

# Лекция 1

Транспортный уровень TCP/IP

Сокеты и порты

UDP

TCP

# Протоколы транспортного уровня TCP/IP

## Transmission Control Protocol

RFC\* 793, 1982г

гарантированная доставка данных

## User Datagram Protocol

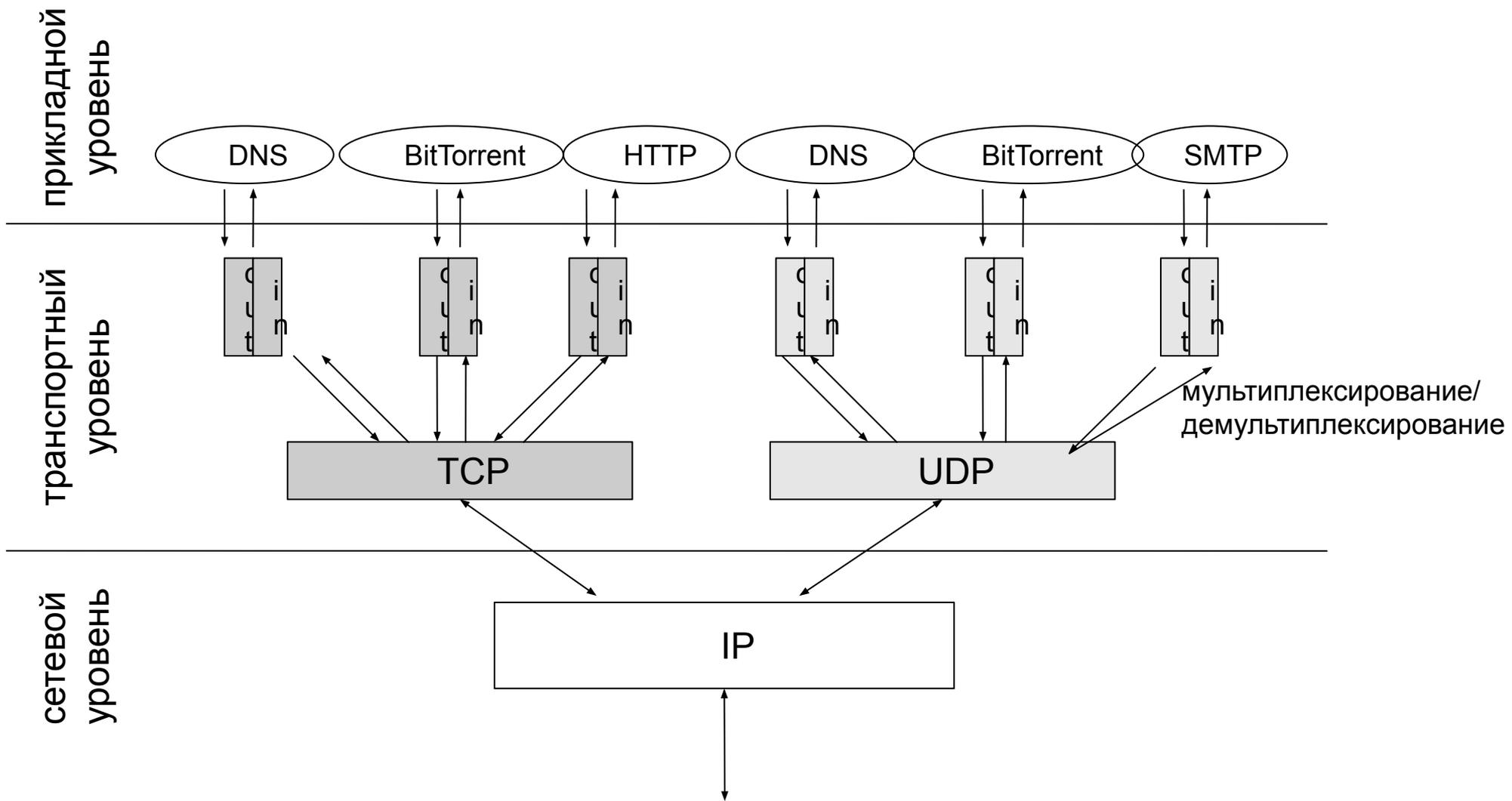
RFC\* 768, 1980г

доставка данных  
с максимальными усилиями

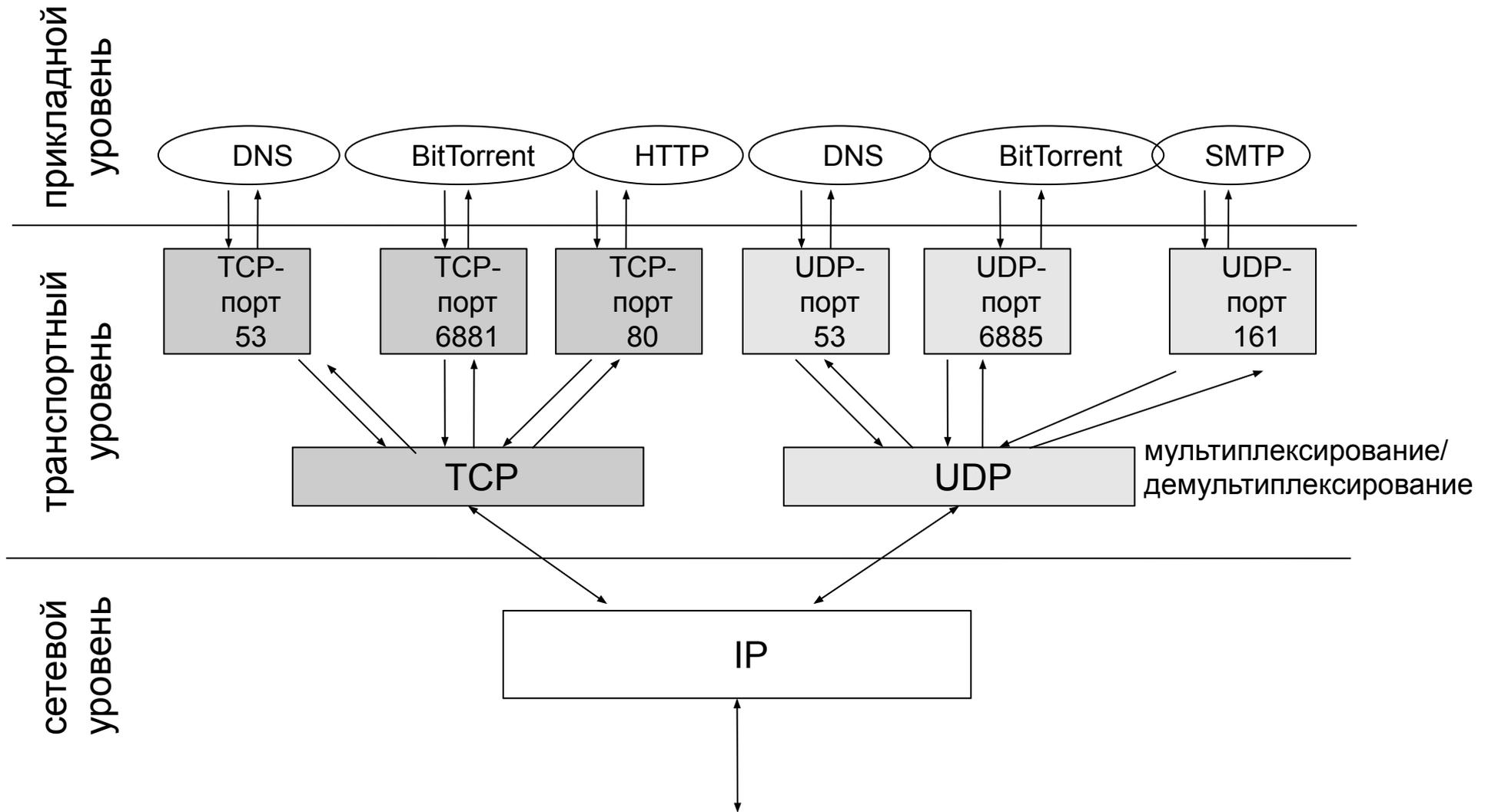
Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

\*RFC - Request For Comments

# ТСР- и UDP-порты



# TCP- и UDP-порты



**Порт** - выделяемый для приложения (процесса) системный ресурс (очереди) для обмена данными с сетью.

Моя безопасность

Сетевая активность

Брандмауэр

Сетевая активность

Используемые порты

Проактивная защита

Активные процессы

Доступ к файлам и реестру

Журнал событий

Процесс	ID процесса	Направление, Протокол	Локальный адрес:Порт	Удаленный адрес:Порт	Отправлено/получено байт	Причина
<SYSTEM>	4				28 826 / 1 236 474	Открыто соединений: 1
<b>THUNDERBIRD.EXE</b>	<b>2724</b>				<b>24 719 / 195 515</b>	<b>Открыто соединений: 5</b>
THUNDERBIRD.EXE	2724	OUT TCP	localhost:loopback: 1037	localhost:loopback: 1036	0 / 4 027	Allow local TCP activity
THUNDERBIRD.EXE	2724	IN TCP	localhost:loopback: 1036	localhost:loopback: 1037	4 027 / 0	Allow local TCP activity
THUNDERBIRD.EXE	2724	OUT TCP	localhost:loopback: 1042	localhost:loopback: 1041	0 / 1 173	Allow local TCP activity
THUNDERBIRD.EXE	2724	IN TCP	localhost:loopback: 1041	localhost:loopback: 1042	1 173 / 0	Allow local TCP activity
THUNDERBIRD.EXE	2724	OUT TCP	nova: 1123	mail.gubkin.ru: 993	10 479 / 67 089	(SSL) Mozilla Thunderbird IMAP con.
<b>CHROME.EXE</b>	<b>1676</b>				<b>147 459 / 668 645</b>	<b>Открыто соединений: 52</b>
CHROME.EXE	1676	OUT TCP	nova: 2230	srv.marketmap.ru: HTTP	17 965 / 51 439	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2231	srv.marketmap.ru: HTTP	1 088 / 69 538	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2232	194.186.179.160: HTTP	681 / 37 277	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2233	87.242.88.6: HTTP	533 / 3 489	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2234	194.186.179.160: HTTP	681 / 37 277	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2235	srv.marketmap.ru: HTTP	13 961 / 21 563	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2236	srv.marketmap.ru: HTTP	12 715 / 10 320	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2237	srv.marketmap.ru: HTTP	13 445 / 10 545	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2239	srv.marketmap.ru: HTTP	15 240 / 30 208	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2240	host03.rax.ru: HTTP	938 / 983	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2241	bs.yandex.ru: HTTP	3 974 / 2 596	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2242	87.242.88.11: HTTP	0 / 1 136	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2243	srv.marketmap.ru: HTTP	3 494 / 5 414	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2244	bw-in-f139.1e100.net: HTTP	1 546 / 988	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2245	bw-in-f102.1e100.net: HTTP	1 251 / 818	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2246	www-12-02-snc5.facebook.com: HTTP	692 / 9 936	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2248	a92-122-190-58.deploy.akamaitech...	3 159 / 9 393	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2249	a92-122-190-58.deploy.akamaitech...	1 910 / 6 916	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2250	a92-122-190-58.deploy.akamaitech...	1 913 / 6 041	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2251	a92-122-190-58.deploy.akamaitech...	1 912 / 6 533	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2252	a92-122-190-58.deploy.akamaitech...	1 917 / 6 061	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2253	a92-122-190-58.deploy.akamaitech...	2 583 / 7 082	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2255	srv.marketmap.ru: HTTP	8 141 / 2 471	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2256	www.gubkin.ru: HTTP	2 114 / 10 856	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2257	87.242.88.21: HTTP	0 / 1 136	Google Chrome HTTP connection
CHROME.EXE	1676	OUT TCP	nova: 2258	195.10.39.82: HTTP	1 290 / 1 025	Google Chrome HTTP connection

Well-known ports: 0-1023

Registered ports: 1024–49151

Dynamic ports: 49152-65535

регистратор - IANA

<http://www.iana.org/assignments/port-numbers>

[http://ru.wikipedia.org/wiki/Список\\_портов\\_TCP\\_и\\_UD](http://ru.wikipedia.org/wiki/Список_портов_TCP_и_UD)

# Firewalls overview

## Proactive Security Challenge 64

<http://www.matousec.com/projects/proactive-security-challenge-64/results.php>

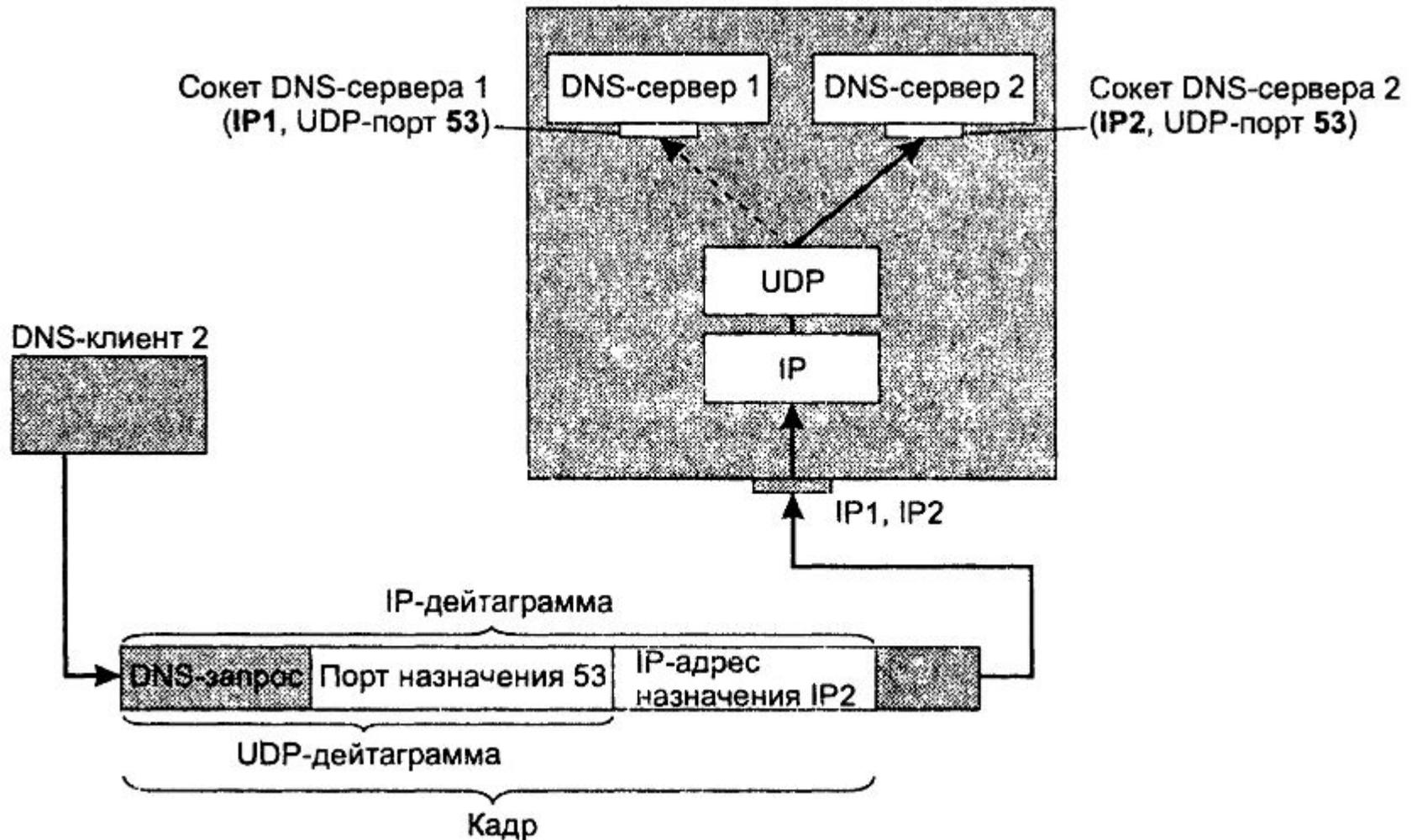
Products tested against the suite with 110 tests

	Product	Product score	Level reached	Protection level
	Comodo Internet Security Premium 6.3.297838.2953 <small>FREE</small>	97 %	11+	Excellent
	Outpost Security Suite Pro 8.0.4164.639.1856	90 %	11	Excellent
	Kaspersky Internet Security 2014 14.0.0.4651	88 %	11	Very good
	Privatefirewall 7.0.29.1 <small>FREE</small>	88 %	11	Very good
	SpyShelter Firewall 2.7	87 %	11	Very good
	Outpost Security Suite Free 7.1.1.3431.520.1248 <small>FREE</small>	71 %	11	Good
	VirusBuster Internet Security Suite 4.1	71 %	10	Good
	Jetico Personal Firewall 2.1.0.13.2471	58 %	10	Poor
	ESET Smart Security 6.0.316.0	55 %	9	Poor
	ZoneAlarm Extreme Security 2013 11.0.780.000	34 %	6	Very poor
	ZoneAlarm Free Antivirus + Firewall 11.0.768.000 <small>FREE</small>	34 %	6	Very poor
	Total Defense Internet Security Suite 8.0.0.215	31 %	6	Very poor
	Dr.Web Security Space 8.2.1.08220	24 %	4	None
	Webroot SecureAnywhere Complete 2013 8.0.2.174	22 %	4	None
	eScan Internet Security Suite 14.0.1400.1381	14 %	3	None
	K7 TotalSecurity 2013 13.1.0.188	9 %	2	None
	Norton Internet Security 2013 20.4.0.40	9 %	2	None
	avast! Internet Security 2014.9.0.2008	8 %	2	None
	TrustPort Total Protection 2013 13.0.10.5106	8 %	2	None
	Bitdefender Total Security 2013 16.30.0.1843	7 %	2	None
	Avira Internet Security 2013 13.0.0.4052	6 %	2	None
	PC Tools Internet Security 2012 9.1.0.2898	6 %	2	None
	FortKnox Personal Firewall 9.0.305.0	5 %	2	None
	F-Secure Internet Security 2014 12.89.202	5 %	2	None
	ThreatFire 4.7.0.53 <small>FREE</small>	5 %	2	None
	ArcaVir Internet Security 2013 13.4.6401.0	4 %	1	None
	G Data TotalProtection 2014 24.0.1.5	4 %	1	None
	Norman Security Suite PRO 10.00	4 %	1	None
	Ad-Aware Total Security 21.1.0.30	3 %	1	None
	AVG Internet Security 2013.0.3392	3 %	1	None
	BullGuard Internet Security 2013 13.0.262	3 %	1	None
	McAfee Total Protection 2013 12.1.323	3 %	1	None

# Сокеты

Сокет (socket) - пара (IP-адрес, номер порта)

Прикладной процесс однозначно идентифицируется сокетом в пределах сети и хоста.



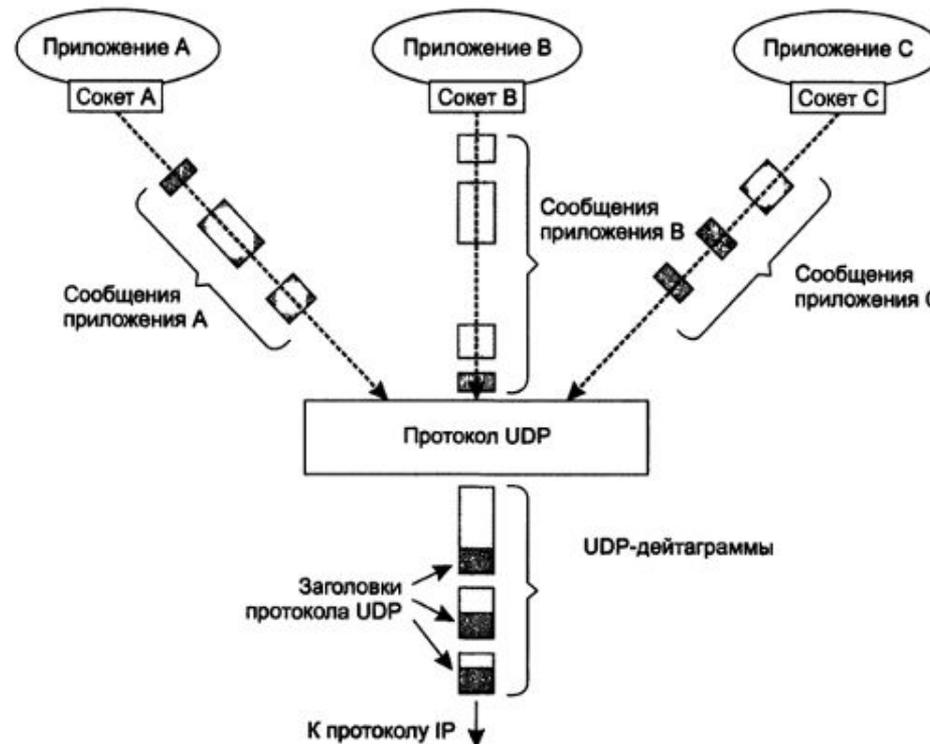
# Протокол UDP

**Порт отправителя** — 0, если не используется  
(Ipv4, Ipv6)

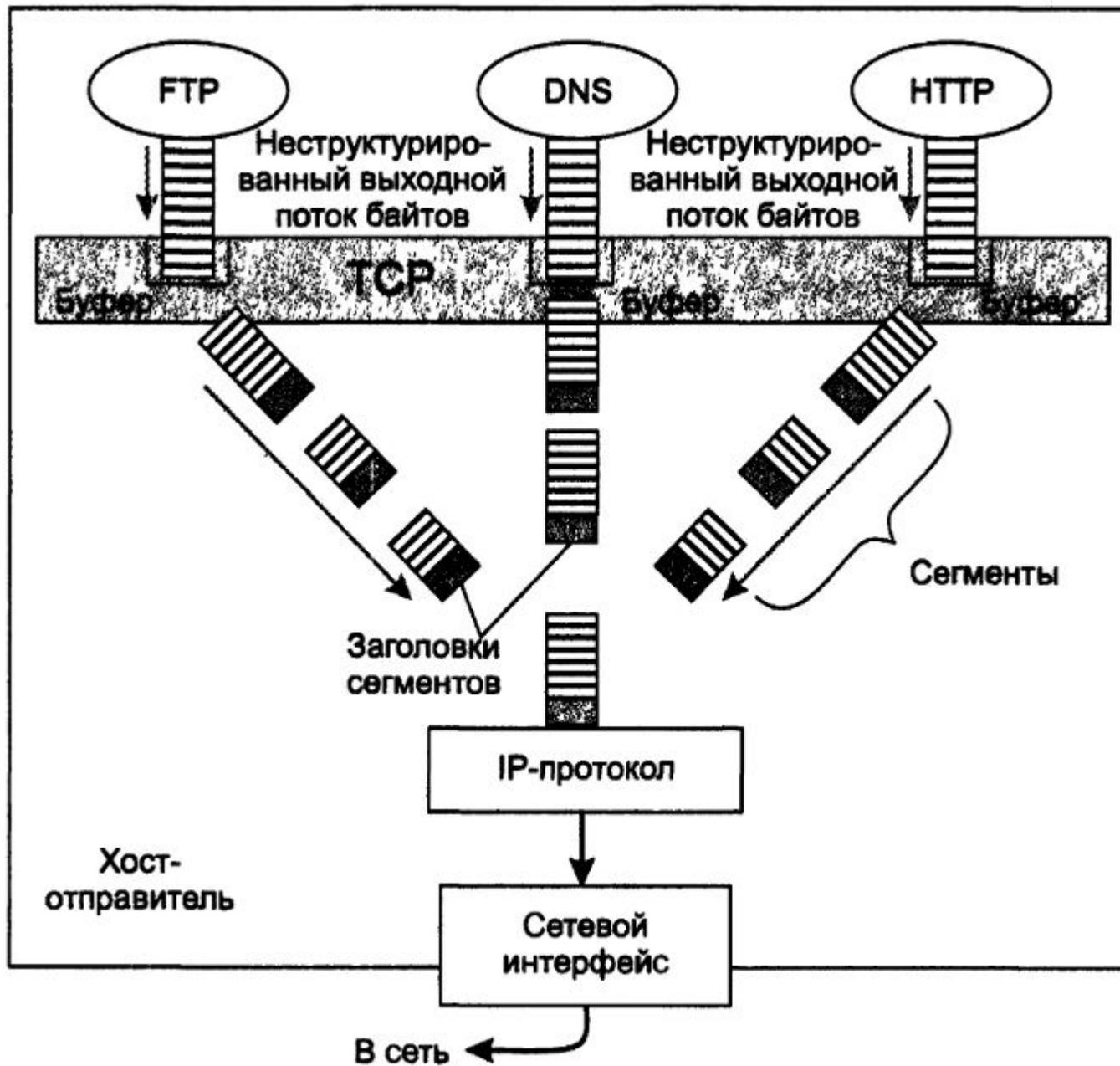
**Длина** — заголовок+данные в байтах  
Min — 8 byte  
Max - 65 507 byte  
(65,535 - 8 byte UDP header - 20 byte IP header)

**Контрольная сумма** — заголовок+данные  
0, если не используется (IPv4)

bits	0 – 15	16 – 31
0	Source Port Number	Destination Port Number
32	Length	Checksum
64	Data	



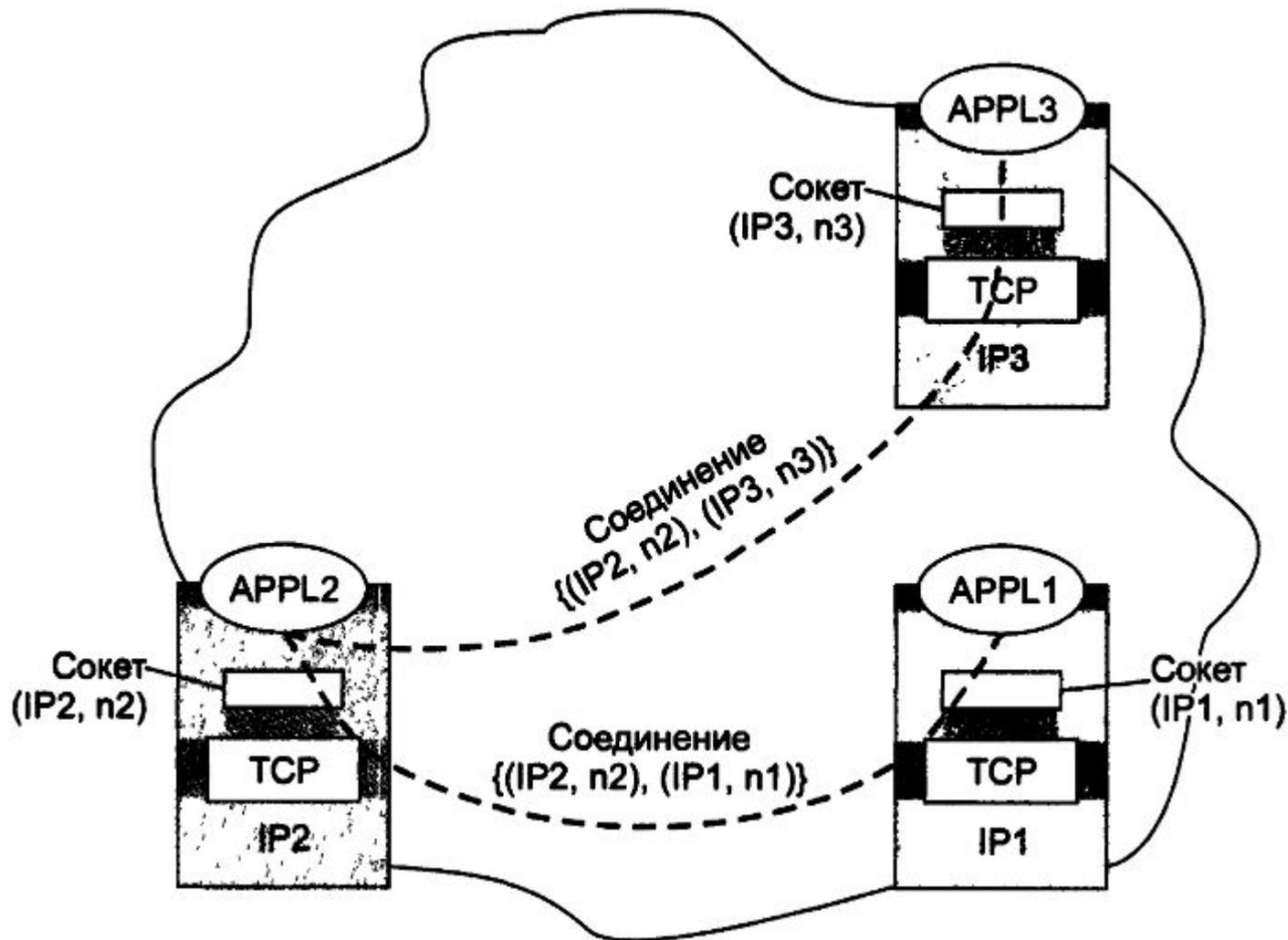
# Протокол ТСР. Мультиплексирование



# Протокол TCP.

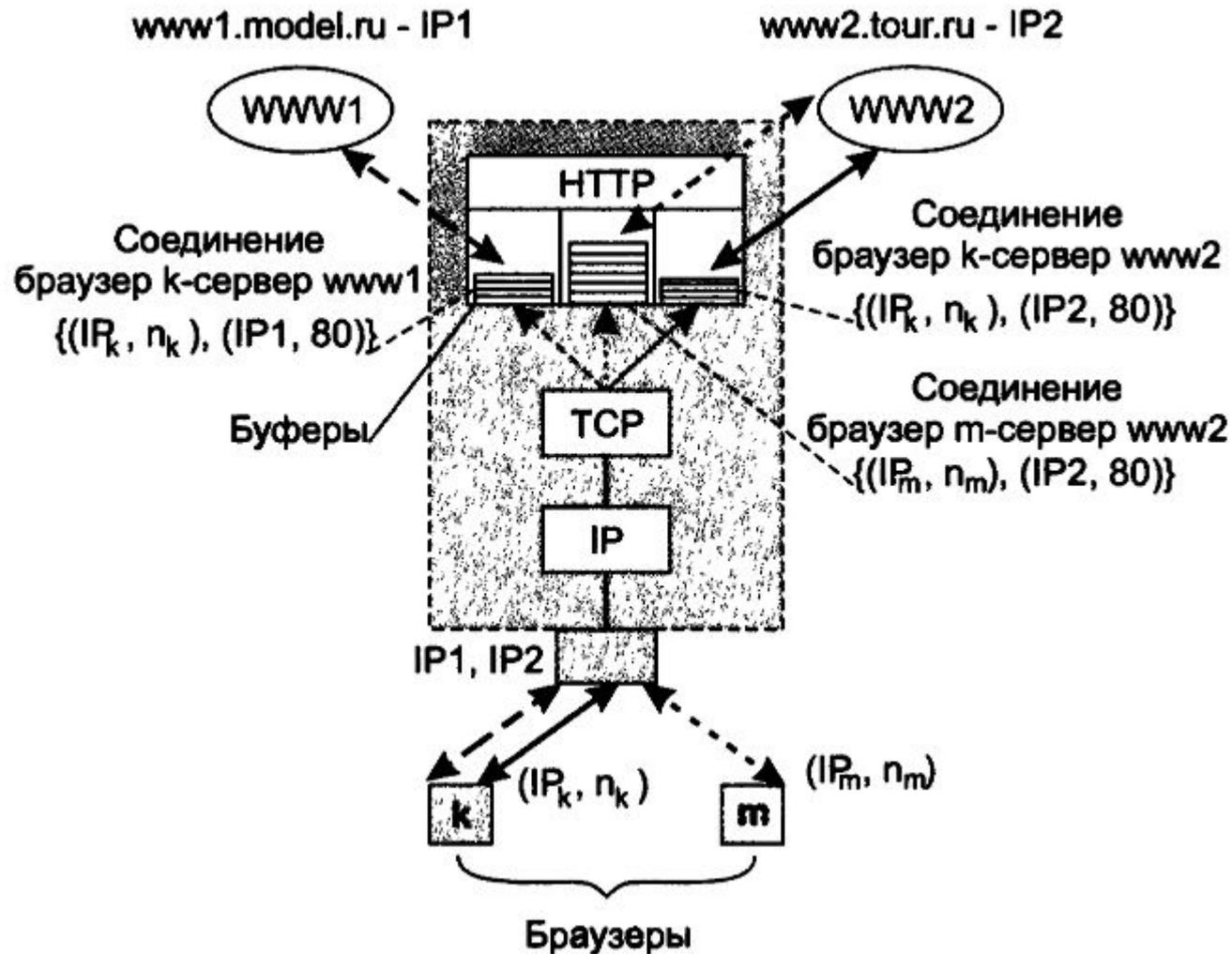
## Логическое соединение

Логическое соединение однозначно идентифицируется парой сокетов

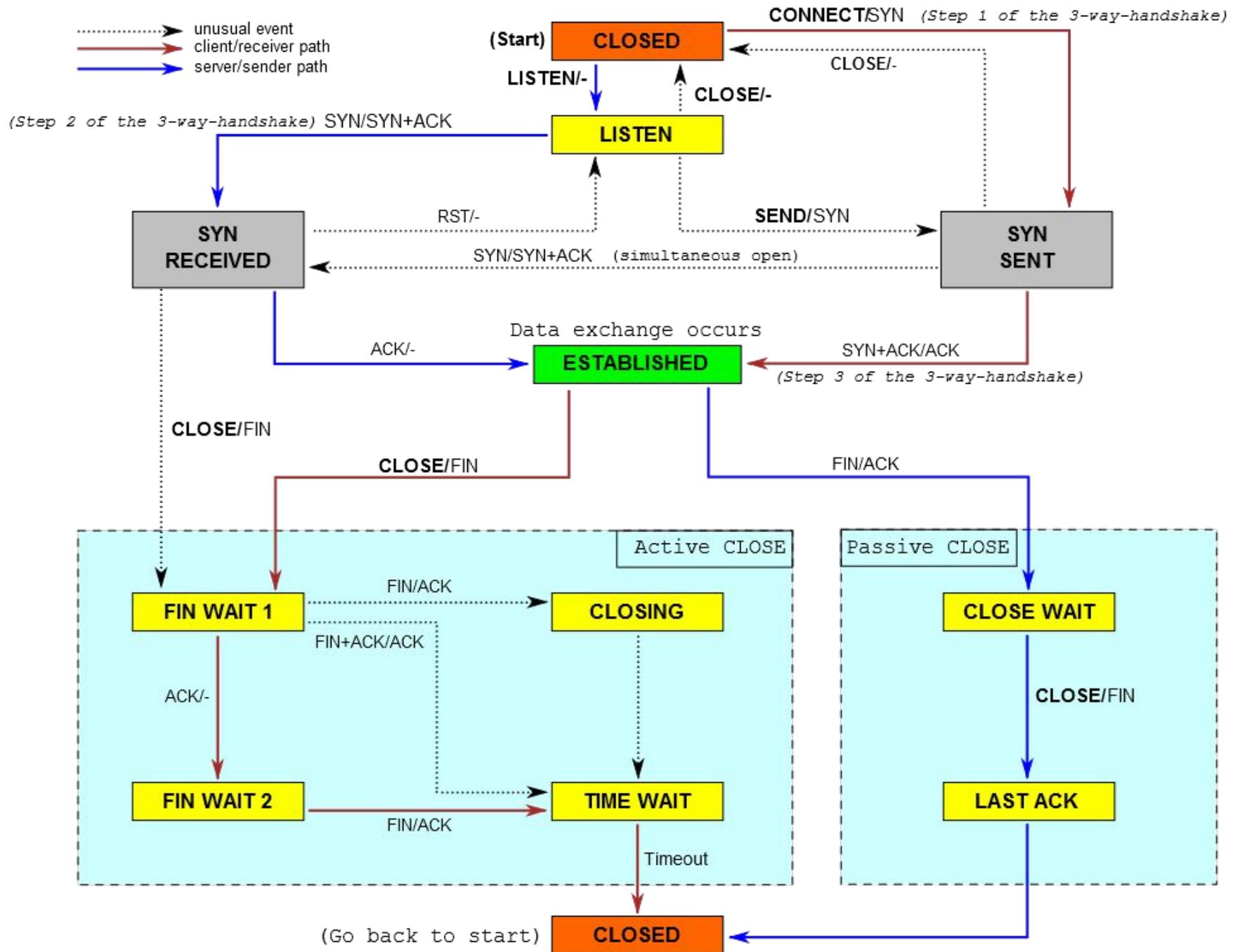


# Протокол ТСР.

## Демультимплексирование на основе соединения



# Диаграмма состояний TCP



# Протокол TCP.

## Заголовок

Bit offset	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
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset				Reserved				C	E	U	A	P	R	S	F	Window Size															
								W	R	R	C	S	S	S	Y	I																
								R	E	G	K	H	T	N	N																	
128	Checksum																Urgent pointer															
160	Options (if Data Offset > 5)																								padding							
...	...																															

Последовательный номер — смещение сегмента относительно потока

Подтвержденный номер — максимальный номер байта в полученном сегменте + 1

Длина заголовка — количество 4-байтных слов в заголовке (5-15)

URG — Указатель важности (Urgent pointer field is significant)

ACK — Номер подтверждения (Acknowledgement field is significant)

PSH — (Push function)

RST — Оборвать соединения, сбросить буфер (Reset the connection)

SYN — Синхронизация номеров последовательности (Synchronize sequence numbers)

FIN — завершение соединения (FIN bit)

Размер окна – размер данных в байтах, которое отправитель может передать

без подтверждения