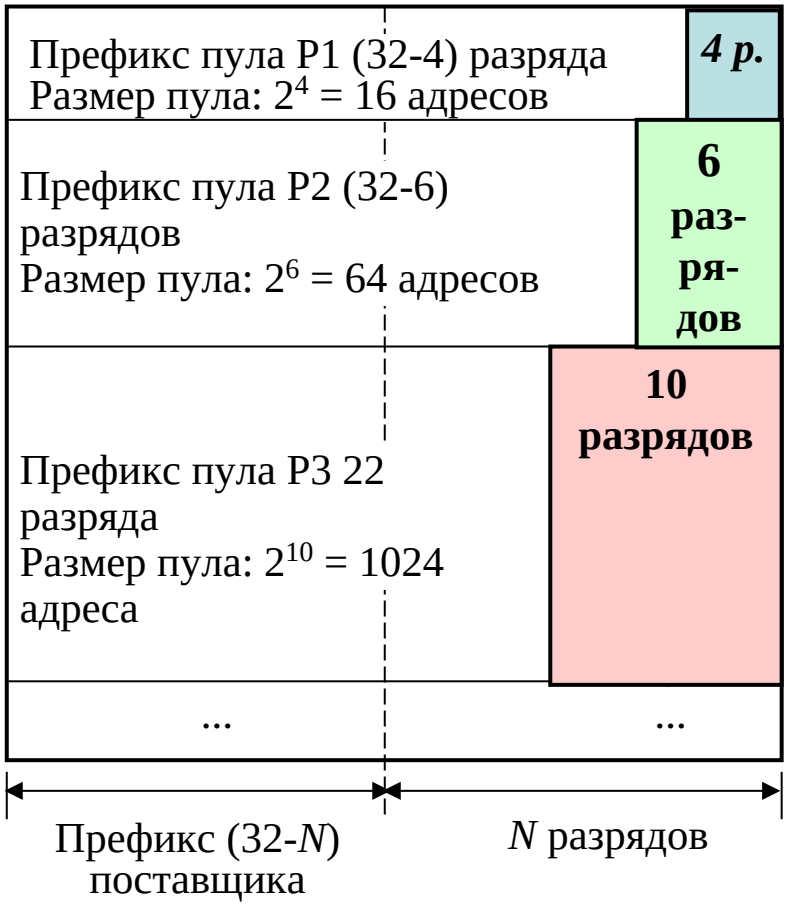
Использование масок для IP-адресов

IP-адрес: 126.65.32.5 соответствует адресу узла **0.65.32.5** в сети **126.0.0**.0
Маска: **255.192.0.0** (255.192.0.0/**10**)
В двоичном виде:
IP-адрес: **01111110.01000001.00100000.00000101** **126.65.32.5/10**
Маска: **11111111.11000000.00000000.00000000**
Тогда **адрес сети:** **01111110.01** или **126.64.0.0**
адрес узла: **000001.00100000.00000101** или **0.1.32.5**

Маски для стандартных классов:
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)

Технология бесклассовой междоменной маршрутизации

CIDR (Classless Inter-Domain Routing)



Первый и последний IP-адрес	***Префикс***	***Адресов***		***Маска***
		всего	***узлов***	
185.68.0.1/***28*** 185.68.0.14/***28***	185.68.0.***0000*** 185.68.0.0	16	***14***	255.255.255.240
185.68.1.1/***26*** 185.68.1.62/***26***	185.68.1.***00*** 185.68.1.0	64	***62***	255.255.255.192
185.68.1.65/***26*** 185.68.1.126/***26***	185.68.1.***01*** 185.68.1.64	64	***62***	
185.68.1.129/***26*** 185.68.1.190/***26***	185.68.1.***10*** 185.68.1.128	64	***62***	
185.68.1.193/***26*** 185.68.1.254/***26***	185.68.1.***11*** 185.68.1.292	64	***62***	
185.68.4.1/***22*** 185.68.7.254/***22***	185.68.***000001*** **185.68.4.0**	1024	***1022***	255.255.252.0

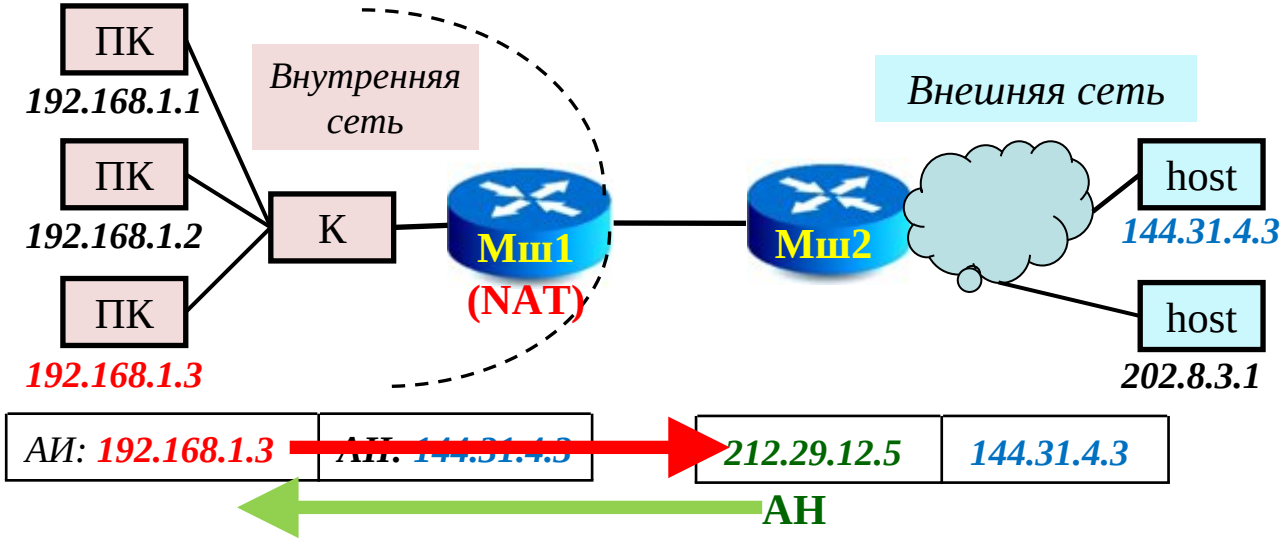
0000 – двоичные цифры

Технология NAT

NAT (Network Address Translation)

Основное назначение NAT –: решение проблемы ограниченного диапазона IP-адресов в IPv4.
Повышение безопасности сети за счет

- ограничения доступа извне к ресурсам внутренней сети при сохранении возможности выхода в публичную (внешнюю) сеть;
- сокрытия внутренних сервисов, хостов, серверов.



NAT-таблица Мш1	
Локальный	***Глобальный***
192.168.1.1	***212.29.12.3***
192.168.1.2	***212.29.12.4***
192.168.1.3	***212.29.12.5***

Локальный адрес	*Порт*	*Глобальный адрес*	*Назн. порт*
192.168.1.1	*1125*	212.29.12.1	*5141*
192.168.1.1	*1145*	212.29.12.1	*5142*
192.168.1.3	*1234*	212.29.12.1	*5143*

ТИПЫ NAT

Статический (Static) NAT: один локальный адрес – один глобальный адрес;
Динамический (Dynamic) NAT: локальный адрес – разные глобальные адреса;
Port Address Translation (PAT) или **NAT Overload** – сопоставление локальных и глобальных адресов с использованием портов.

Распределение IP-адресов

Способы распределения IP-адресов

Централизованное распределение

Главный орган регистрации глобальных адресов в Internet: **ICANN** – Internet Corporation for Assigned Names and Numbers

Региональные отделы

ARIN (Америка) | RIPE (Европа) | …

Поставщики услуг (провайдеры)

Клиенты

Автоматизированное распределение в сети (на основе протокола DHCP)

Протокол для автоматического назначения IP-адресов:
Dynamic Host Configuration Protocol (DHCP)
(1993 г.; RFC 2131)

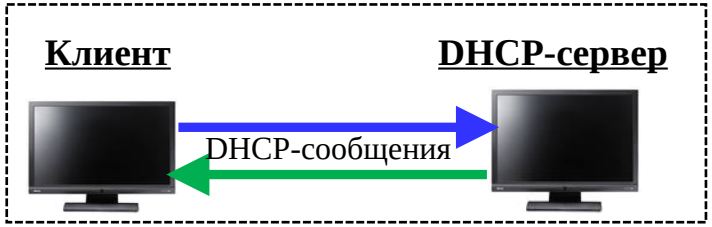
Способы назначения IP-адресов на основе протокола DHCP

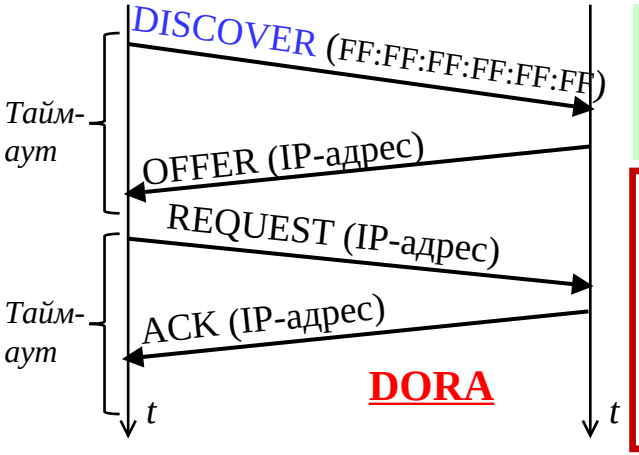
- Ручное статическое
- Автоматическое статическое
- Автоматическое динамическое

Дополнительные конфигурационные параметры (опции) DHCP-сервера:

- маска;
- IP-адрес маршрутизатора по умолчанию;
- IP-адрес сервера DNS;
- доменное имя компьютера и т.д.

Протокол DHCP

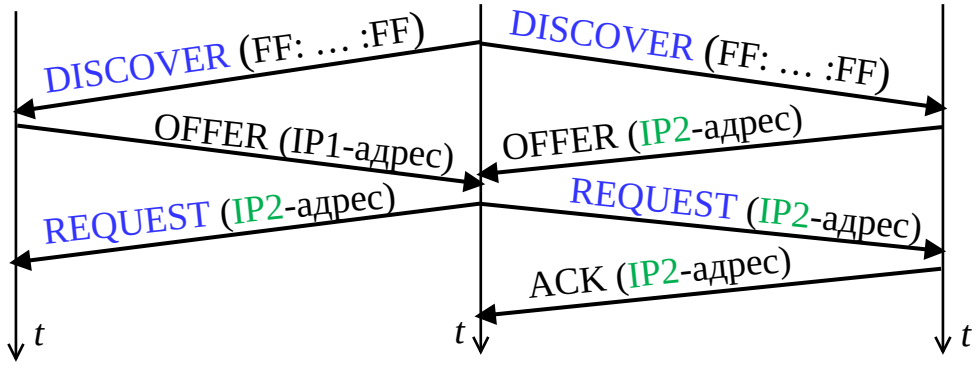




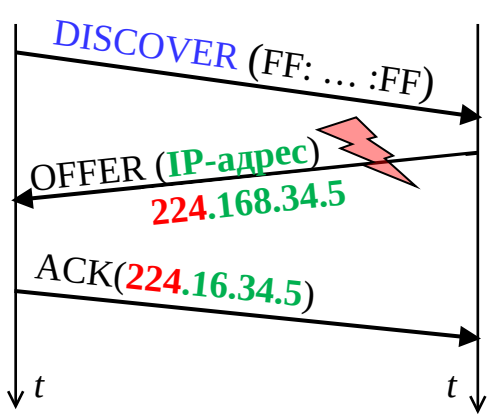
DORA

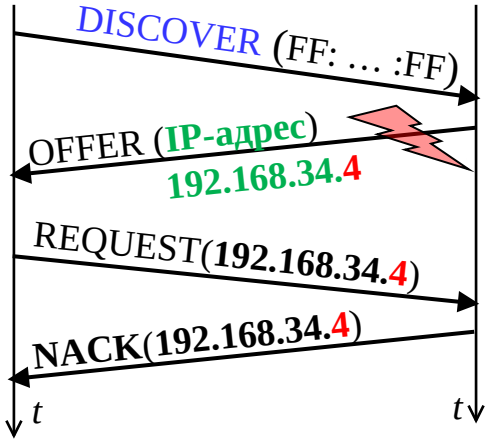
Время аренды (lease time)
REQUEST - ACK

Конфигурация маршрутизатора **DHCP Relay** (2 и более подсети)



Ошибка в IP-адресе при передаче





DHCP-сообщ.	*Назначение*	*Источн.*
DISCOVER	***Найти DHCP-сервер***	***Клиент***
OFFER	***Предложение IP-адреса***	***Сервер***
REQUEST	***Запрос IP-адреса***	***Клиент***
ACK	***Подтверждение IP-адреса или доп. параметров***	***Сервер***
NACK	***Запрет использования IP-адреса***	***Сервер***
RELEASE	***Освобождение IP-адреса***	***Клиент***
DECLINE	***Отказ от IP-адреса***	***Клиент***
INFORM		***Клиент***
FORCEREN		***Сервер***

ACK – **Ack**nowledgemente
NACK – Negative ACK

Протоколы ARP, InARP и RARP

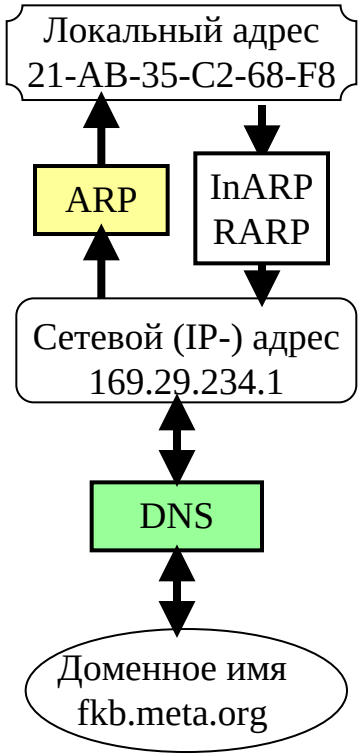
Протоколы разрешения адресов

ARP (Address Resolution Protocol)

InARP (Inverse ARP) *(FrameRelay, ATM)*

RARP (Reverse ARP)

DNS (Domain Name System)



ARP-таблица

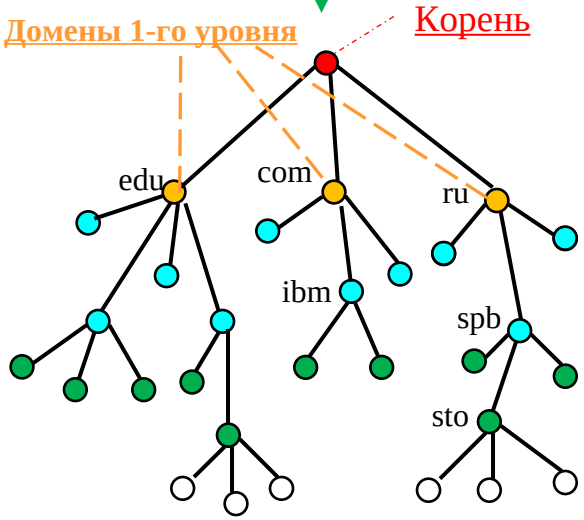
```
Интерфейс: 192.168.93.11 --- 0xf
  адрес в Интернете      Физический адрес      Тип
  192.168.93.104         f6-e2-1a-c1-55-a6     динамический
  192.168.93.214         a6-0e-39-94-28-2d     динамический
  192.168.93.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.22             01-00-5e-00-00-16     статический
```

Просмотр ARP-таблицы: **arp –a**

Добавление записи в ARP-таблицу: **arp –s <IP-адрес> <MAC-адрес>**

Форматы ARP-запроса (ответа)

Поле	Значение
«Тип сети» канального уровня	**1** (для Ethernet)
«Тип протокола» сетевого уровня	**2048** (=0800_{16} для IP)
«Длина локального адреса»	**6** (для Ethernet)
«Длина сетевого адреса»	**4** (для IP)
«Операция»	**1** (**2**) –запрос (-ответ)
«Локальный адрес отправителя»	**00-80-48-EB-6A-15**
«Сетевой адрес отправителя»	**195.67.8.9**
«Локальный адрес получателя»	**000000000000** (для ARP-запроса)
«Сетевой адрес получателя»	**195.67.8.12**



com, edu, gov, org, net, …

Формат DNS-таблицы

Доменное имя	IP-адрес
sota.park.org	213.45.7.12

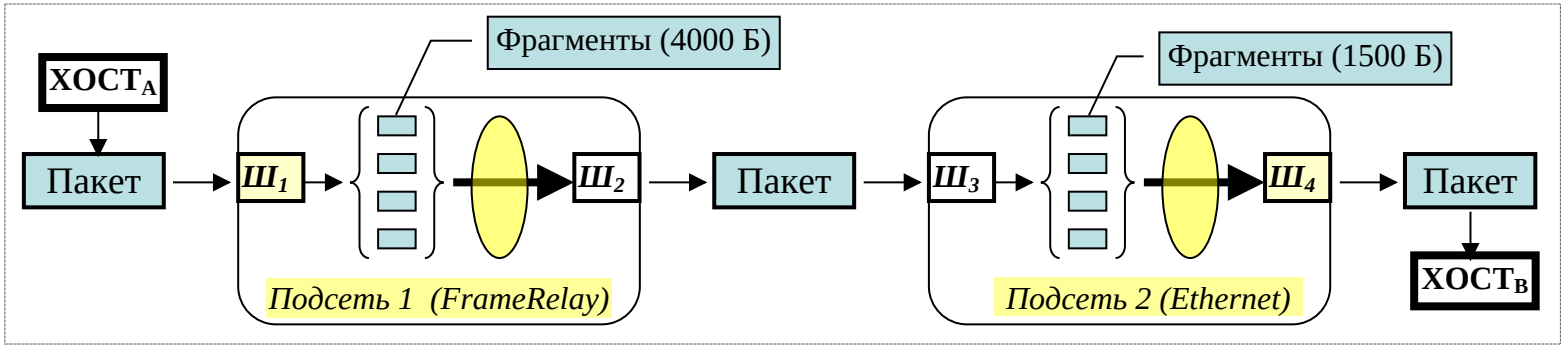
2.3. Фрагментация IP-пакетов

MTU (Maximum Transfer Unit) – максимальный размер поля данных:

от 48 байт (ATM) до 65515 байт (IP-пакеты)

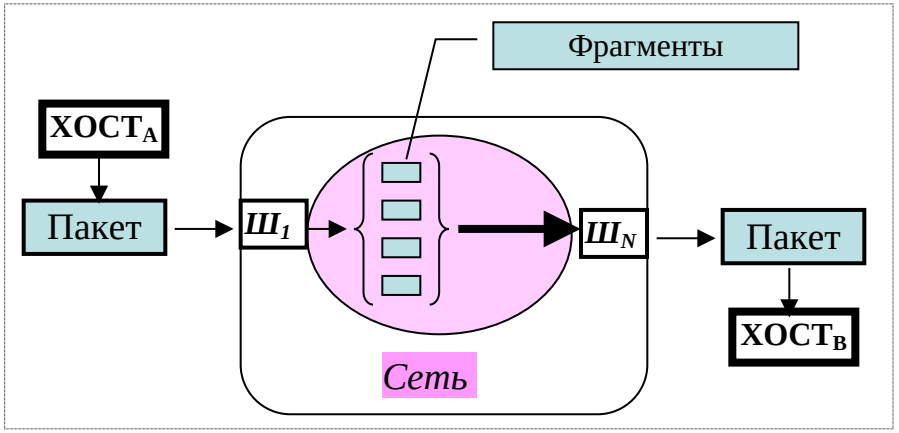
Стратегии фрагментации

- Прозрачная фрагментация
- Сквозная фрагментация



Параметры фрагментации:

- идентификатор пакета (ИП)
- признак конца пакета (ПК)
- смещение фрагмента (СФ)
- время жизни TTL (Time To Live)
- флаг MF (More Fragments)
- флаг DF (Do not Fragment)



Исходный пакет

ИП	СФ	ПК	Элементарные фрагменты (по 8 Байт)											
32	0	1	A	B	C	D	E	F	G	H	I	J	K	L

Фрагменты (по 40 Байт)

32	0	0	A	B	C	D	E
32	5	0	F	G	H	I	J
32	10	1	K	L			

2.4. Транспортные протоколы TCP/IP

Общие принципы

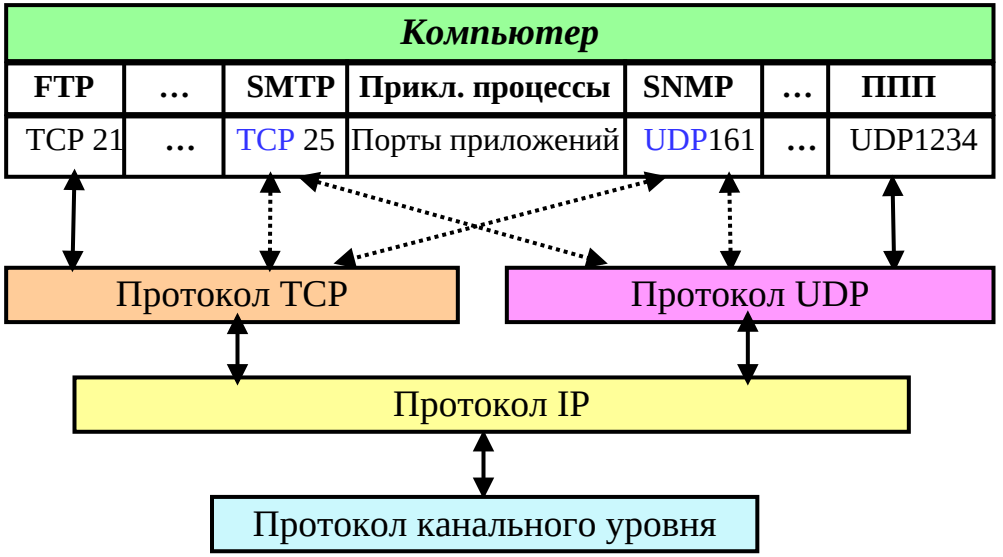
TCP (*Transmission Control Protocol*)
UDP (*User Datagram Protocol*)

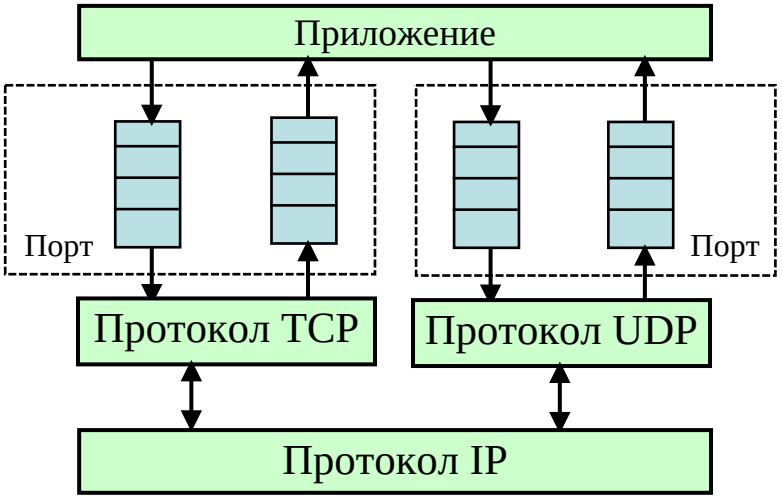
RDP (*Reliable Data Protocol*) – *надёжный протокол передачи данных* за счет **подтверждения доставки** пакетов, **повторной отправки** пакетов, **управления потоками** данных (среднее между TCP и UDP)

DCCP (*Datagram Congestion Control Protocol*) – отслеживание перегрузок в сети

SCTP (*Stream Control Transmission Protocol*) – протокол передачи с «управлением потоком»: **многопоточность**, **защита от DDoS атак**, поддержка **множественных интерфейсов**

QUIC («быстрый») - для соединения (подключений) веб-браузера Chrome к серверам Google





Способы присвоения порта приложению:

- ***Общеизвестные*** (системные) – номера от 0 до 1023, присвоенные централизованно общедоступным службам (приложениям): **FTP - 21, SMTP – 25, DNS – 53, HTTP – 80, SNMP – 161/162**.
- ***Зарегистрированные*** (пользовательские) – номера от 1024 до 49151.
- ***Динамические*** (частные) – номера от 49152 до 65535 выделяются по запросу от приложения из списка свободных номеров.

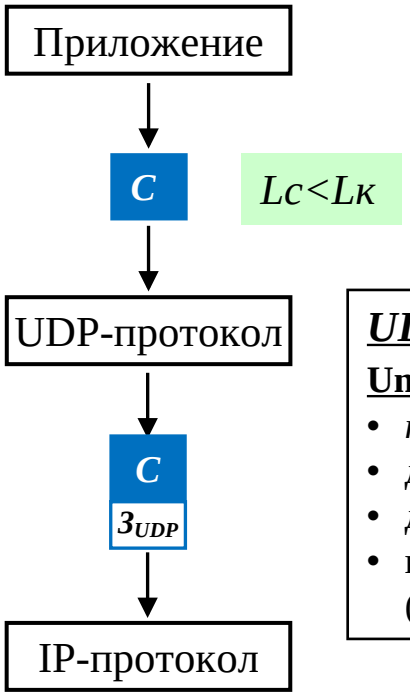
<Сокет>: <IP-адрес>, <номер порта>

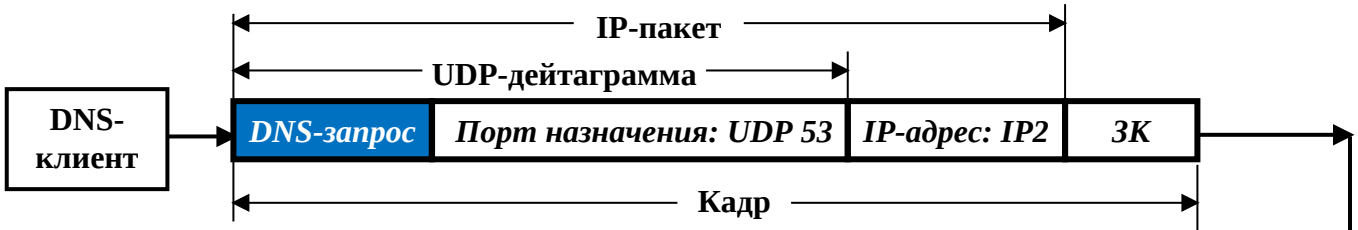
2.4. Транспортные протоколы TCP/IP

Протокол UDP

Формат заголовка UDP-дейтаграммы

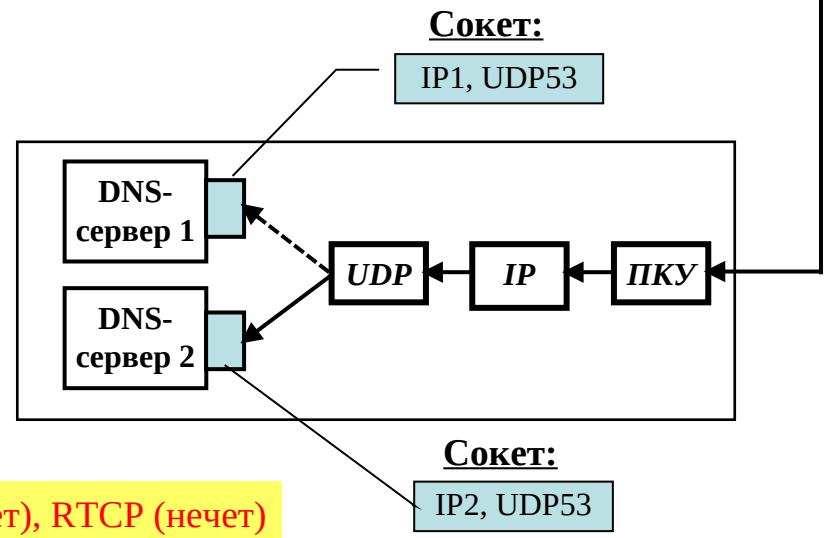
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Порт источника (Source Port)																Порт назначения (Destination Port)															
Длина UDP-дейтаграммы (Total length)																Контрольная сумма (Checksum)															





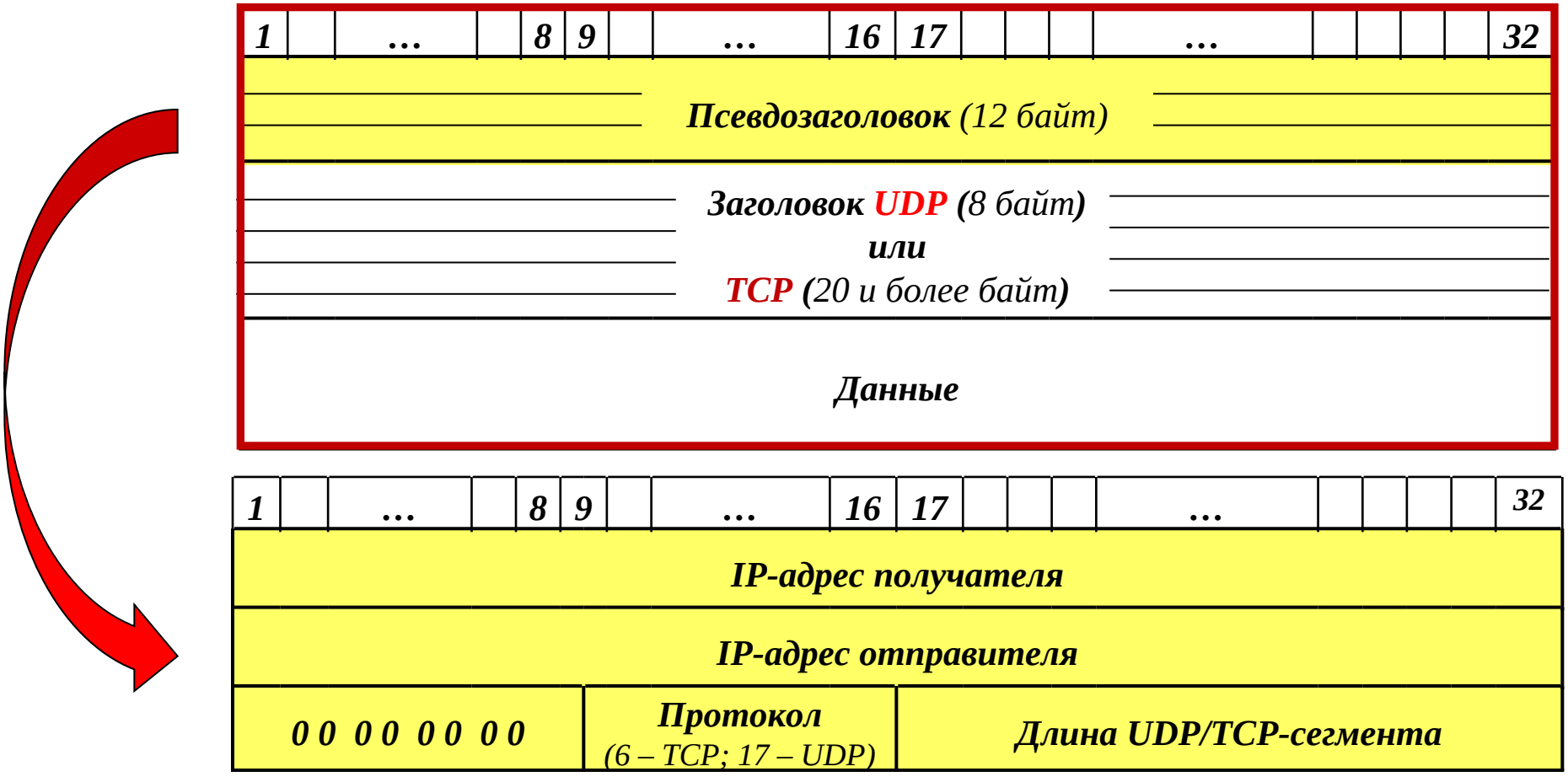
UDP (User Datagram Protocol / Unreliable Datagram Protocol):

- *ненадежная* доставка сообщений;
- доставка по возможности;
- доставка без гарантий;
- контроль ошибок без исправления (ошибочное сообщение отбрасывается).



DNS (UDP/53), DHCP (UDP/67, 68), SNMP (UDP/161, 162), RTP (чет), RTCP (нечет)

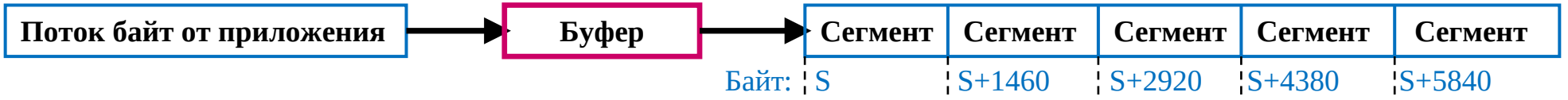
Псевдозаголовок протоколов UDP и TCP



Контрольная сумма UDP-дейтаграммы (TCP-сегмента) рассчитывается с учетом псевдозаголовка, который *не передается* по сети!

Протокол TCP: принципы реализации

1. ***Надежная передача*** за счет установления *логического соединения* (без потерь, ошибок и дублирования).
2. ***Согласование параметров***: а) **начальный порядковый номер байта** ISN; б) **максимальный размер сегмента** (*обычно* 1460 байт; *максимально* 65 495 байт); в) **максимальный объем принимаемых данных** (байт).
3. ***Неструктурированный поток байтов*** от протоколов более высокого уровня заносится в буфер, из которого для передачи на сетевой уровень ***вырезается сегмент***.

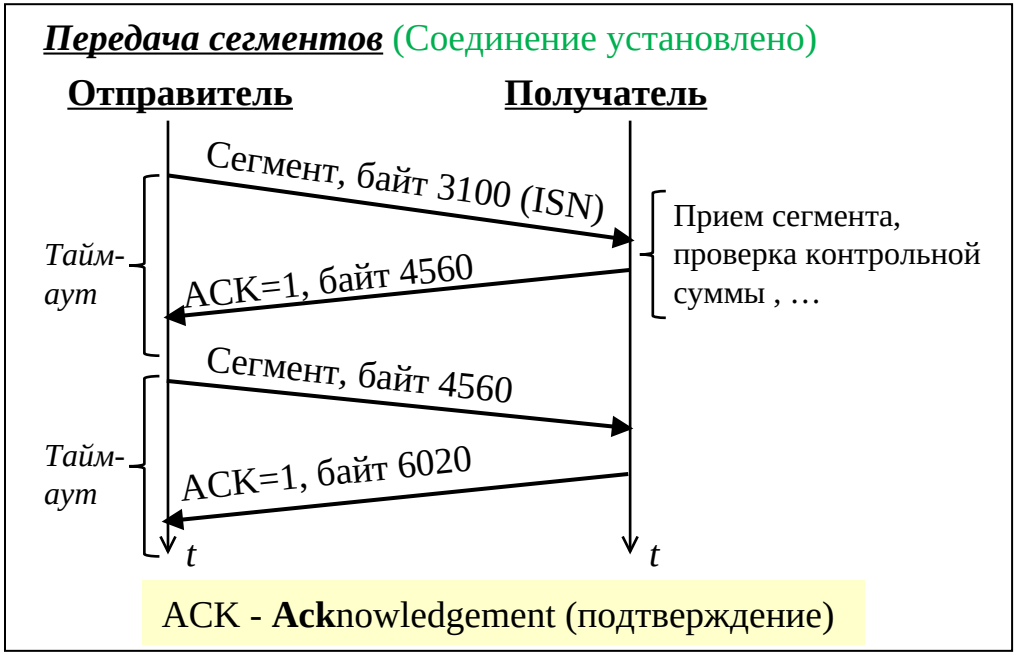


4. ***Дуплексная передача*** сегментов.
5. ***Скользящее окно*** *переменного* размера.
6. ***Механизм тайм-аута.***
7. ***Отрицательные квитанции*** не посылаются.
8. Номер подтверждения - порядковый номер ***ожидаемого байта*** (не сегмента!)**.**
9. ***Контроль ошибок***: контрольная сумма (**заголовок + данные + псевдозаголовок**) вычисляется в ***дополнительном коде*** для 16 разрядных слов.

S = ISN+1, ISN **(Initial Sequence Number)** – случайное число в интервале (0; 2^{32}).

Типы подтверждений:

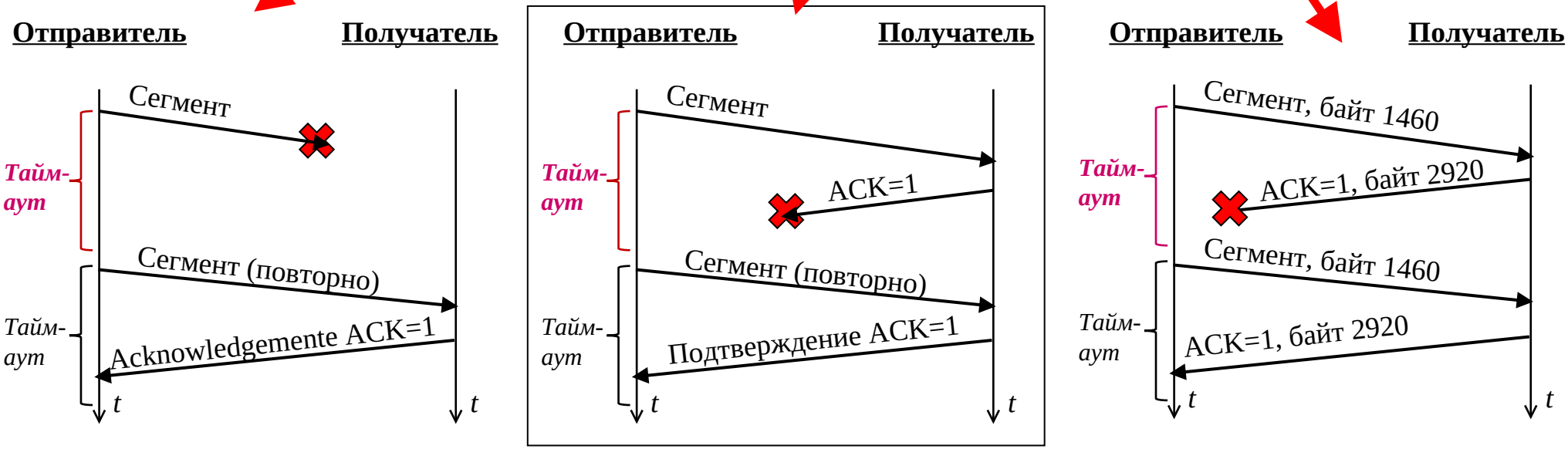
- ***кумулятивное*** (по умолчанию в TCP) – подтверждение приема **указанного байта** и всех предыдущих;
- ***выборочное*** – подтверждение **диапазона принятых байт** при большом размере окна (используется дополнительное поле заголовка TCP).



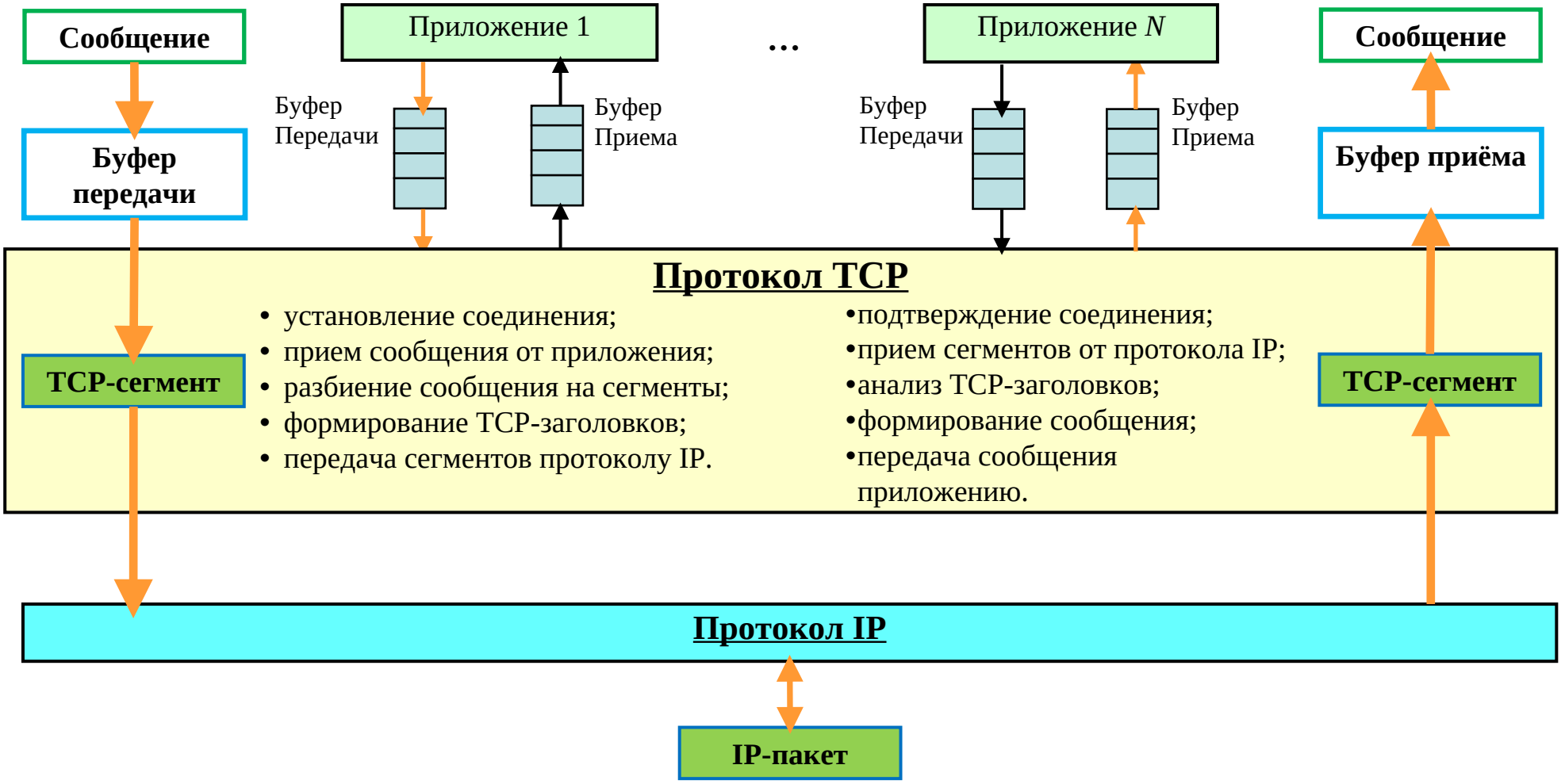
Протокол TCP: проблемы реализации

Возможные проблемы:

1. ***Сегмент*** или ***подтверждение*** могут быть *потеряны*, *искажены*, *продублированы*.
2. При фрагментации ***часть сегмента*** может быть потеряна.
3. Сегменты могут прибывать в узел назначения в ***произвольном порядке***, из-за чего подтверждение не может быть выслано, так как часть сегментов еще не получена.
4. Сегменты могут ***задержаться*** в сети дольше интервала тайм-аута, переданный повторно сегмент может: а) пройти *по другому маршруту*; б) быть *иначе фрагментирован*; в) попасть в *перегруженную сеть*.
5. ***Скорость*** отправителя может превышать возможности получателя (управление потоком).
6. Сеть (маршрутизаторы, каналы) может быть ***перегружена*** (*контроль и борьба с перегрузками*).



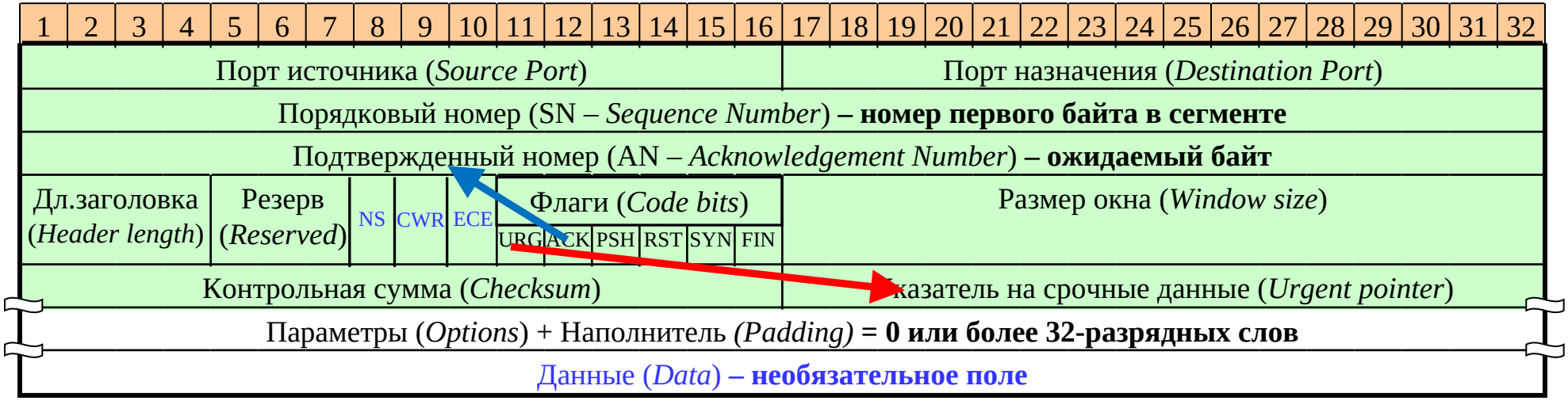
Протокол TCP: основные функции



Протокол TCP: формат заголовка TCP-сегмента

Логическое соединение: <сокет1> < сокет2> **<Сокет>: <IP-адрес>, <номер порта>**

Формат заголовка TCP-сегмента (1460 байт – 64 Кбайт)



Флаги или кодовые биты (code bits):

URG = 1 – срочные данные (используется поле «Указатель на срочные данные») (*urgent*)

ACK = 1 – квитанция (используется поле «Подтвержденный номер ») (*acknowledgement*)

PSH = 1 – PUSH-флаг – запрос на отправку данных приложению без ожидания заполнения буфера и отправка подтверждения

RST = 1 – сброс соединения / отказ от неверного сегмента / отказ на запрос о создании соединения (*reset*)

SYN = 1 – установка соединения (*syncing*)

FIN = 1 – завершение (разрыв) соединения передающей стороной (*finish*)

FTP (20-дан., 21-ком.), DNS (53), ***SMTP (25)***, ***POP3 (110)***, ***IMAP (143)***, TELNET (23), BGP (179), HTTP (80), PPTP

Протокол TCP: флаги для управления перегрузкой

Длина заголовка	Резерв			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Размер окна
	-	-	-										

Для ***управления перегрузкой*** в поле «Резерв (*разряды 8,9,10*)» добавлены **3 однобитовых флага**:

- **ECE** – «ECN-Echo» – в зависимости от значения флага SYN:
  - при установлении соединения (SYN=1) указывает, что **отправитель** поддерживает технологию ***явного уведомления о перегрузке* (*Explicit Congestion Notification*, ECN)**;
  - при передаче данных (SYN=0) **получатель** указывает отправителю о перегрузке в сети;
- **CWR** (*Congestion Window Reduced*) – «окно перегрузки уменьшено» – **отправитель** подтверждает получение сегмента с флажком ECE=1 от узла-получателя и включение механизма управления перегрузкой (Congestion Control);
- **NS** (*Nonce Sum*) – «одноразовая сумма» – для улучшения работы механизма **ECN**: защиты от ошибок реализации и от преднамеренных злоупотреблений (*ECN - nonce*).

Параметры в заголовке TCP (необязательные):

1. **MSS** (Maximum Segment Size) - **максимальный размер сегмента** (для Ethernet - 1460 байт), согласовывается отправителем и получателем при установке соединения.
2. **Масштаб окна** - позволяет увеличить размер окна до 1 ГБ (вместо 65535 байт).
3. **Выборочное подтверждение** - подтверждение диапазона принятых байт, а не всех данных, если потерян всего лишь один сегмент или небольшая часть в большом потоке данных.

Протокол TCP: вычисление контрольной суммы

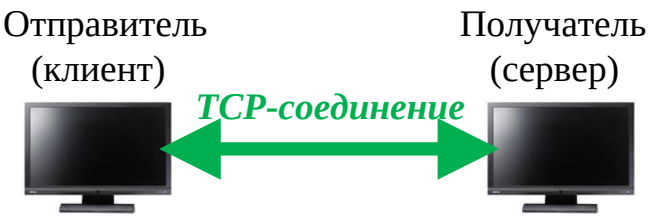
Алгоритм вычисления контрольной суммы

1. Поле данных – чётное число байтов (в противном случае дополняется нулевой байт).
2. TCP-сегмент (включая псевдозаголовок) – совокупность 16-разрядных двоичных чисел.
3. Сложение с переносом, если сумма более 16 разрядов.
4. Поразрядное инвертирование – контрольная сумма.

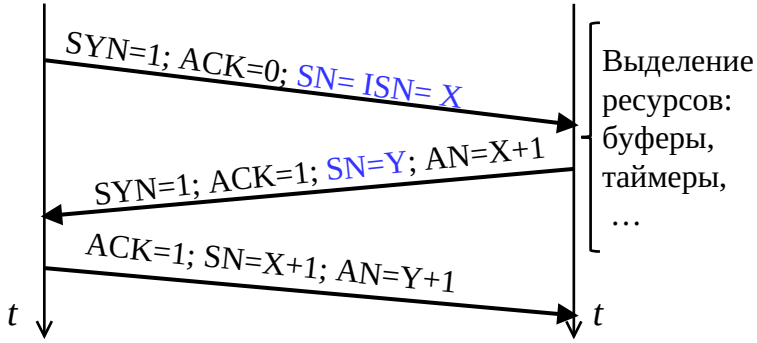
Пример. Длина TCP-сегмента – 4 полубайта (***нибл***): 1110 1001 1000 1011
Сложение в двоичном коде: 1110+1001+1000+1011=101010 1010+0010=**1100**
Контрольная сумма: **0011**
На приемной стороне: 1110+1001+1000+1011+**0011** = 111101 1101+0011= ***0000***

Пусть в процессе передачи в первом полубайте исказился первый бит: **0**110.
На приемной стороне: складываются все полубайты, включая контрольную сумму:
0110+1001+1000+1011=100010
0010+0010+ **0011** = 0111 (ошибка).

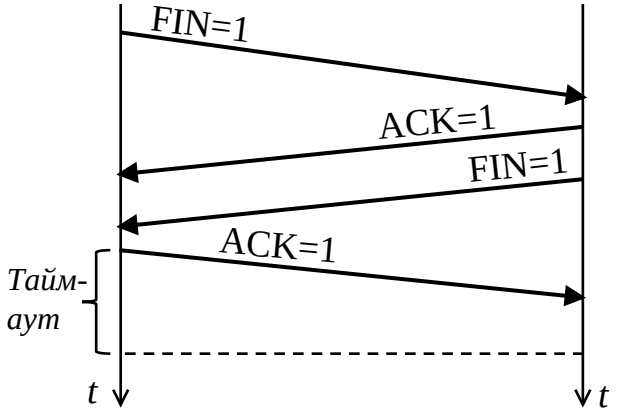
Протокол TCP: установление и разрыв соединения



Установление соединения
(состояние ESTABLISHED)



Разрыв соединения

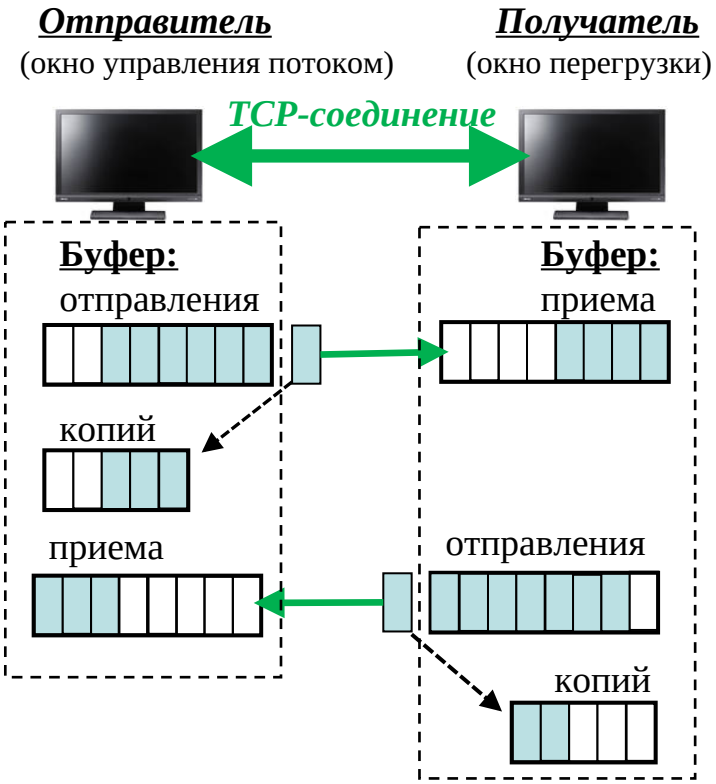


Этапы передачи данных в TCP:
- установление соединения: «*трехкратное рукопожатие*»:
  К) SYN=1; ***С***) SYN=1 и ACK=1; ***К***) ACK=1;
- передача данных;
- разрыв соединения (FIN=1 или RST=1).

При установлении соединения:
- необходимо убедиться, что отправитель и получатель готовы передавать данные друг другу;
- договориться о параметрах соединения: **максимальный размер сегмента**; **начальный размер окна**; **начальный порядковый номер байта** (ISN – *Initial Sequence Number*) и др.

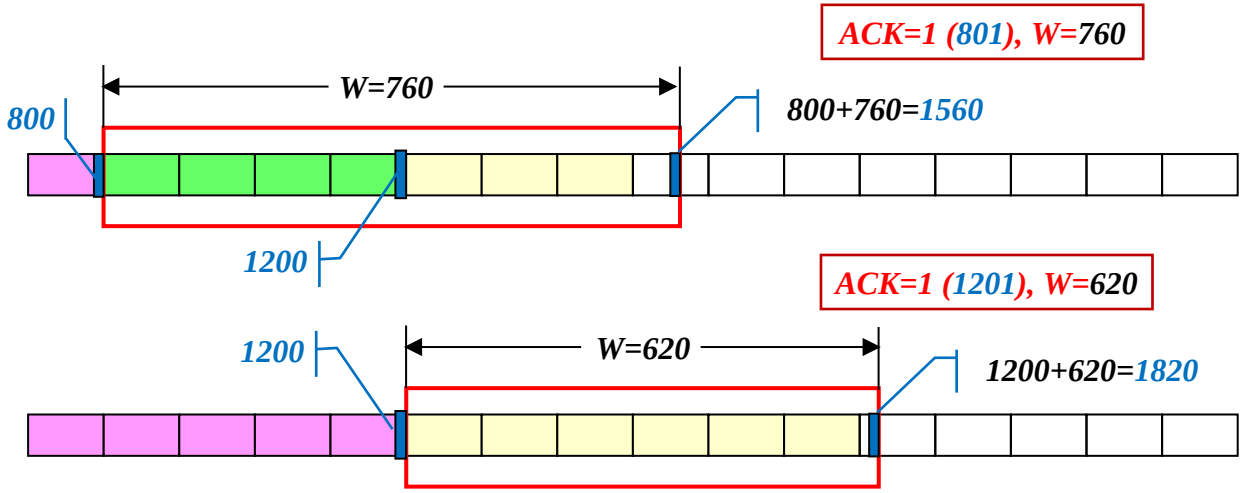
Разрыв соединения:
- *односторонний* - одна сторона прекращает передачу (FIN), но может принимать данные;
- *одновременный* - обе стороны разорвали соединение (FIN / FIN);
- *принудительный* – при возникновении нестандартной ситуации (RST).

Протокол TCP: перегрузка и управление потоком



Причины перегрузки:
- заполнен буфер приёма узла-получателя;
- перегружены маршрутизаторы и каналы связи на пути передачи.

Методы предотвращения перегрузки узла-получателя:
- выбор *величины тайм-аута*;
- выбор и адаптивное изменение *размера окна, диктуемого узлом-получателем сегментов*.



Признаки перегрузки:
- потеря сегментов;
- увеличенная задержка сегментов;
- сигнал от маршрутизатора о перегрузке.

Размер окна устанавливается как минимальное значение из размера **окна управления потоком** *(получателем)* и размера **окна перегрузки** *(рассчитанный/уменьшенный при возникновении перегрузки)*.

Протокол TCP: управление перегрузкой

Методы управления перегрузкой сети (маршрутизаторов) реализуются путем выбора и адаптивного изменения размера окна с учетом загруженности сети:

- **AIMD** (*Additive Increase / Multiplicative Decrease*) - метод аддитивного увеличения, мультипликативного уменьшения (на медленных каналах);
- «**медленный старт**» с **AIMD в протоколе TCP.**

Метод AIMD:

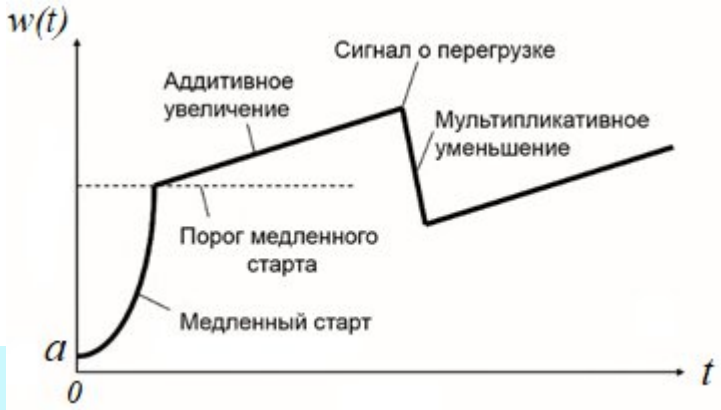
$$w(t+1) = \begin{cases} w(t) + a, & \text{если нет перегрузки;} \\ w(t) * b, & \text{если есть перегрузка,} \end{cases}$$

где $t = 0, 1, 2, \ldots$; $w(0) = 0$; a = MSS – максимальный размер сегмента (по умолчанию MSS=536; MSS=1460 для сети Ethernet); $b = 0{,}5$.

Метод «медленный старт» с AIMD:

$$w(t+1) = \begin{cases} 2w(t), & \text{если } w(t) < \text{порога медленного старта;} \\ w(t) + a, & \text{если } w(t) \geq \text{порога медленного старта;} \\ w(t) * b, & \text{если есть перегрузка,} \end{cases}$$

где $w(0) = a$; a = MSS; $b = 0{,}5$.



Системный администратор может задать **максимальный размер окна** и **добавляемую константу**.

Протокол TCP: сигналы о перегрузке

Признаки перегрузки (сигналы о перегрузке) :
1) потеря сегмента;
2) задержка сегмента;
3) сигнал о перегрузке от маршрутизатора.

1. Потеря сегмента (из-за перегрузки *сети*, но не каналов связи).

Перегрузка не предотвращается, поскольку уже произошла

Возможность возникновения новой перегрузки когда все отправители после перегрузки и уменьшения размера окна начинают практически одновременно передавать сегменты

2. Задержка сегмента (отслеживание времени RTT - Round Trip Time).

Необъективный показатель - задержка сегментов может быть не связана с перегрузкой сети

Несправедливое распределение пропускной способности каналов связи – другие компьютеры, использующие показатель «потеря сегмента», увеличивают размер окна

Совместное использование двух показателей: **«задержка сегмента»** и **«потеря сегмента»** (реализовано в протоколе Compound TCP фирмы Microsoft).

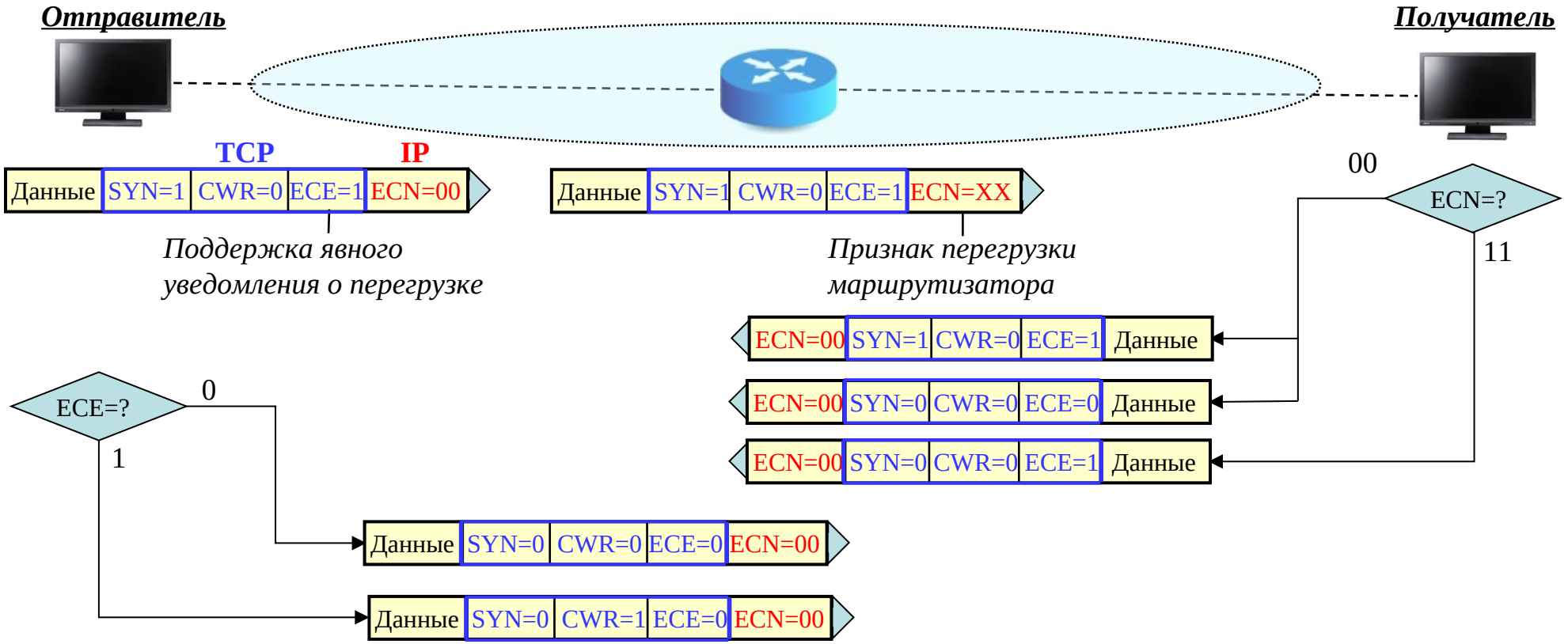
3. Сигнал о перегрузке от маршрутизатора (маршрутизатор должен поддерживать отправку сигналов).

Неявная передача сигнала - маршрутизатор начинает отбрасывать пакеты до того, как буфер заполнится (технология **RED –** Random Early Detection)

Явная передача сигнала - маршрутизатор сообщает отправителю о перегрузке (технология **ECN** - Explicit Congestion Notification, встроенная в протоколы TCP и IP)

ECN – технология явного уведомления о перегрузке

ECN (Explicit Congestion Notification)



ECN – явное уведомление о перегрузке: 00 и 11 (перегрузка) – в **заголовке IP-пакета**.

ECE – «ECN-Echo»: 1) поддерживает ECN (**отправитель** при SYN=1); 2) перегрузка в сети (**получатель** при SYN=0).

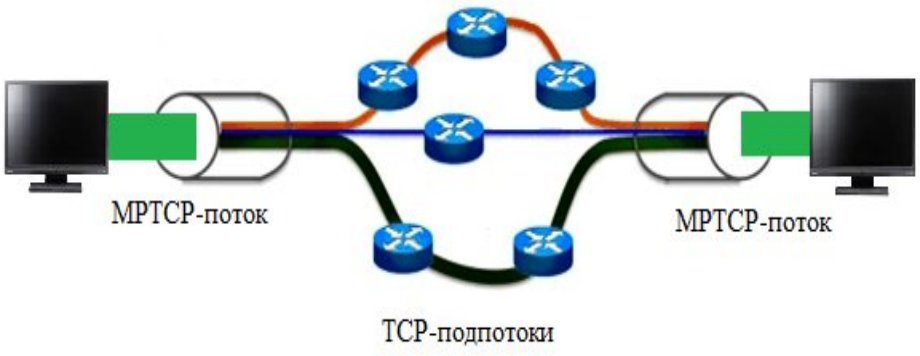
CWR (*Congestion Window Reduced*) – **отправитель**: подтверждение «окно перегрузки уменьшено».

Сравнение TCP и UDP

Показатель	TCP	UDP
Размер заголовка	20 – 60 байт	8 байт
PDU	Сегмент	Дейтаграмма
Соединение	устанавливается дуплексное соединение	передача без установления соединения
Контроль ошибок	ошибочный сегмент посылается повторно	ошибочная дейтаграмма отбрасывается
Последовательность доставки	есть	не контролируется
Упорядоченность доставки	есть	нет
Контроль и управление перегрузками	реализован	нет
Накладные расходы	есть на установление соединения	нет
Приложения	FTP, HTTP, SMTP	DNS, SNMP, TFTP, DHCP

Многопутевой TCP - Multipath TCP (MPTCP)

MPTCP – технология передачи данных по протоколу TCP одновременно по нескольким каналам связи с целью *увеличения пропускной способности* и *надежности* за счет максимальной загрузки ресурсов компьютерной сети и увеличения избыточности (2013 год, спецификация RFC 6824).
При многопутевом TCP соединение устанавливается *между двумя хостами*, а не интерфейсами, как в TCP.



В MPTCP по каждому каналу (пути) создается TCP-соединение – TCP-***подпоток*** (sub-flow).

Основные операции протокола MPTCP:

- ***добавление/удаление пути*** (при перегрузках);
- ***обеспечение совместимости с устаревшим оборудованием*** TCP (например, с брандмауэрами, которые могут автоматически отклонять TCP-соединения, если порядковый номер не является последовательным);
- ***справедливый контроль перегрузки*** между разными соединениями и разными хостами (особенно с теми, которые не поддерживают MPTCP).

Новые механизмы:

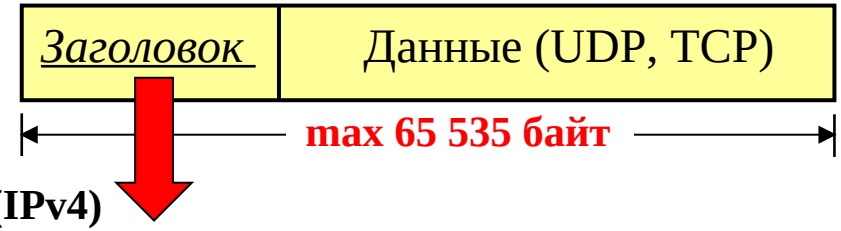
1. ***Система подпотока*** для организации нескольких TCP-соединений путем *добавления* или *удаления подпотоков*.
2. ***Опция MPTCP DSS*** (*Data Sequence Signal* – сигнал последовательности данных), содержащая *порядковый номер данных* и *номер подтверждения*, что позволяет получать данные из нескольких подпотоков *в исходном порядке*.
3. ***Модифицированный протокол повторной передачи***, обеспечивающий *контроль и управление перегрузкой*, а также *повышенную надежность*, не проявляя при этом несправедливости к TCP-соединениям с одним путем, которые могут конкурировать на каком-то пути.

2.5. Коммуникационный протокол IPv4

Протокол IP специфицирует три основных элемента:

- ❑ блок данных, с которым работает протокол (пакет IP);
- ❑ механизмы передачи пакетов;
- ❑ способы обработки конфликтных ситуаций.

Пакет IP



Формат заголовка (IPv4)

Биты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Номер версии				**Длина заголовка**				**Тип сервиса (DS-байт)**								**Общая длина** (байт)															
									PR			D	T	R	ECN																
	Идентификатор пакета																**Флаги**			**Смещение фрагмента** (кратно 8 байтам)											
																	-	DF	MF													
	Время жизни (TTL – Time To Live)																**Протокол** (6 - TCP, 17 - UDP, 1 - ICMP)															
																	Контрольная сумма заголовка (в дополнительном коде)															
	IP-адрес источника																															
	IP-адрес назначения																															
	Параметры																															

По умолчанию:
TTL = 64 (Linux)
128 (Windows)

D=1 (*Delay* – задержка);
T=1 (Throughput – пропускная способность);
R=1 (Reliability – надежность)

DF (Do not Fragment – не фрагментировать);
MF (More Fragments – больше фрагментов)

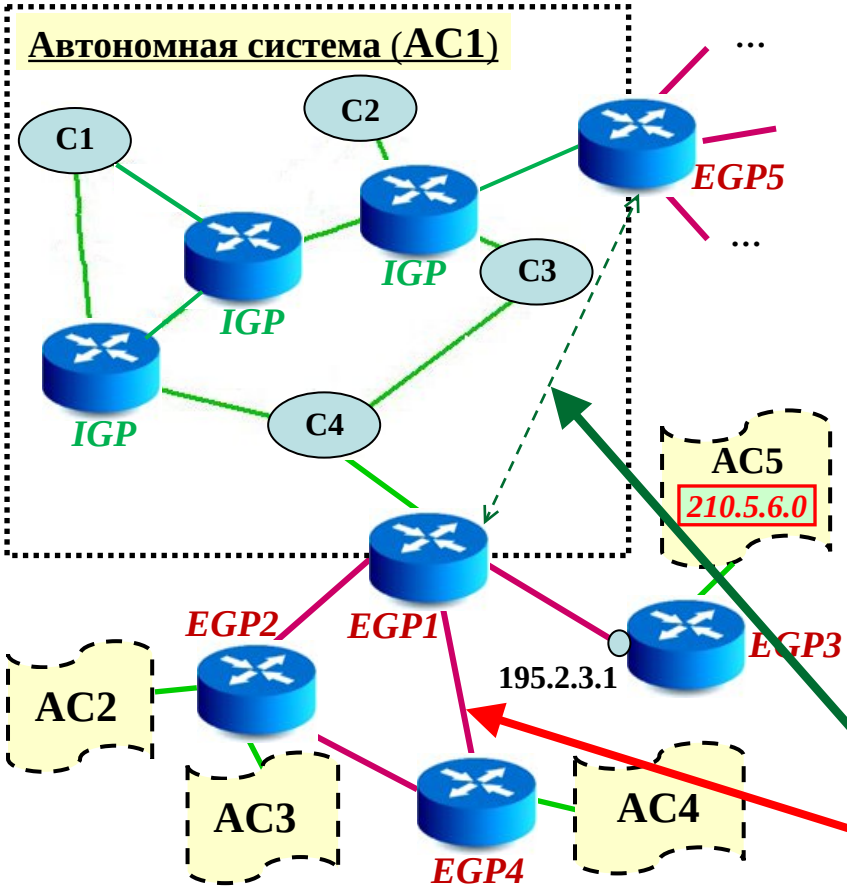
DS-байт (разряды 14-15) – ECN (*Explicit Congestion Notification)* – явное уведомление о перегрузке: 00 и 11 (перегрузка)

2.6. Протоколы маршрутизации

Методы маршрутизации

Классификация методов маршрутизации

- статические (фиксированные)
- динамические (адаптивные)



Протоколы динамической маршрутизации

Внешней маршрутизации EGP (Exterior Gateway Protocol)	Внутренней маршрутизации IGP (Interior Gateway Protocol)
	RIP, OSPF, IS-IS, ES-IS

BGP (Border Gateway Protocol):

- UPDATE-сообщения (*триггерные*);
- указываются номера АС;
- быстрая стабилизация;
- мало служебной информации;
- использует протокол TCP.

Реализации протокола:
iBGP – Interior BGP
eBGP – Exterior BGP

IS - Intermediate System
ES - End System
OSPF *– Open Shortest Path First*
RIP *– Routing Information Protocol*

№AS	*Router*	*Net/Mask*
AC5	*195.2.3.1*	*210.5.6.0/24*

2.6. Протоколы маршрутизации

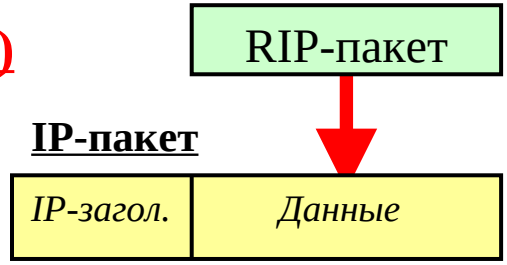
Протоколы внутренней маршрутизации

Классификация протоколов внутренней маршрутизации

типа ***DVA*** *(Distance Vector Algorithm)*	типа ***LSA*** *(Link-State Algorithm)*
RIP (*Routing Information Protocol*) – протокол маршрутной информации (1969 г.)	**OSPF** (*Open Shortest Path First*) - алгоритм предпочтения кратчайшего пути (1988 г.)

Протокол RIP (*Routing Information Protocol*)

1. Каждые 30 с - широковещательное сообщение : (***V, D***), где ***V*** - адрес доступной сети (вектор); ***D*** – расстояние до этой сети (дистанция).
2. Метрика RIP - длина вектора в ***хопах*** (ограничение – 15 транзитных участков; 16 – «бесконечно большая метрика»).



Формат RIP-пакета

Биты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Команда (1/2) (Command)								**Версия** (Version)								**Номер автономной системы (0)** (Routing Domain)															
	Запись маршрутной информации (от 1 до 25) (RIP Entry)																															

- **Command:** 1 – request; 2 – response;
- **Version:** 1 (1969 г.) или 2 (1994 г., дополнительная маршрутная информация для обеспечения высокого уровня безопасности);
- **Routing Domain:** 0 (не используется);
- **RIP Entry:** 1) тип адреса (2 – IP); 2) IP-адрес назначения (сети или хоста); 3) *маска подсети*; 4) метрика.

Недостатки протокола RIP:

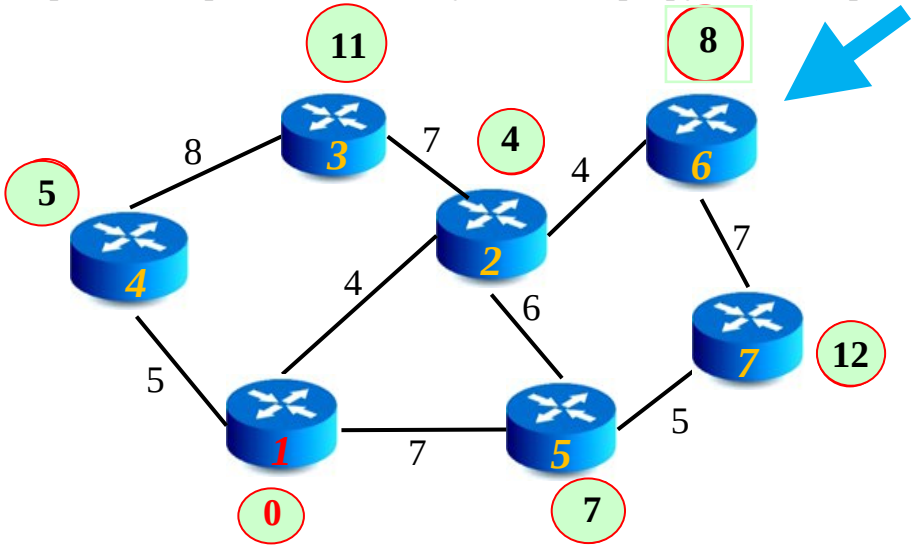
- медленная стабилизация маршрутов;
- большая загрузка сети таблицами «вектор-длина»;
- для небольших сетей (до 15 хопов).

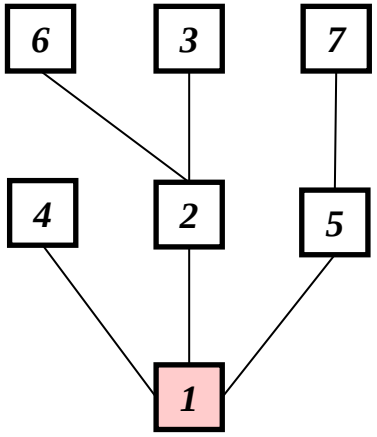
2.6. Протоколы маршрутизации

Протокол OSPF

OSPF (*Open Shortest Path First*)

Алгоритм SPF (Shortest Path First - «выбор кратчайшего пути») строит кратчайший путь к каждой сети в виде **дерева**, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям (маршрутизаторам). Процесс определения наилучшего маршрута (конвергенция) реализуется с использованием ***алгоритма Дейкстры***.





АН	Мш	Метрика	Мш альт.	Метрика
2	2	4	5	13
3	2	11	4	13
4	4	5	2	19
5	5	7	2	10
6	2	8	5	17
7	5	12	2	15

Поле «**Протокол**» для OSPF = **89**

Hello-пакет - установление и поддержание связей с соседними Мш
Пакет Database Description - содержание базы данных состояния каналов
Пакет Link State Request - запрос части базы данных соседнего Мш
Пакет Link State Update - рассылка объявлений о состоянии каналов
Link State Acknowledgment - подтверждение получения пакета Link State Update

Протокол OSPF

Типы сетей, поддерживаемые протоколом OSPF:

- широковещательные сети с множественным доступом (***Ethernet***, ***Token Ring***);
- точка-точка (***коммутируемый доступ***);
- нешироковещательные сети с множественным доступом (***Frame relay***).

Алгоритм реализации:

1. По умолчанию каждые 10 с – для широковещательных сетей и сетей точка-точка или 30 с – для нешироковещательных сетей с множественным доступом посылается широковещательное сообщение - **hello-пакет**.
2. Ожидание ответа.
3. Есть ответ – «канал активный».
4. Нет ответа – через 5 с повторный запрос.
5. Если нет ответа в течение 4-х кратного интервала посылки (40 с или 120 с) – канал считается «неактивным» и маршрутизатор распространяет соответствующую информацию всем остальным маршрутизаторам.

Метрика протокола OSPF
–стоимость (cost) :

$$M_{OSPF} = K / C_{KC},$$

где C_{KC} – пропускная способность КС;

K – коэффициент, равный максимальной пропускной способности (по умолчанию $K=10^8$);

M_{OSPF} – целое число: $M_{OSPFmin} = 1$.

Для составного соединения из n КС:

$$M_{OSPF} = \sum_{i=1}^{n} M_i,$$

где M_i - стоимость i-го КС ($i = 1,\ldots,n$).

Дополнительные возможности:

- маршрутизация в соответствии с *типом и классом обслуживания*;
- учет *приоритетов*;
- *равномерное распределение нагрузки* между альтернативными путями;
- *аутентификация* маршрутов;
- создание *виртуального канала* между маршрутизаторами, соединенными через транзитную сеть.

Преимущества OSPF по сравнению с RIP:

- более высокая скорость сходимости;
- поддержка сетевых масок;
- более эффективное использование пропускной способности сети за счет построения дерева кратчайших путей.

2.7. Протокол межсетевых управляющих сообщений ICMP

Назначение ICMP (Internet Control Message Protocol): формирование *диагностических* сообщений узлу-источнику об ошибках и *информационных* сообщений типа «запрос-ответ» в процессе мониторинга сети.

Формат ICMP-сообщения

Биты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Тип (Type)								**Код** (Kod)								**Контрольная сумма** (Check Sum)															
	Служебная информация (зависит от типа и кода)																															
	Поле данных ICMP (фрагмент пакета с ошибкой)																															

Тип	*Код*	*Содержание сообщения*
3	***0***	***Сеть не достижима***
	1	***Узел не достижим***
	2	***Протокол не достижим***
	3	***Порт не достижим***
	4	***Ошибка фрагментации***
	5	***Ошибка в маршруте источника***
	6	***Сеть назначения не известна***
	…	
11	***0***	***Время жизни пакета (TTL) истекло при передаче***
	1	***Время жизни пакета истекло при сборке фрагментов***
12	***1***	***Отсутствует требуемая опция***
	2	***Некорректная длина***

IP-пакет

Поле «**Протокол**» для ICMP = **1**

Особенности протокола ICMP:

1. Используется для передачи данных на **сетевом уровне OSI-модели** *без гарантии доставки*.
2. При потере или ошибках в ICMP-сообщении *новое сообщение не генерируется*.
3. ICMP-сообщения не генерируются в ответ на IP-пакеты *с широковещательным или групповым адресом*, чтобы не вызывать перегрузку в сети («широковещательный шторм»).
4. При повреждении фрагментов IP-пакета ICMP-сообщение об ошибке формируется и отправляется сразу после получения первого повреждённого фрагмента, при этом отправитель повторит передачу всего IP-пакета.

Применение ICMP

Утилита **ping:** проверка доступности компьютера или сервера в сети

```
C:\Users\ersin>ping ifmo.ru

Обмен пакетами с ifmo.ru [77.234.204.10] с 32 байтами данных:
Ответ от 77.234.204.10: число байт=32 время=40мс TTL=52
Ответ от 77.234.204.10: число байт=32 время=46мс TTL=52
Ответ от 77.234.204.10: число байт=32 время=37мс TTL=52
Ответ от 77.234.204.10: число байт=32 время=66мс TTL=52

Статистика Ping для 77.234.204.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 37мсек, Максимальное = 66 мсек, Среднее = 47 мсек
```

Тип	*Код*	*ICMP-сообщение*
8	*0*	*Эхо-запрос (обычно 64 байт)*
0	*0*	*Эхо-ответ*

По умолчанию:

- 4 эхо-запроса – 4 эхо-ответа, содержащие некоторую диагностическую информацию.

Утилита **tracert (traceroute):** определение маршрута от отправителя к получателю

По умолчанию:

- ICMP-пакетов к узлу – 3;
- хопов – 30;
- интервал ожидания – 4 с.

Причины превышения интервала ожидания от узла:

- узел не принимает ICMP-пакеты;
- нет связи со следующим узлом;
- не указан маршрут к данному узлу на предыдущем маршрутизаторе.

```
C:\Users\ersac>tracert 10.226.8.1

Трассировка маршрута к 10.226.8.1 с максимальным числом прыжков 30

  1     *        *        *     Превышен интервал ожидания для запроса.
  2    44 ms   141 ms   208 ms  10.255.128.0
  3    51 ms    41 ms    29 ms  10.3.246.81
  4    61 ms    48 ms    54 ms  10.226.8.1

Трассировка завершена.
```

2.8. Коммуникационный протокол IPv6

Цели:

- *создание масштабируемой системы адресации*;
- уменьшение размера таблиц маршрутизации и, как следствие, времени обработки пакетов в маршрутизаторах;
- предоставление гарантий качества транспортных услуг для неоднородного трафика;
- более надёжное обеспечение безопасности;
- возможность развития протокола в будущем;
- *возможность сосуществования старого (IPv4) и нового (IPv6) протоколов*.

Особенности протокола IPv6 :

1) длина IP-адреса - 16 байт (**10^{38} *адресов***);

2) упрощенная *структура заголовка* (8 полей и 13 в IPv4);
меньше *размер таблиц маршрутизации*;
фрагментация – в конечных узлах;
маршрутизация от источника;

3) улучшена поддержка необязательных параметров (ускоряется обработка пакетов в маршрутизаторах за счёт пропуска не относящихся к ним параметров);

4) обязательная поддержка шифрования – защищенный протокол IP (IPSec – Security Internet Protocol);

5) предусмотрена возможность расширения типов (классов) предоставляемых услуг;

6) разработаны способы межсетевого взаимодействия, обеспечивающие совместимость протоколов IPv4 и IPv6.

Адресация

Типы адресов IPv6

Индивидуальный адрес (unicast)

Групповой адрес (multicast)

Адрес произвольной рассылки (anycast) *(для маршрутизаторов)*

Глобальный агрегируемый уникальный адрес:

3	13	8	24	16	64 бит
FP	**TLA**		**NLA**	**SLA**	**IdInt**
001	0…1011	0…0	01…1101	0…1	**{MAC; IPv4-*адрес*, …}**

Префикс маршрутизации

Префикс сети (64 бит)

Идентификатор интерфейса

FP – Format Prefix (префикс формата)
TLA (NLA, SLA) – Top- (Next-, Site-) Level Aggregation

наименьший: **2001:0000:0001:0001:[8байт]**
наибольший: **3FFF:00FF:FFFF:FFFF:[8байт]**

2001:00b7:7900:abcd:0500:43f0:1000:e040/48

Локальный адрес подсети **(SubNet, SN)**:

8	40	16	64 бит
FP	**Random**	**SNId**	**IdInt**
11111101	000000000…0	00 … 1	

Адрес обратной петли: **0:0:0:0:0:0:0:1** *(127.0.0.0)*
Неопределенный адрес: **0:0:0:0:0:0:0:0** *(0.0.0.0)*

Локальный адрес канала связи **(Link Local, LL)**:

10	54	64 бит
FP	**Zeroes**	**02:a1:2f:ff:ee:35:B4:12**
1111111010	000000000…0000000	

Тип адреса	*Первые цифры*
Глобальный	***2 или 3***
Локальный SN	***fd***
Локальный LL	***fe80::/10***
Групповой	***ff***

Адресация

Типы адресов IPv6

- **Индивидуальный (unicast)**
- **Групповой (multicast)**
- **Произвольный (anycast)**

Групповые адреса IPv6:

- идентифицируют группу интерфейсов для получения одного и того же контента;
- начинаются с префикса ff::/8

***Базовая структура группового адреса* IPv6:**

8	4	4	112 бит
FP	**Flag**	**Scope**	**GroupID**
1 1 1 1 1 1 1 1	0 0 0 0	0 0 1 0	

Flag – определяет тип адреса:

0000 – фиксированный (*Internet Assigned Numbers Authority, IANA*);

0001 – временный (локально выделенный)

Scope – определяет диапазон адресов

Scope	*Диапазон*
0001	*Interface-Local*
0010	*Link-Local*
0100	*Admin-Local*
0101	*Site-Local*
1000	*Organization*
1110	*Global*

Адресация

Примеры адресов IPv6

Глобальный агрегируемый уникальный адрес:
наименьший: 2001:0000:0001:0001: [8байт]
наибольший: 3FFF:00FF:FFFF:FFFF: [8байт]

Правила отображения адресов IPv6 :

2ba5:0:0:0:3200:0019:0:f084 → 2ba5::3200:19:0:f084
::abcd:189.56.10.1 → 0:0:0:abcd:189.56.10.1

Примеры адресов IPv6

Тип адреса	*Первые цифры*
Глобальный	*2 или 3*
Локальный SN	*fd*
Локальный LL	*fe80*
Групповой	*ff02::1 и ff02::2*

2001:0067:89ab:cdff:0b05:0009:0000:c054 →
→ 2001:67: 89ab:cdff:b05:9:0:c054
fe80:0:0:0:0:0:0012:a2c1 → fe80::12:a2c1

Специальные адреса: **::1 и ::**

IPv6-адрес в URL в квадратных скобках:
https://[2001:00b5:31a4:1015:3c45:6abe:700a:981f]/
https://[2001:00b5:31a4:1015:3c45:6abe:700a:981f]:8080/

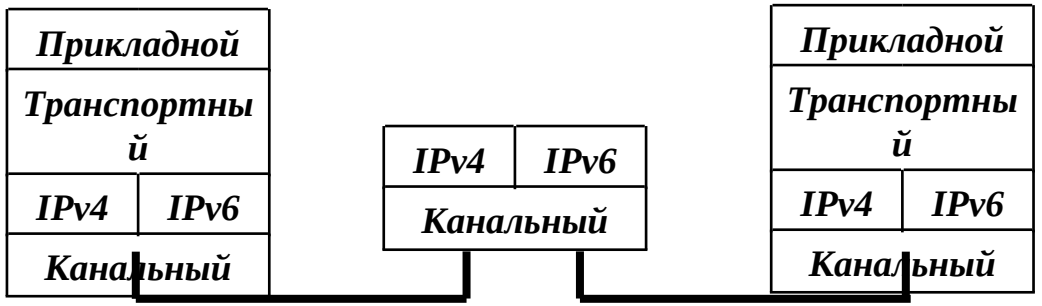
Преимущества адресации IPv6:
1. Ускорение маршрутизации (всего 8192 TLA-сетей – сетей верхнего уровня).
2. Возможность указать непосредственно физический адрес устройства (MAC- адрес).
3. Не нужен ARP-протокол и ручное конфигурирование конечных узлов.
4. Не нужно маскирование адресов.

Совместимость протоколов IPv6 и IPv4

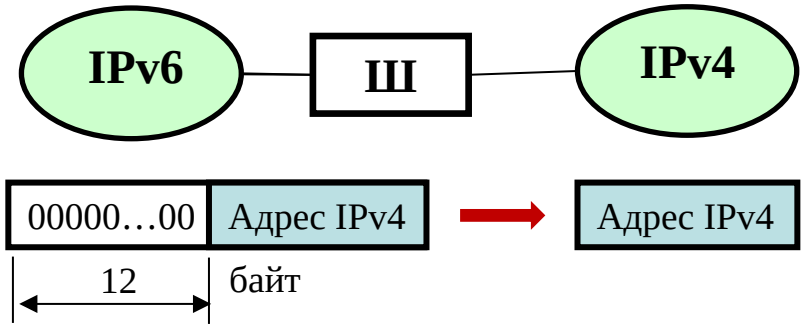
Способы межсетевого взаимодействия:

- трансляция протоколов;
- мультиплексирование стеков протоколов IPv4/ IPv6 в конечных узлах и во всех маршрутизаторах;
- инкапсуляция (туннелирование).

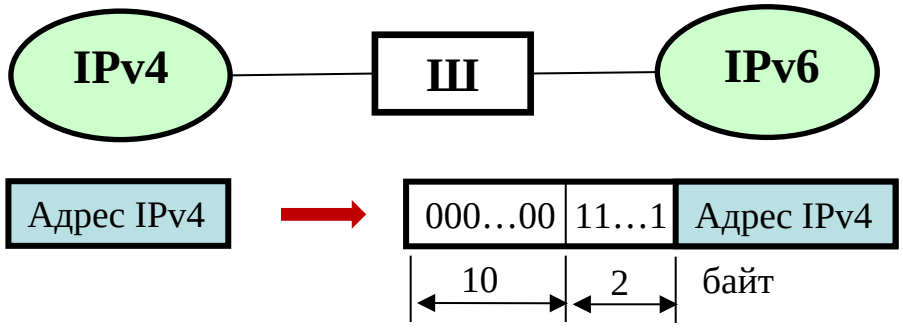
Двойной стек (dual stack) протоколов IPv4/ IPv6

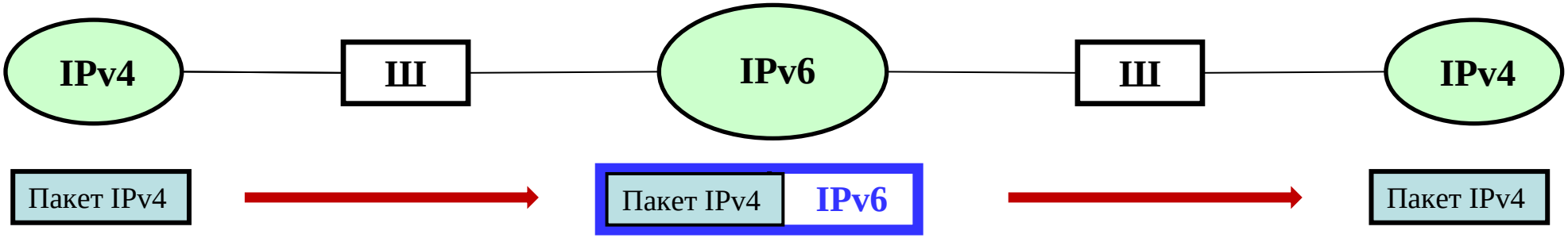


IPv4-совместимый IPv6 -адрес



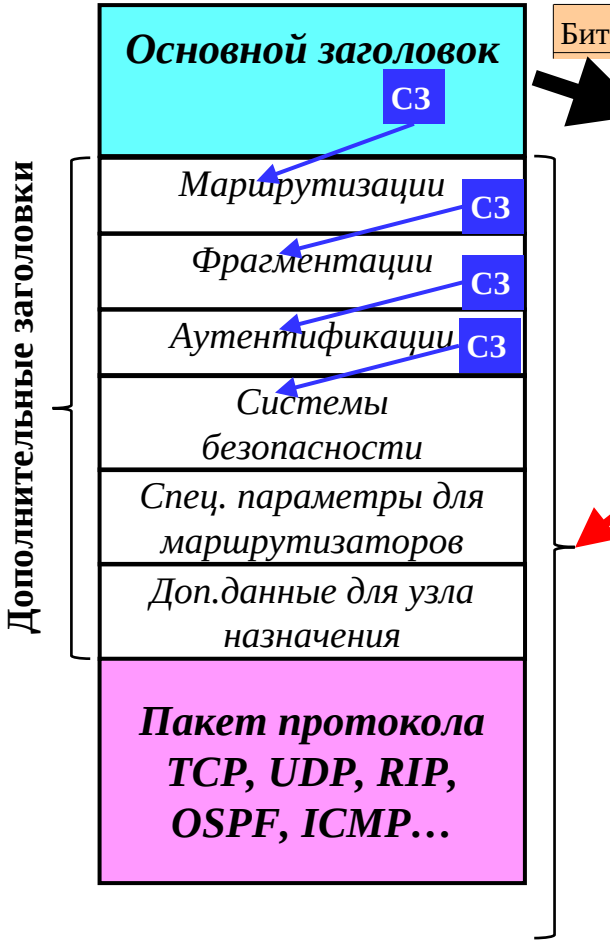
IPv4-отображенный IPv6 -адрес





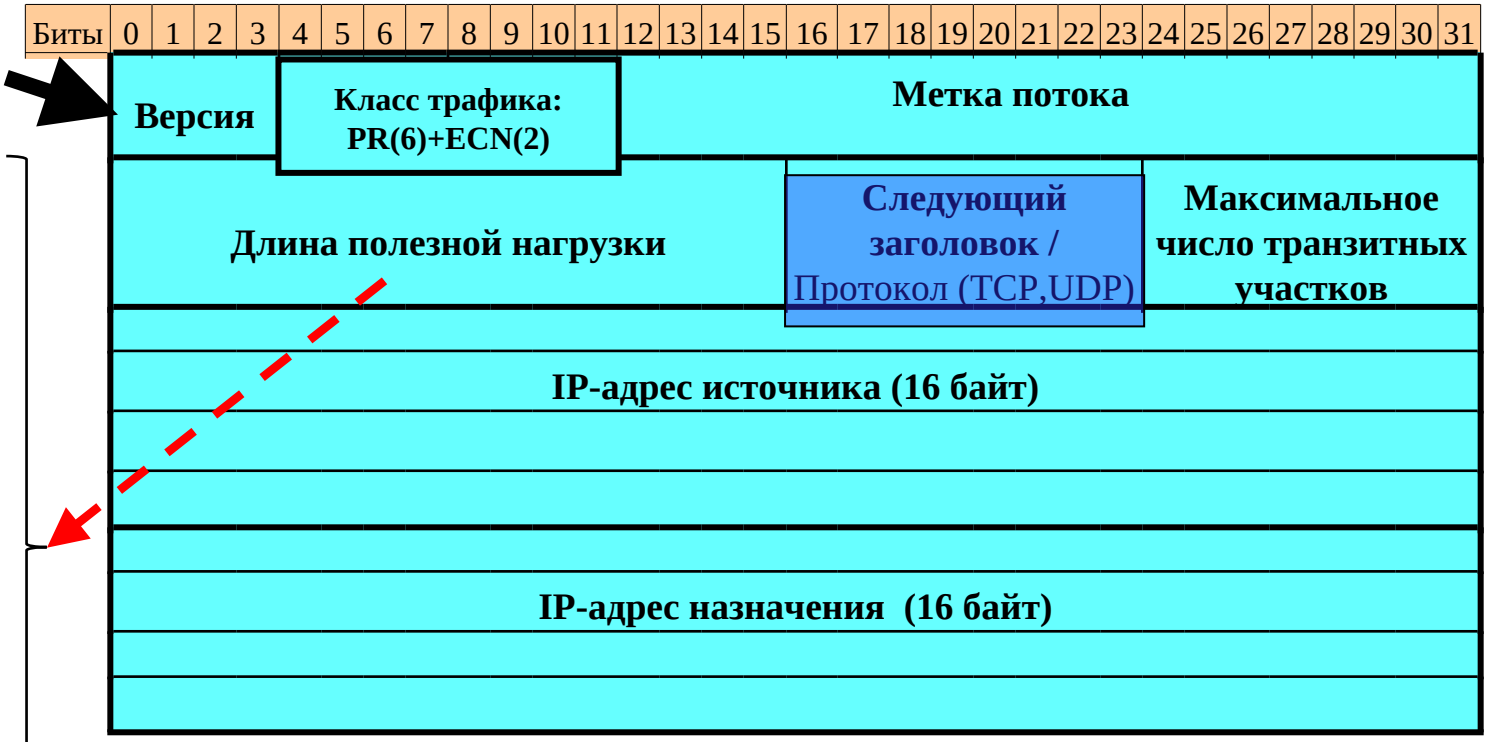
Структура пакета и формат заголовка IPv6

Структура пакета IPv6



IPv6 – *простой, быстрый, гибкий!*

Формат *основного* заголовка IPv6 (40 байт)

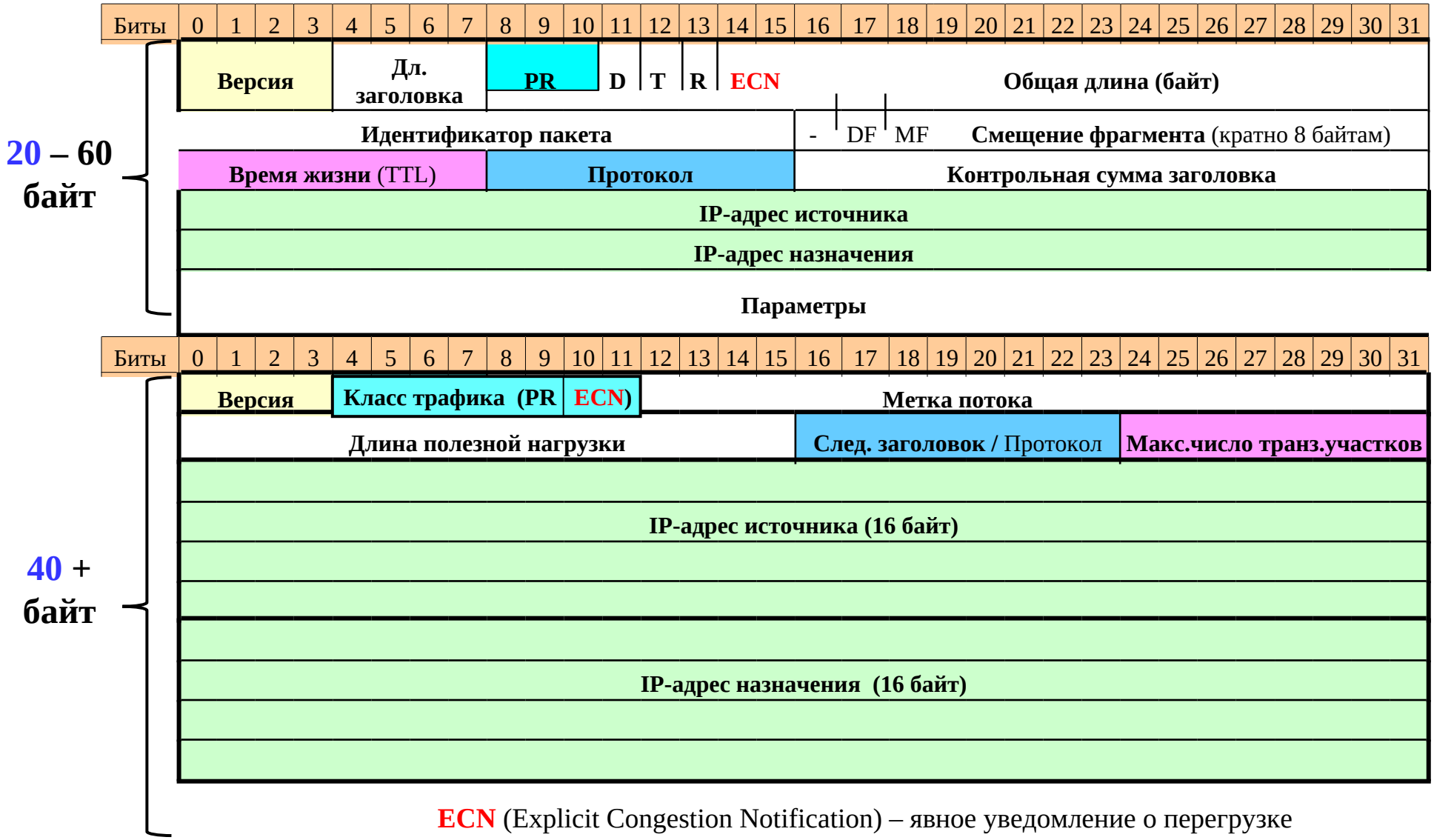


Изменения IPv6 по сравнению с IPv4:

- фрагментация только в конечных узлах;
- не нужны ARP-протокол и маскирование;
- в сверхскоростных сетях возможна поддержка пакетов до 4 гигабайт (джамбограмм);
- появились метки потоков и классы трафика (приоритет): 0 – обычный трафик; 1 – сетевые новости; 2 –электронная почта; 4 – существенный трафик (FTP, HTTP); 6 – интерактивный трафик; 7 – управляющий трафик (маршрутная информация, SNMP);
- появилось многоадресное вещание.

2.8. Коммуникационный протокол IPv6

Сравнение заголовков IPv4 и IPv6



ECN (Explicit Congestion Notification) – явное уведомление о перегрузке

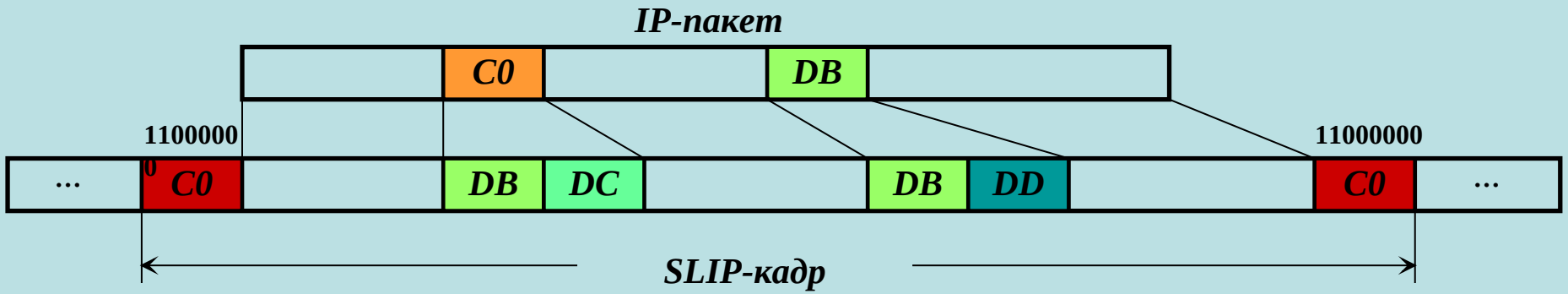
2.9. Протоколы канального уровня для выделенных линий

компьютер, коммутатор, маршрутизатор, …

Функции протоколов канального уровней:
- обеспечение надежной передачи;
- управление потоком кадров и предотвращения переполнения соседних узлов.

Протоколы канального уровня:
- **SLIP;**
- ***протоколы семейства HDLC;***
- **PPP (PPTP).**

Протокол SLIP (*Serial Line IP*)



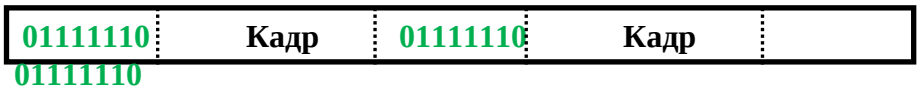
Недостатки:
- нет возможности обмениваться адресной информацией;
- невозможна передача пакетов, отличных от IP-пакетов;
- нет процедур обнаружения и коррекции ошибок;
- высокая избыточность — из-за передачи полных заголовков верхних уровней и байт-стаффинга.

2.9. Протоколы канального уровня для выделенных линий

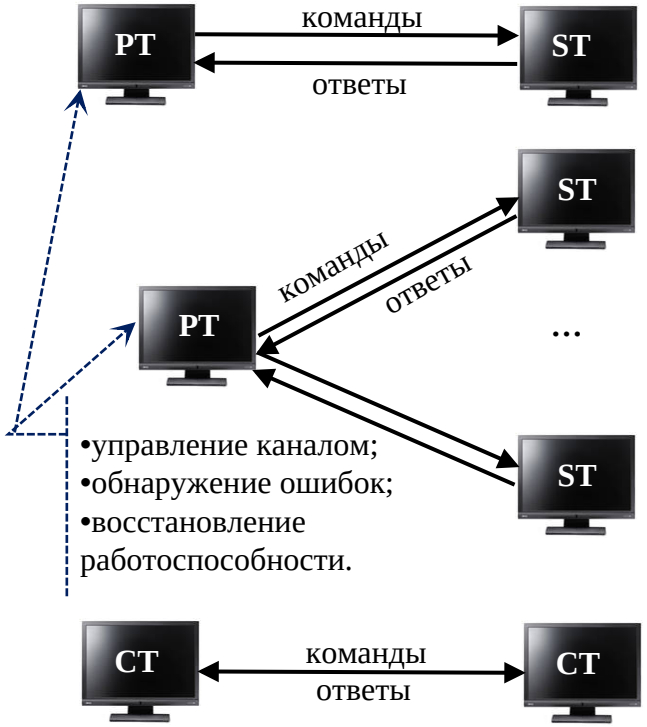
Протокол HDLC *(High-level Data Link Control Procedure)*

HDLC – стандарт ISO для выделенных линий – семейство протоколов LAP (*Link Access Procedure*):
- LAP-B – для сетей X.25 (B – Balanced);
- LAP-D – для сетей ISDN (D – D-channel);
- LAP-M – для модемов (M – Modem);
- LAP-F – для сетей Frame Relay (F – Frame Relay).

Типы станций:
- ***Первичная (ведущая)*** (PT – Primary Terminal)
- ***Вторичная (ведомая)*** (ST – Secondary Terminal)
- ***Комбинированная*** (CT – Combined Terminal)



Режимы логического соединения:
1. **Режим нормального ответа** (Normal Response Mode, NRM) – требует явного разрешения на передачу от первичной станции; круговой опрос вторичных станций в соединениях точка-многоточка.
2. **Режим асинхронного ответа** (Asynchronous Response Mode, ARM) – вторичная станция может сама инициировать передачу в соединениях типа кольцо и многоточечных по типу маркера (token).
3. **Асинхронный сбалансированный режим** (Asynchronous Balanced Mode, ABM) используется комбинированными станциями в *дуплексном режиме* (оба устройства равноправны и обмениваются командами и ответами).



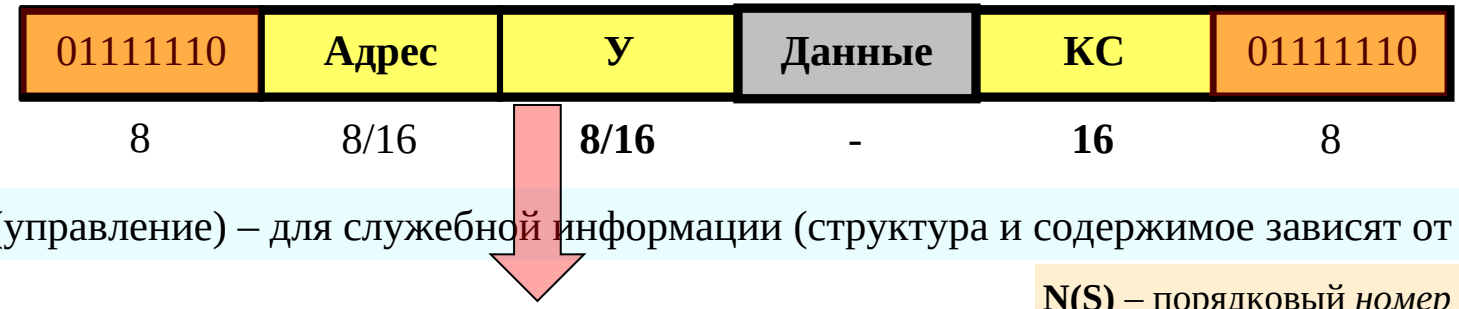
Типы соединений

синхронные (битстаффинг) — асинхронные (байтстаффинг)

Межкадровое временное заполнение: **0111110 0111110 0111110** (битовая синхронизация)

2.9. Протоколы канального уровня для выделенных линий

Формат кадра HDLC



У (управление) – для служебной информации (структура и содержимое зависят от **типа** HDLC-кадра):

Информационный

Управляющий (супервизорный)

Ненумерованный (служебный)

N(S) – порядковый *номер передаваемого* кадра;
N(R) – *номер* очередного *ожидаемого* кадра;
P/F (Poll/Final) – *промежуточный* или *последний* кадр;

Type – **тип управляющего кадра**: 0 – подтверждение; 1 – отрицательное подтверждение; 2 – отказ; 3 –выборочное подтверждение);

Type+Modifier – **тип и модификация команд**: запрос на установление соединения, подтверждение соединения, запрос на разрыв соединения.

Особенности протокола HDLC:

- в HDLC-кадре отсутствует **поле длины кадра**, причем длина поля **Данные** - произвольная;
- **флаг** конца одного кадра может служить начальным флагом следующего кадра;
- в двухточечном соединении **Адрес** служит для обозначения команд и ответов, а также направления передачи кадра: 10000000 или 11000000;
- в поле данных могут находиться пакеты IP, IPX, AppleTalk, DECnet, X25, Frame Relay,…;
- контрольная сумма – CRC-16 (*Cyclic Redundancy Check*);
- **механизм окна**: размер окна 7 или 127 кадров, квитанции положительные и отрицательные.

2.9. Протоколы канального уровня для выделенных линий

Протокол PPP *(Point-to-Point Protocol)*

PPP *– байт-ориентированный* протокол канального уровня, представляющий собой семейство протоколов:

- **LCP (Link Control Protocol)** – *протокол управления соединением* (установка, поддержка и завершение соединения);
- **NCP (Network Control Protocol)** – *протокол управления сетью* для определения настроек сетевого уровня (сетевой адрес и пр.);
- **MLPPP (Multi Link PPP)** – *многоканальный протокол* PPP формирует несколько физических каналов для одного логического соединения;
- **PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) –** протоколы аутентификации

PPP основан на четырех принципах:

• ***автоматическая настройка интерфейсов*** за счет согласования параметров соединения (качество ЛС, размер кадров, тип протокола аутентификации) на основе переговоров (LCP);

• ***многопротокольная поддержка*** (IP, IPX, XNS, …) за счет конфигурирования сетевого протокола (NCP);

• расширяемость протокола;

• независимость от глобальных служб.

Подвиды протокола PPP:

- Point-to-Point Protocol over Ethernet (PPPoE) для подключения по Ethernet;
- Point-to-Point Protocol over ATM (PPPoA), который используется для подключения по ATM.

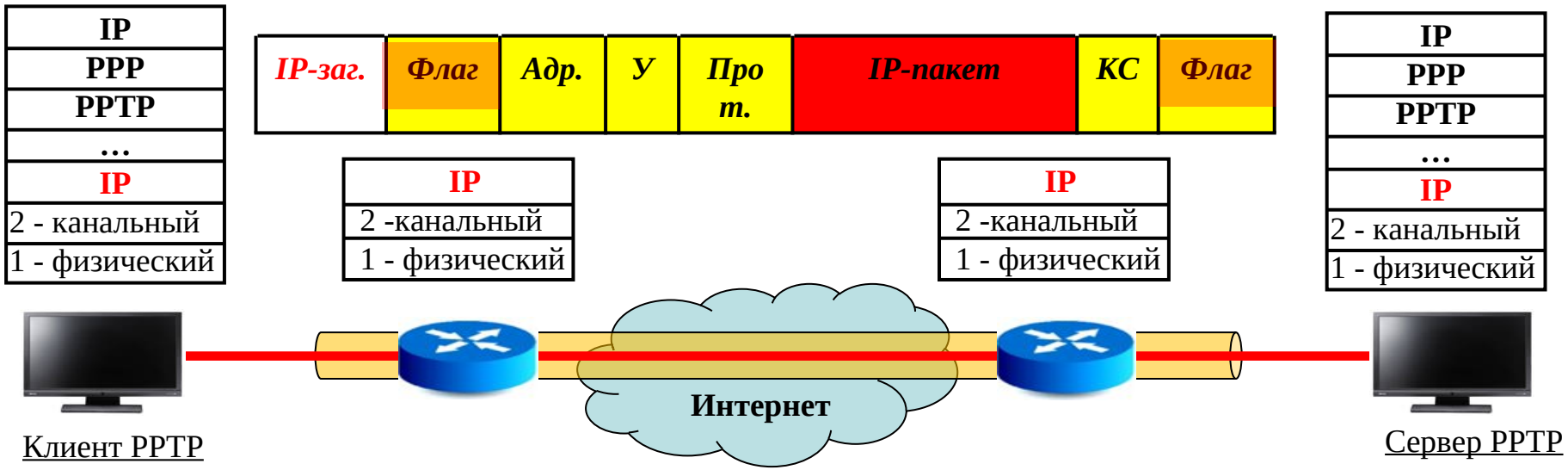
2.9. Протоколы канального уровня для выделенных линий

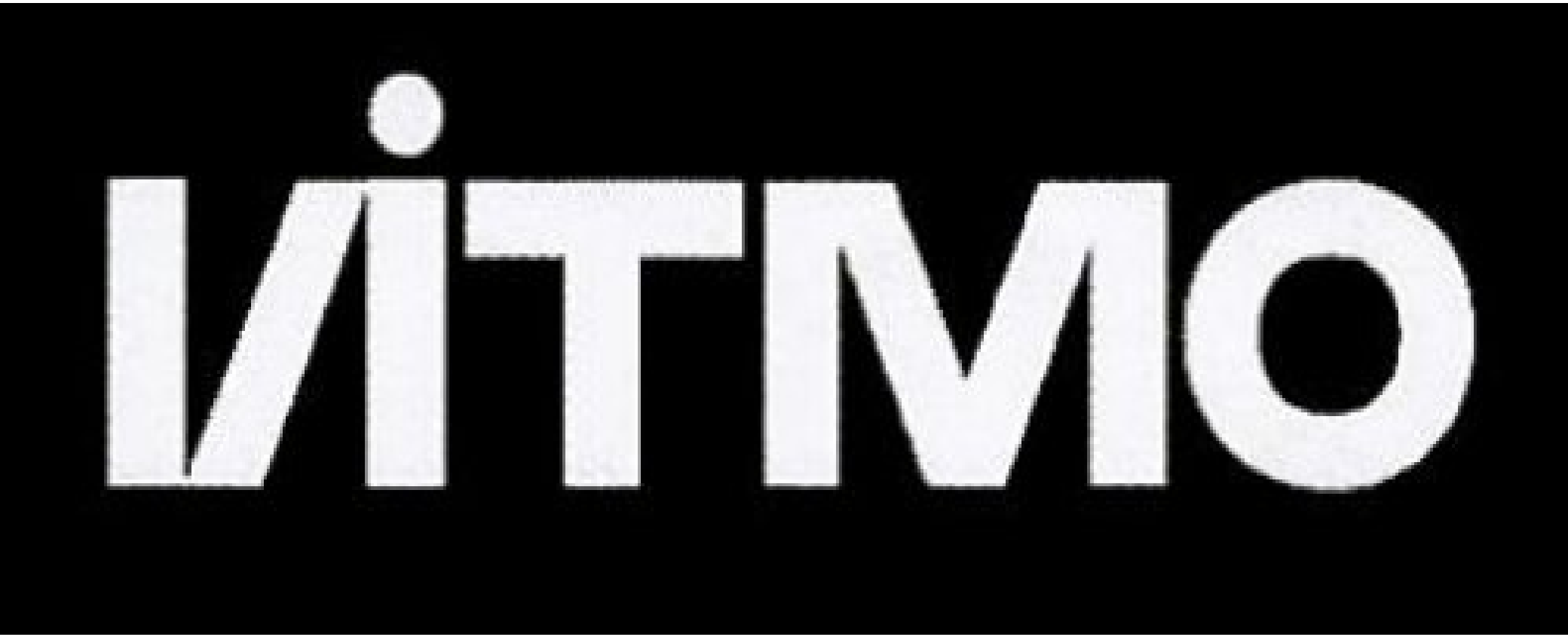
Формат кадра PPP для работы в ненумерованном режиме

Флаг	Адрес	У	Протокол	Данные	КС	Флаг
01111110	11111111	**00000011**				01111110
1	1	**1**	**1/2**	**1494**	**2/4**	1 байт

Протокол PPTP *(Point-to-Point Tunneling Protocol)*

- *туннельный протокол* «точка-точка» для создания защищённого соединения в незащищённой сети путем инкапсуляции кадров PPP в IP-пакеты;
- может использоваться для организации туннеля между двумя компьютерами или между локальными сетями;
- для обслуживания туннеля использует дополнительное TCP-соединение.




ИТМО

1. Основная особенность стека протоколов TCP/IP.

2. В каком поле заголовка пакета протокола IPv4 указывается контрольная сумма пакета?

3. Какие записи не являются корректными глобальными агрегируемыми уникальными адресами IPv6?

3	13	8	24	16	64 бит
FP	TLA		NLA	SLA	IdInt
001	0…1011	0…0	01…1101	0…1	

A. 21ac:b17:3a:1c7:b00:9876:0:0
B. 40c1:7:a5:17:50b0:91:10:f4
C. 2702:8:88:17k:a50:19:50:14
D. 1234:aa:153a:1f7f:f15:9999:10:51
E. 20f::777:a2:74c:ff
F. 20ab::66:ab:11::d123
G. 2001:0067:89ab:cdff:0b05:0009:0000:c054
H. 20cc:17:33a:17:b050:9:0:c054
I. 3FFF::1A2B:345
J. 3d3d:f:44:ff::1

1. **Какую длину в битах имеют MAC-адрес и IP-адрес?**
2. **Сколько IP-адресов имеет: а) маршрутизатор; б) коммутатор; в) концентратор)?**
3. **Сколько MAC-адресов имеет: а) маршрутизатор; б) коммутатор; в) концентратор)?**
4. **Простой протокол передачи почты – это ...?**
5. **Поле "Длина заголовка" пакета IPv4 имеет вид: 1001. Чему равна длина заголовка в байтах?**
6. **Какая цель отправки ARP-запроса при назначении IP-адреса компьютеру?**
7. **Как определить размер кадра HDLC, если в заголовке отсутствует поле длины кадра:**

1. В чем различие между вычислительной системой и вычислительной машиной?
2. Как правильно: вычислительная сеть, компьютерная сеть или сеть ЭВМ?
3. В чем разница между данными и информацией?
4. Основное достоинство коммутации пакетов.
5. На каком уровне OSI-модели решается задача маршрутизации?
6. Для чего используется процедура «бит-стаффинг»?
7. **Простой протокол передачи почты – это ...?**
8. **Для чего нужен псевдозаголовок в протоколах TCP и UDP?**
9. **Какую длину в байтах имеют MAC-адрес и IP-адрес?**

Специальные групповые адреса Ipv6

Scope	*Диапазон*	*Адрес*	
0001	*Interface-Local (Node)*	*ff01::1*	*Все IPv6 узлы*
0010	*Link-Local*	*ff02::1*	*Все IPv6 узлы*
0100	*Admin-Local*	*ff01::2*	*Все маршрутизаторы*
0101	*Site-Local*	*ff05::2*	*Все маршрутизаторы*
1000	*Organization*	*ff01::1*	
1110	*Global*	*ff01::1*	

Групповые адреса

Специальный групповой адрес Solicited-Node:

- используется в процессе разрешения IPv6-адресов для сегмента сети;
- присваивается каждому интерфейсу вместе с индивидуальными адресами;
- используется только на канале связи или в сегментах сети.

- **Генерация адреса:**

младшие 24 бита поля Interface ID индивидуального или альтернативного адреса
+
префикс FF02:0:0:0:0:1:FF00::/104

Пример:

Адрес IPv6:	FE80::0202:B3FF:FE1E:8329
Префикс Solicited-Node:	FF02:0000:0000:0000:0000:0001:FF00:0000
Групповой адрес Solicited-Node:	FF02:0000:0000:0000:0000:0001:FF1E:8329 или FF02::1:FF1E:8329

IPv6 Multicast addresses(cont.)

- Special multicast IPv6 address
  - FF01::1
    - Node-local scope all-nodes multicast address
  - FF02::1
    - Link-local scope all-nodes multicast address
  - FF01::2
    - Node-local scope all-routers multicast address
  - FF02::2
    - Link-local scope all-Routers multicast address
  - FF05::2
    - Site-local scope all-routers multicast address
- Use low-order 32 bits, each group ID maps to a unique Ethernet MAC address (RFC 2373)