

Стек протоколов TCP/IP

Источники стандартов и координаторы

- ◆ Internet Engineering Task Force / IETF

- <http://www.ietf.org/>

- Request For Comments (RFC)

- ◆ Internet Corporation for Assigned Names And Numbers / ICANN

- <http://www.icann.org/>

- Internet Assigned Numbers Authority / IANA

- <http://www.iana.org/>

- ◆ Доменные имена
 - ◆ IP адреса
 - ◆ Реестр названий и номеров протоколов
 - ◆ ...

Источники стандартов

◆ World Wide Web Consortium / W3C

<http://www.w3c.org/>

- HTTP
- HTML
- CSS
- XML
- ...

Местные регистраторы

- ◆ Европейский региональный реестр
RIPE Network Coordination Centre
<http://www.ripe.net/>
 - IP адреса

- ◆ Russian Institute for Public Networks / RIPN
Российский НИИ Развития Общественных
сетей / РосНИИРОС
<http://www.ripn.net/>
 - IP адреса
 - Домен .ru

Сетевой порядок байтов

Как хранится в памяти многобайтовое значение, например 0x1234?

◆ Little Endian (Intel 80x86)

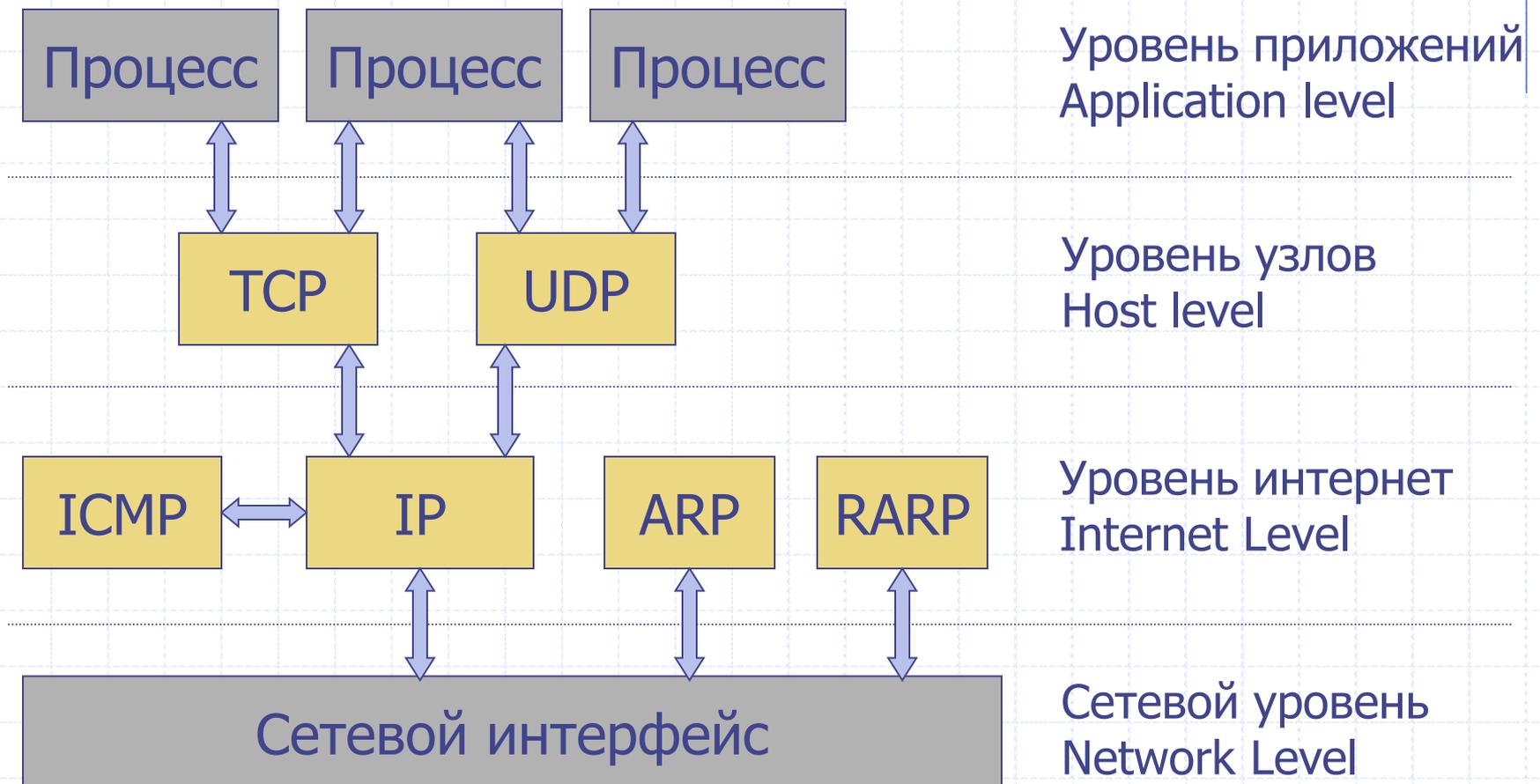


◆ Big Endian (Sparc, PowerPC,...)



- Сетевой порядок байтов

Многоуровневая модель стека TCP/IP



Сетевой уровень

Network level

Задача уровня:

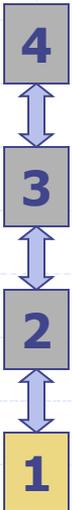
- ◆ Обеспечивает передачу данных между устройствами, соединёнными разделяемой средой передачи данных (физический и канальный уровни модели OSI).

Реализуется сетевым адаптером и драйверами.

Не определяется стандартами TCP/IP.

На этом уровне вводятся MAC-адреса.

Для обозначения группы устройств, соединённых единой разделяемой средой передачи данных используется термин «локальная сеть».



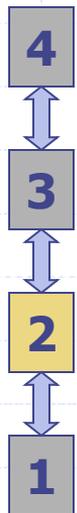
Уровень интернет

Internet level

Задача уровня:

- ◆ Объединение локальных сетей в единую глобальную сеть произвольной топологии.

На этом уровне вводятся сетевые адреса: IP-адреса.



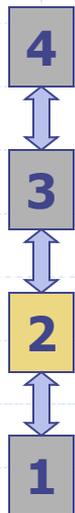
Уровень интернет Протокол IP (RFC 791)

Задача протокола:

- ◆ Передача данных в глобальной сети.

Основные функции:

- Адресация
- Маршрутизация
- Фрагментация пакетов



Уровень интернет IP адреса

IP адрес

192	0	2	75
1 1 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	0 1 0 0 1 0 1 1

Маска

255	255	255	192
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

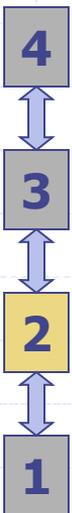
Адрес
сети

192	0	2	64
1 1 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	0 1 0 0 0 0 0 0

Адрес
хоста

0	0	0	11
0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 0 1 1

Альтернативная форма записи: 192.0.2.75/26



IP адреса

Особые значения адресов хоста

IP адрес, у которого все биты адреса хоста равны 0 не выдаётся - он является адресом сети.

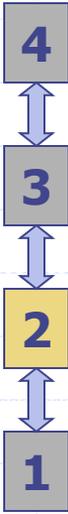
IP адрес, у которого все биты адреса хоста равны 1 также не выдаётся - он является широковещательным адресом.

Таким образом, самая маленькая сеть имеет маску /30 (255.255.255.252) и включает следующие адреса:

00 – адрес сети

01 и 10 – адреса хостов

11 – широковещательный адрес



4

3

2

1

IP адреса

Иерархическая структуризация

192	168	0	0
11000000	10101000	00000000	00000000

22 24 26

192.168.0.0/22

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

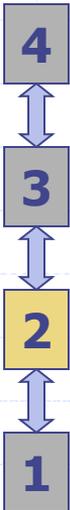
192.168.3.0/24

192.168.2.0/26

192.168.2.64/26

192.168.2.128/26

192.168.2.192/26



IP адреса

Специальные блоки адресов

Ряд блоков адресов выделен для использования вне сети интернет (RFC 1918):

Сеть 10/8:

10.0.0.0 - 10.255.255.255

Сеть 172.16/12:

172.16.0.0 - 172.31.255.255

Сеть 192.168/16:

192.168.0.0 - 192.168.255.255

Сеть 127/8 зарезервирована для использования в loopback интерфейсе. Обычно используется адрес 127.0.0.1.

Другие особые случаи описаны в RFC 5735.

4

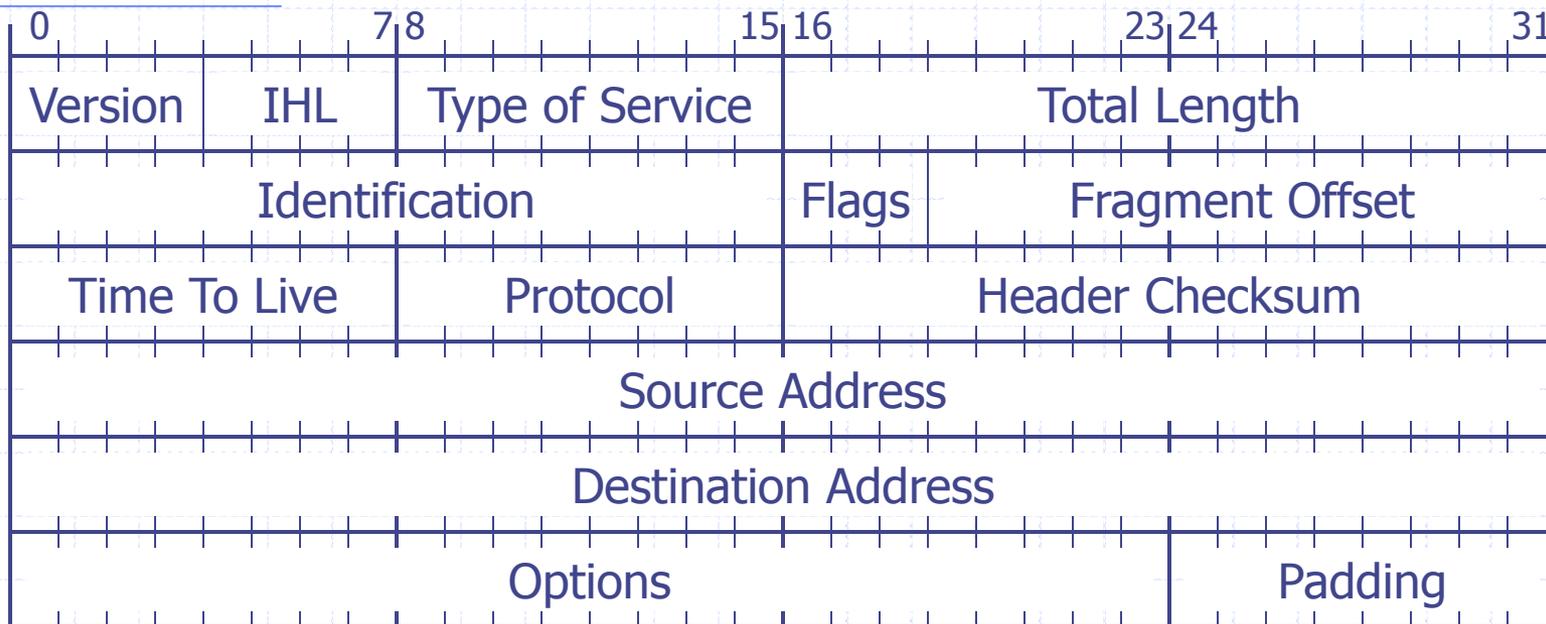
3

2

1

Протокол IP (RFC 791)

Формат заголовка



Version - версия (4)

IHL - размер заголовка (4 байта)

Type of Service - приоритет

Total Length – размер пакета

Identification – номер пакета

Flags – флаги (0=0, 1-DF, 2-MF)

Fragment Offset - смещение

Time to Live – время жизни

Protocol – протокол уровня узлов

Header checksum – контрольная сумма

Source Address – IP отправителя

Destination Address – IP получателя

Options – опции IP

Padding - выравнивание

4

3

2

1

Протокол IP (RFC 791)

Фрагментация



A → B:

Identification	Flags		Fragment Offset
	DF	MF	
735	0	0	0

B → C:

Identification	Flags		Fragment Offset
	DF	MF	
735	0	1	0

Identification	Flags		Fragment Offset
	DF	MF	
735	0	0	200

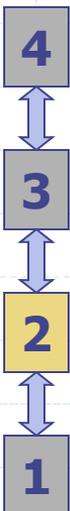
C → D:

Flags		Fragment Offset
DF	MF	
1		0

Flags		Fragment Offset
DF	MF	
1		100

Flags		Fragment Offset
DF	MF	
1		200

Flags		Fragment Offset
DF	MF	
0		300



Протокол IP (RFC 791)

Опции IP

- ◆ 0 – End of Option List
 - конец списка опций
- ◆ 1 – No Operation
 - нет операции
- ◆ 2 – Security
 - безопасность
- ◆ 3 – Loose Source And Record Route
 - не строго задает маршрут
- ◆ 4 – Strict Source And Record Route
 - строго задаёт маршрут
- ◆ 5 – Record Route
 - запись маршрута
- ◆ 6 – Stream Identifier
 - идентификатор потока сети SATNET
- ◆ 7 – Internet Timestamp
 - запись времени на маршрутизаторах

4

3

2

1

Internet Control Message Protocol ICMP (RFC 792)

Задача протокола:

◆ Передача служебных сообщений IP.

Для передачи используется протокол IP.

4
3
2
1

Сообщения ICMP посылаются при возникновении проблем с доставкой IP пакетов и для решения других задач.

При уничтожении ICMP пакетов новый ICMP пакет не генерируется.

Internet Control Message Protocol

Виды сообщений

- ◆ Destination unreachable
 - маршрут к получателю не доступен
- ◆ Source Quench
 - пакет удалён из-за недостатка ресурсов маршрутизатора
- ◆ Time Exceeded
 - поле TTL заголовка IP достигло значения 0
- ◆ Parameter Problem
 - неправильный заголовок IP (опции)
- ◆ Redirect
 - указание изменить таблицу маршрутизации
- ◆ Echo / Echo reply
 - запрос/ответ «проверка связи»
- ◆ Timestamp/Timestamp reply
 - запрос/ответ времени
- ◆ Information Request/Information Reply
 - запрос/ответ маски сети

4

3

2

1

Уровень интернет Протоколы ARP и RARP

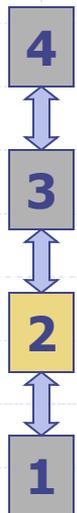
Задача протоколов:

- ◆ Преобразование сетевых адресов в MAC адреса.

Address Resolution Protocol (ARP)

- С помощью широковещательного пакета хост запрашивает, кто владеет интересующим IP адресом.
- Владелец (если он работает) в ответ сообщает свой MAC-адрес.
- Полученное значение запоминается в ARP таблице

Обратное преобразование выполняется Reverse Address Resolution Protocol (RARP).



Уровень узлов

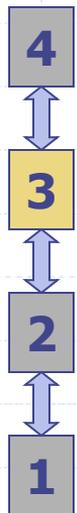
Host level

Задача уровня:

- ◆ Предоставление услуг заданного качества и обеспечение адресации процессов в рамках хоста.

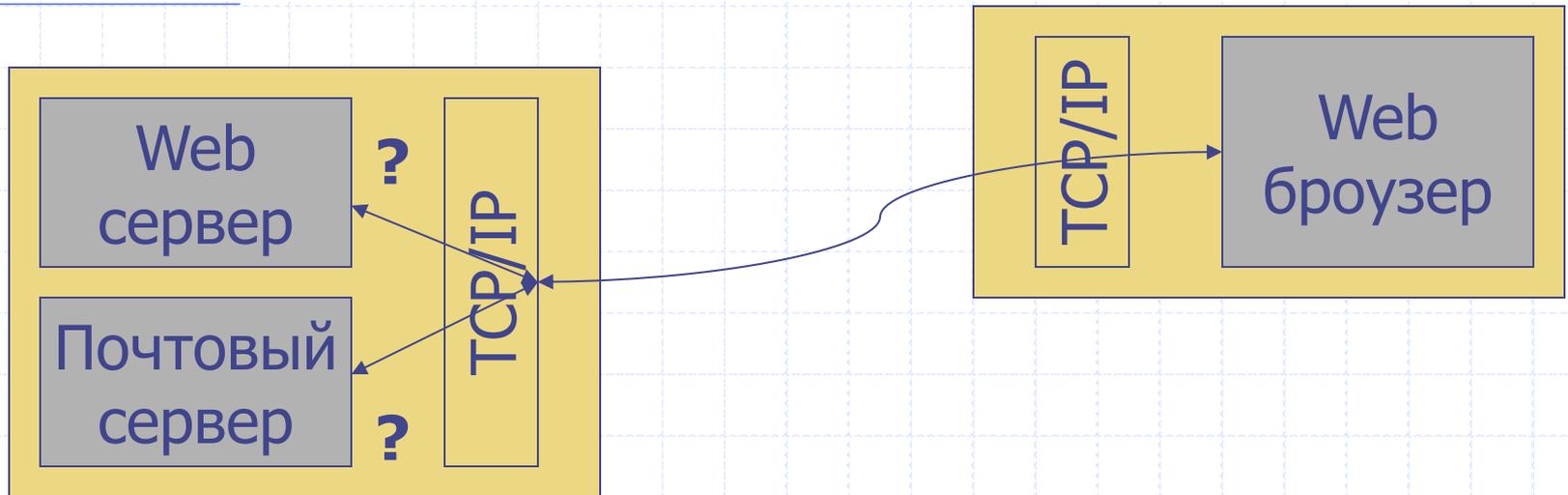
Возможные проблемы доставки IP пакетов:

- ◆ Потеря пакетов
- ◆ Дублирование пакетов
- ◆ Нарушение порядка пакетов
- ◆ Отсутствуют средства для организации каналов передачи данных – возможна только отправка отдельных пакетов.



Уровень узлов

Адресация в пределах узла



Для идентификации процесса в рамках хоста используется **порт** – двухбайтное число.

Известные значения портов могут быть найдены в файле /etc/services (windows\system32\drivers\etc\services) или на сайте IANA <http://www.iana.org/assignments/port-numbers>

4

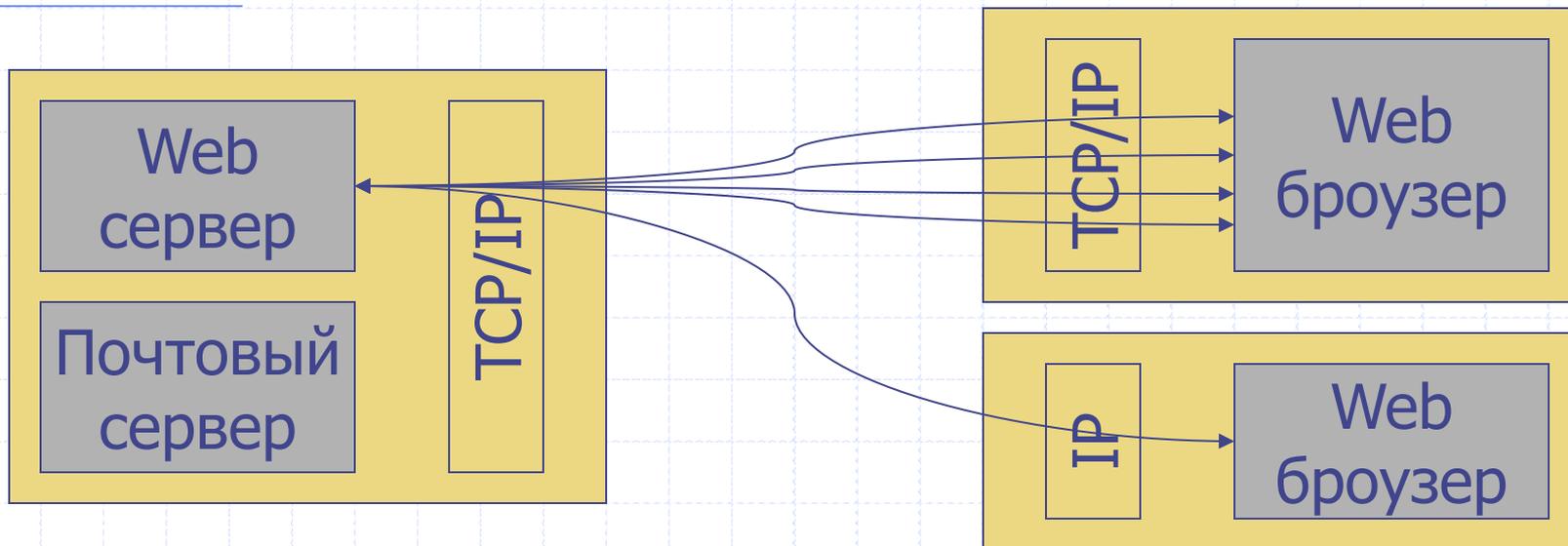
3

2

1

Уровень узлов

Адресация в пределах узла



Для идентификации процесса в рамках хоста используется **порт** – двухбайтное число.

Пара {IP адрес, порт} называется **сокетом**.

Соединение идентифицируется парой сокетов {локальный сокет, удалённый сокет}.

4

3

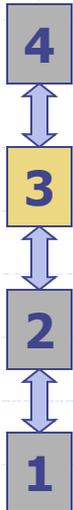
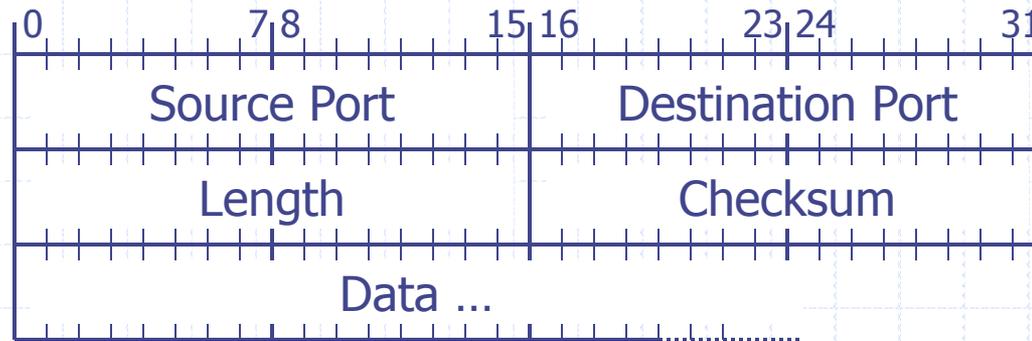
2

1

User Datagram Protocol UDP (RFC 768)

Задача протокола:

- ◆ Передача датаграмм с минимальными накладными расходами.



Source Port

- порт отправителя

Destination Port

- порт получателя

Length

- размер пакета (данные и заголовок)

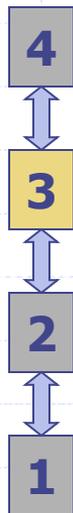
Checksum

- контрольная сумма (данные, заголовок, псевдозаголовок)

Transmission Control Protocol TCP (RFC 761)

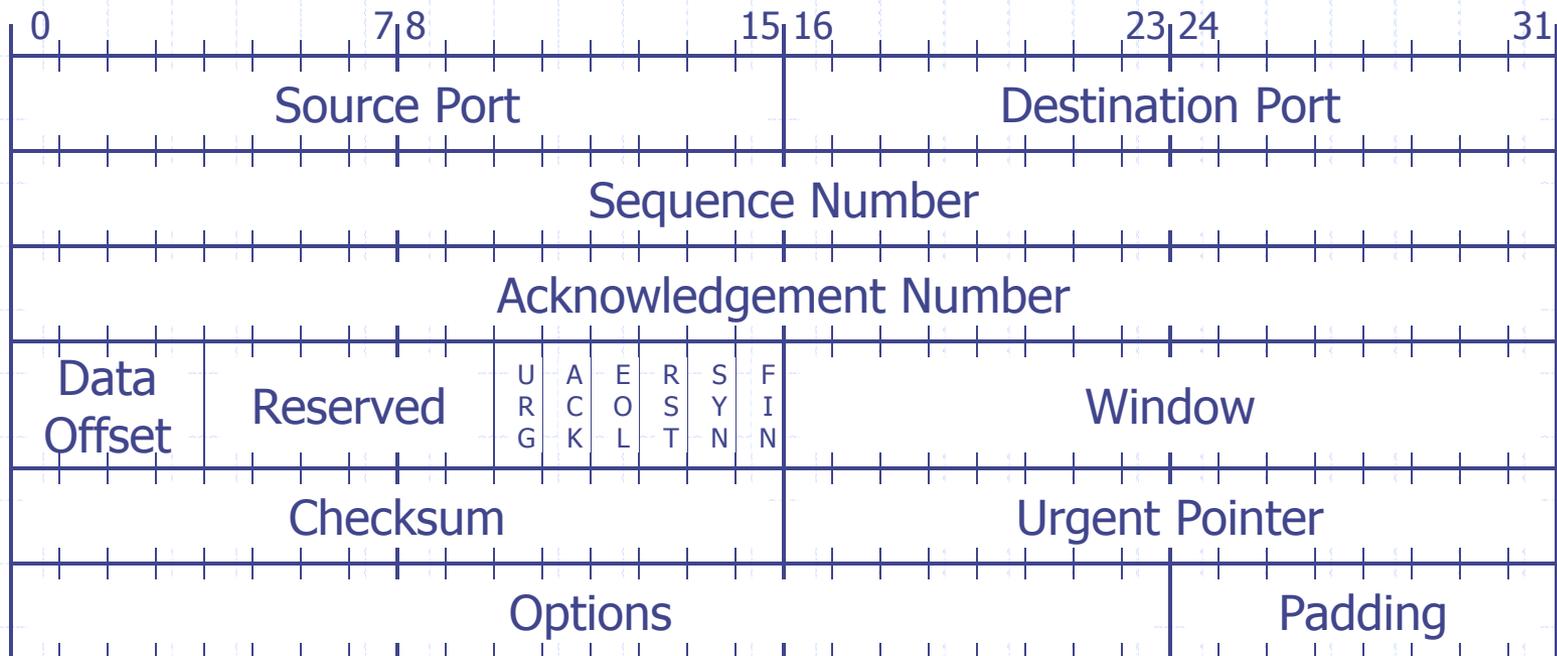
Задача протокола:

- ◆ Организация надёжного канала передачи данных.



TCP (RFC 761)

Формат заголовка



4

3

2

1

Source Port - порт отправителя

Destination Port - порт получателя

Data Offset - смещение от начала пакета до начала данных (4 байта)

Checksum - контрольная сумма

Urgent Pointer – смещение до начала срочных данных

(присутствуют если установлен флаг URG)

TCP (RFC 761)

Контроль передачи данных

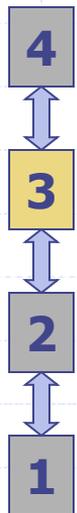
В поле **Sequence Number** указывается порядковый номер первого передаваемого байта данных в пакете.

В поле **Acknowledgement Number** указывается номер байта, который система ожидает принять (если установлен флаг **ACK**).

В поле Window указан размер буфера приёма, используемого системой. Будут сохранены байты, начиная с **ACK Number** до **ACK Number+Window**.

Начальное значение Sequence Number (**ISN**) генерируется случайно, чтобы:

- Исключить возможность приёма «старых» пакетов
- Для защиты от атак



TCP (RFC 761)

Установка связи

Система А

Открывает соединение с В

Генерирует ISN_A

<seq=ISN_A> <CTL=SYN>

Система В

Ожидает соединений

Генерирует ISN_B

Посылает подтверждение

<seq=ISN_B> <ACK=ISN_A+1> <CTL=SYN,ACK>

Переходит в состояние
«соединение установлено»

Посылает подтверждение

<seq=ISN_A+1> <ACK=ISN_B+1> <CTL=ACK>

Переходит в состояние
«соединение установлено»

Начинает отправку данных

<seq=ISN_A+1> <ACK=ISN_B+1> <CTL=ACK> <DATA>

4

3

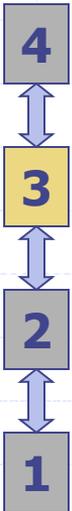
2

1

TCP (RFC 761)

Передача данных

- ◆ Для приёма и передачи данных используются интерфейсы RECEIVE и SEND.
- ◆ Фрагмент данных, переданный за один вызов через интерфейс SEND называют **письмом (letter)**, его конец помечается флагом **EOL**.
- ◆ При отправке данные хранятся до тех пор, пока не будет получено подтверждение об их приёме. Если оно не поступает, производится повторная отправка.
- ◆ Принятые данные накапливаются в буфере. Данные, выходящие за предел окна приёма игнорируются.



TCP (RFC 761)

Завершение соединения

- ◆ Для завершения соединения используется интерфейс **CLOSE**.
- ◆ Завершение соединения происходит после доставки всех данных удалённой системе.
- ◆ Соединение может быть независимо закрыто в направлении приёма и отправки данных.
- ◆ Для аварийного завершения предусмотрен интерфейс **ABORT**. Не доставленные данные теряются.

4

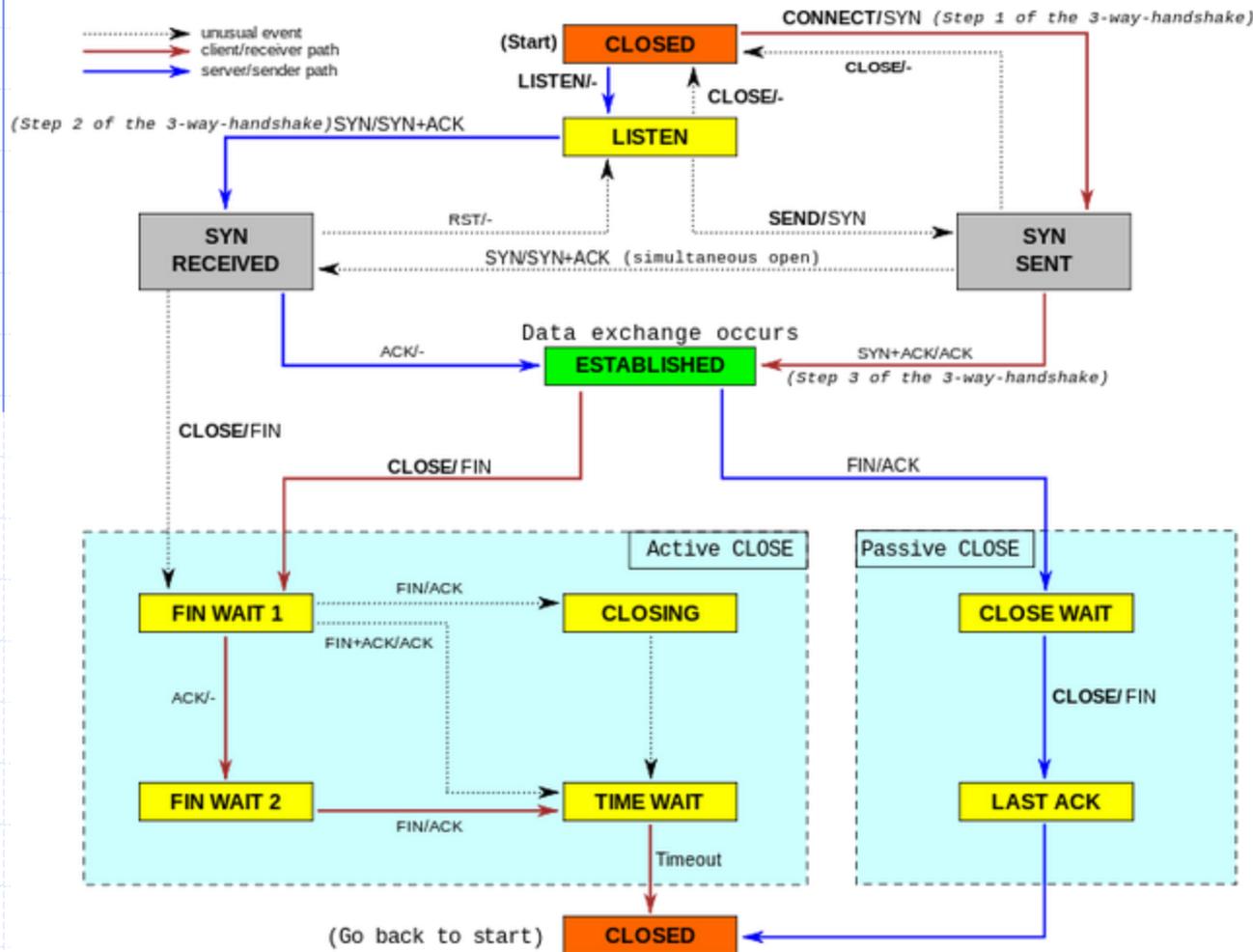
3

2

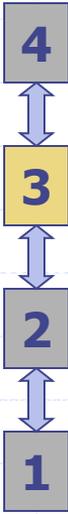
1

TCP (RFC 761)

Машина состояний TCP



- Listen** - ожидание входящих соединений
- SYN Sent** - ожидание открытия соединения после отправки ISN
- SYN Rcvd** - ожидание подтверждения открытия соединения
- Established** - соединение установлено
- Fin-Wait-1** - ожидание подтверждения о закрытии соединения
- Fin-Wait-2** - ожидание закрытия соединения
- Time-Wait** - ожидание времени, достаточного для доставки подтверждения закрытия соединения
- Close-Wait** - ожидание вызова CLOSE
- Closing** - ожидание подтверждения закрытия
- Closed** - соединение отсутствует



Уровень приложений

Application level

Задача уровня:

- ◆ Предоставление пользователю сетевых услуг

FTP – протокол передачи файлов (RFC 959)

Электронная почта:

SMTP – отправка почты (RFC 2821)

POP3 – получение почты (RFC 1939)

IMAP – получение почты (RFC 3501)

NNTP – передача конференций USENET (RFC 3977)

HTTP – передача гипертекстовых документов (w3c.org)

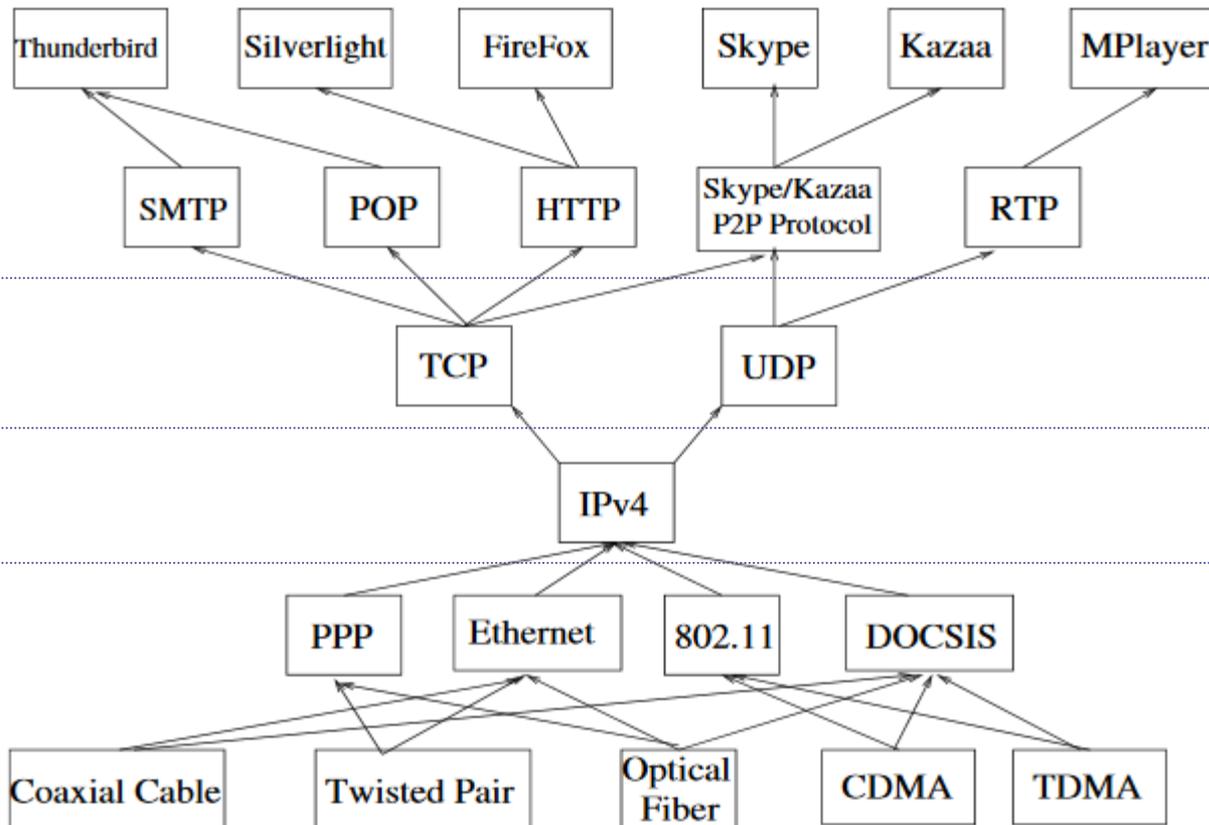
4

3

2

1

Принцип песочных часов



Уровень приложений
Application level

Уровень узлов
Host level

Уровень интернет
Internet Level

Сетевой уровень
Network Level