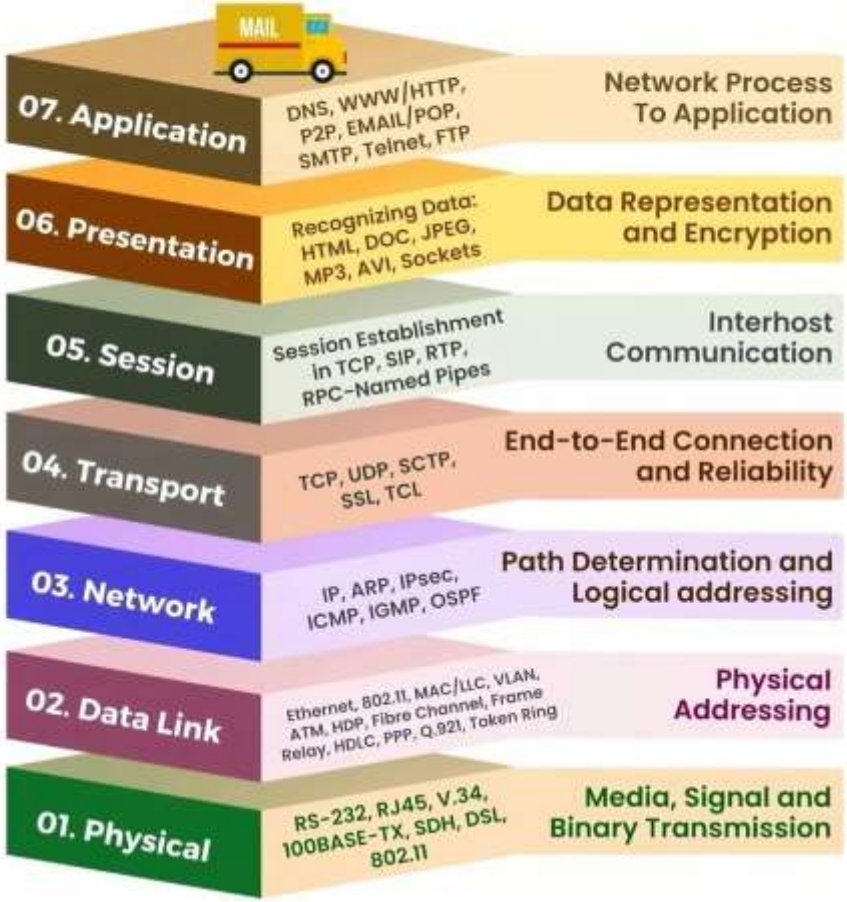
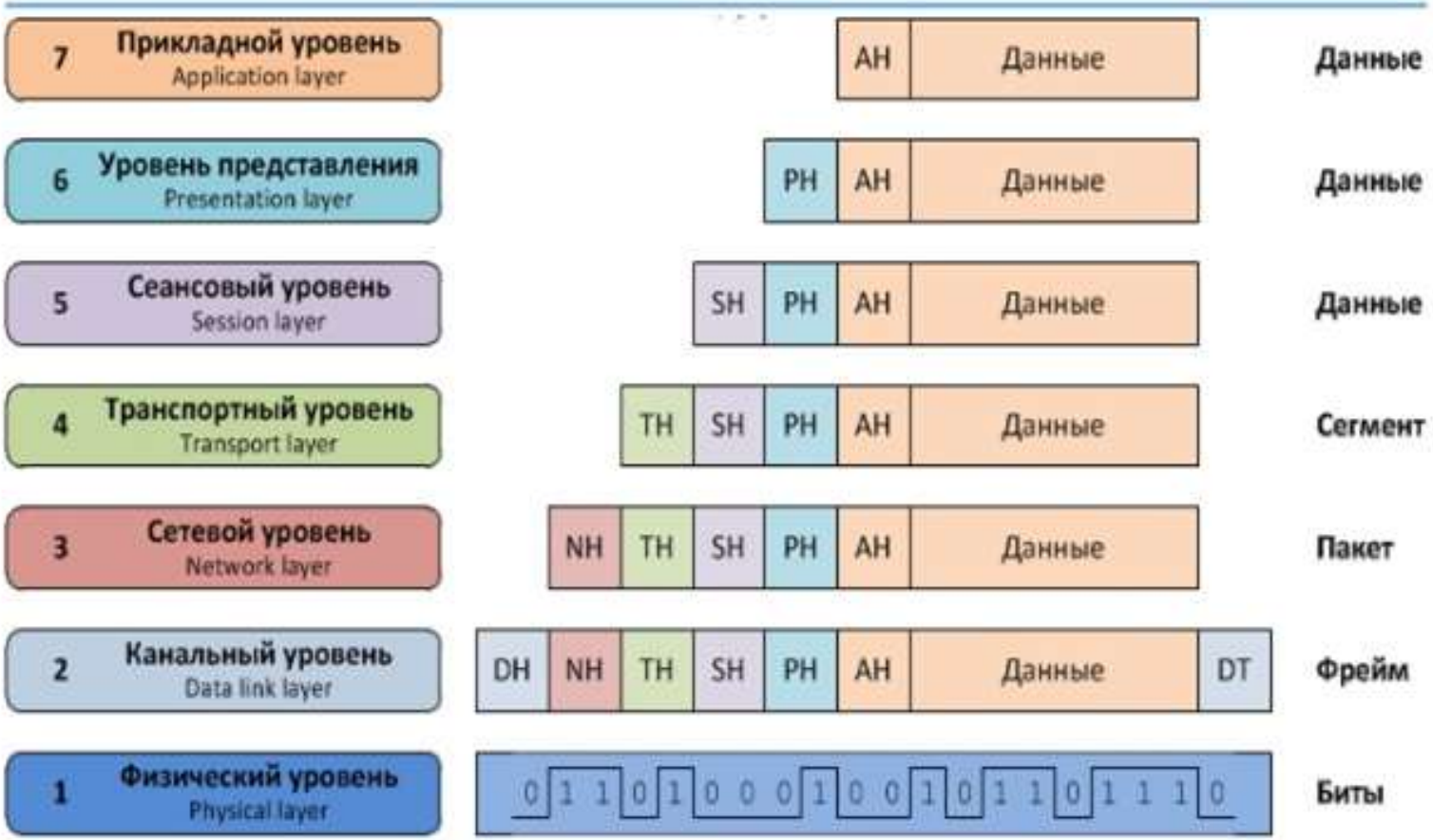
THE 7 LAYERS OF OSI MODEL



TCP/IP модель


7 Прикладной уровень Application layer
AH Данные
Данные
6 Уровень представления Presentation layer
PH AH Данные
Данные
5 Сеансовый уровень Session layer
SH PH AH Данные
Данные
4 Транспортный уровень Transport layer
TH SH PH AH Данные
Сегмент
3 Сетевой уровень Network layer
NH TH SH PH AH Данные
Пакет
2 Канальный уровень Data link layer
DH NH TH SH PH AH Данные DT
Фрейм
1 Физический уровень Physical layer
0 1 1 0 1 0 0 0 1 0 0 1 0 1 1 0 1 1 1 0
Биты


Компьютер-отправитель
Компьютер-получатель
Виртуальная связь
Прикладной
Представительский
Сеансовый
Транспортный
Сетевой
Канальный
Физический
Физическая среда
Прикладной
Представительский
Сеансовый
Транспортный
Сетевой
Канальный
Физический

MAC-адрес

MAC-адрес

Уникальный идентификатор сетевого интерфейса (обычно сетевой карты) для реализации коммуникации устройств в сети на физическом уровне.

Длинна MAC-адреса - 48 бит, что обеспечивает 281474976710656 общее число всех возможных адресов. Как правило, MAC-адрес записывается как шесть групп двойных шестнадцатеричных чисел, разделенных символами "-" или ":".
Например, MAC-адрес может выглядеть так - "**00:11:22:33:44:55**", или так - "**67-78-89-AB-CD-EF**".

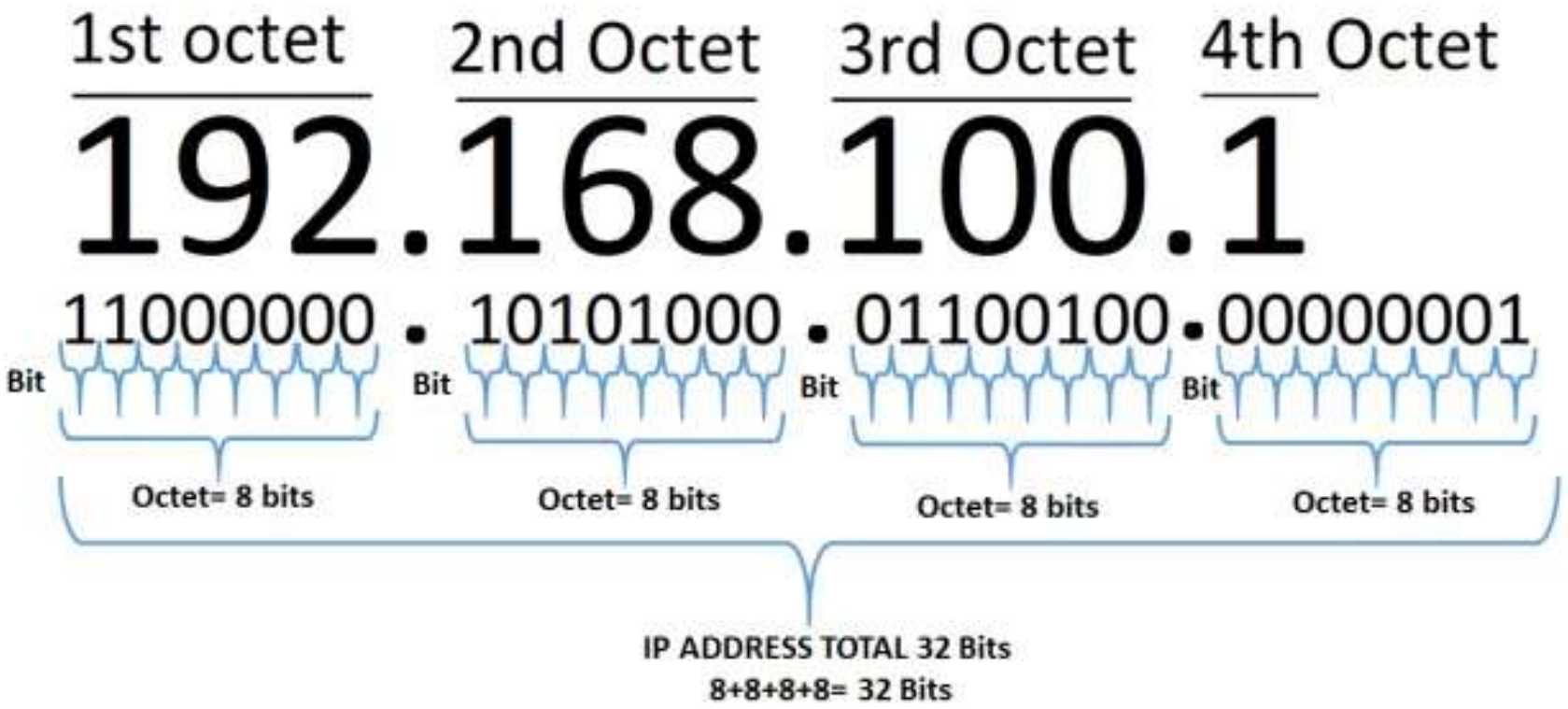
IP-адрес

IP-адрес

Internet Protocol Address — уникальный идентификатор устройства (обычно компьютера), подключенного к локальной сети или Интернету.

90.189.165.13 - внешний (публичный)
192.168.1.5 - внутренний (локальный)

Структура IP



IP vs MAC

MAC адрес	IP адрес
Работает на канальном уровне	Работает на сетевом уровне
Является физическим адресом	Является логическим адресом
Фиксирован	Изменяется при перемещении устройств из одной сети в другую
Длина адреса 48 бит	Длина адреса 32 бита (для IPv4)

Сетевые протоколы
Сниффинг и крафтинг

Маска подсети

Определение границ подсети

Не может быть маски
120.22.123.12=01111000.00010110.01111011.00001100

Но может быть маска
255.255.248.0=11111111.11111111.11111000.00000000

Запись

Короткая: 192.168.11.10/21

Длинная 192.168.11.10 255.255.248.0

пример **192.168.11.10/21**:

11000000.10101000.00001011.00001010
11111111.11111111.11111000.00000000

11000000.10101000.00001000.00000000 = 192.168.8.0

Сетевая маска	Инверсия	Префикс	Используется	Размер
0.0.0.0	255.255.255.255	/0	4,294,967,294	весь интернет
128.0.0.0	127.255.255.255	/1	2,147,483,646	128 классов 'a'
192.0.0.0	63.255.255.255	/2	1,073,741,822	64 класса 'a'
224.0.0.0	31.255.255.255	/3	536,870,910	32 класса 'a'
240.0.0.0	15.255.255.255	/4	268,435,454	16 классов 'a'
248.0.0.0	7.255.255.255	/5	134,217,726	8 классов 'a'
252.0.0.0	3.255.255.255	/6	67,108,862	4 класса 'a'
254.0.0.0	1.255.255.255	/7	33,554,430	2 класса 'a'
255.0.0.0	0.255.255.255	/8	16,777,214	1 класс 'a'
255.128.0.0	0.127.255.255	/9	8,388,606	128 классов 'b'
255.192.0.0	0.63.255.255	/10	4,194,302	64 класса 'b'
255.224.0.0	0.31.255.255	/11	2,097,150	32 класса 'b'
255.240.0.0	0.15.255.255	/12	1,048,574	16 классов 'b'
255.248.0.0	0.7.255.255	/13	524,286	8 классов 'b'
255.252.0.0	0.3.255.255	/14	262,142	4 класса 'b'
255.254.0.0	0.1.255.255	/15	131,070	2 класса 'b'
255.255.0.0	0.0.255.255	/16	65,534	1 класс 'b'
255.255.128.0	0.0.127.255	/17	32,766	128 классов 'c'
255.255.192.0	0.0.63.255	/18	16,382	64 класса 'c'
255.255.224.0	0.0.31.255	/19	8,190	32 класса 'c'
255.255.240.0	0.0.15.255	/20	4,094	16 классов 'c'
255.255.248.0	0.0.7.255	/21	2,046	8 классов 'c'
255.255.252.0	0.0.3.255	/22	1,022	4 класса 'c'
255.255.254.0	0.0.1.255	/23	510	2 классов 'c'
255.255.255.0	0.0.0.255	/24	254	1 класс 'c'
255.255.255.128	0.0.0.127	/25	126	128 хостов
255.255.255.192	0.0.0.63	/26	62	64 хоста
255.255.255.224	0.0.0.31	/27	30	32 хоста
255.255.255.240	0.0.0.15	/28	14	16 хостов
255.255.255.248	0.0.0.7	/29	6	8 хостов
255.255.255.252	0.0.0.3	/30	2	4 хоста
255.255.255.254	0.0.0.1	/31	0	2 хоста
255.255.255.255	0.0.0.0	/32	1	1 хост

Шлюз и broadcast

Шлюз - обычно это первый адрес сети. Через него обеспечивается взаимодействие между локальной и внешней сетью

Broadcast - широковещательный адрес. Это всегда последний адрес сети. Отправляя сообщение на него, его получат все пользователи подсети. Используется для широковещательных запросов (DNS, ARP, и т.д.)

Задача 1

Найдите подсеть для 192.168.5.13/24

Найдите шлюз для адреса 10.0.0.5 и маски /30

Какая минимальная маска сети подойдёт для адресов в диапазоне от 172.0.16.5 до 172.0.16.13

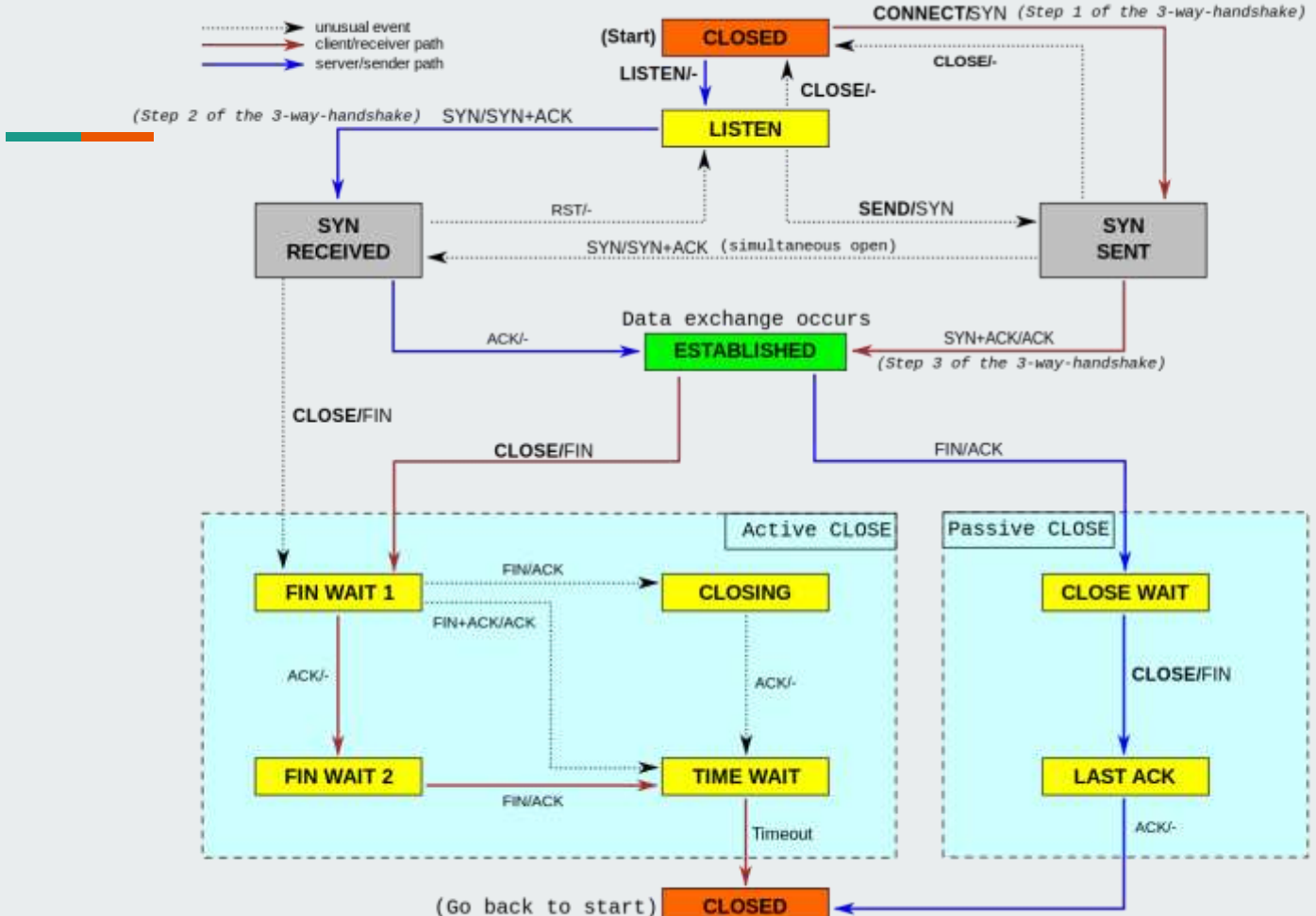
Статический и динамический IP

Статика (установлен вручную)
Благодаря протоколу DHCP (назначается роутером или шлюзом)

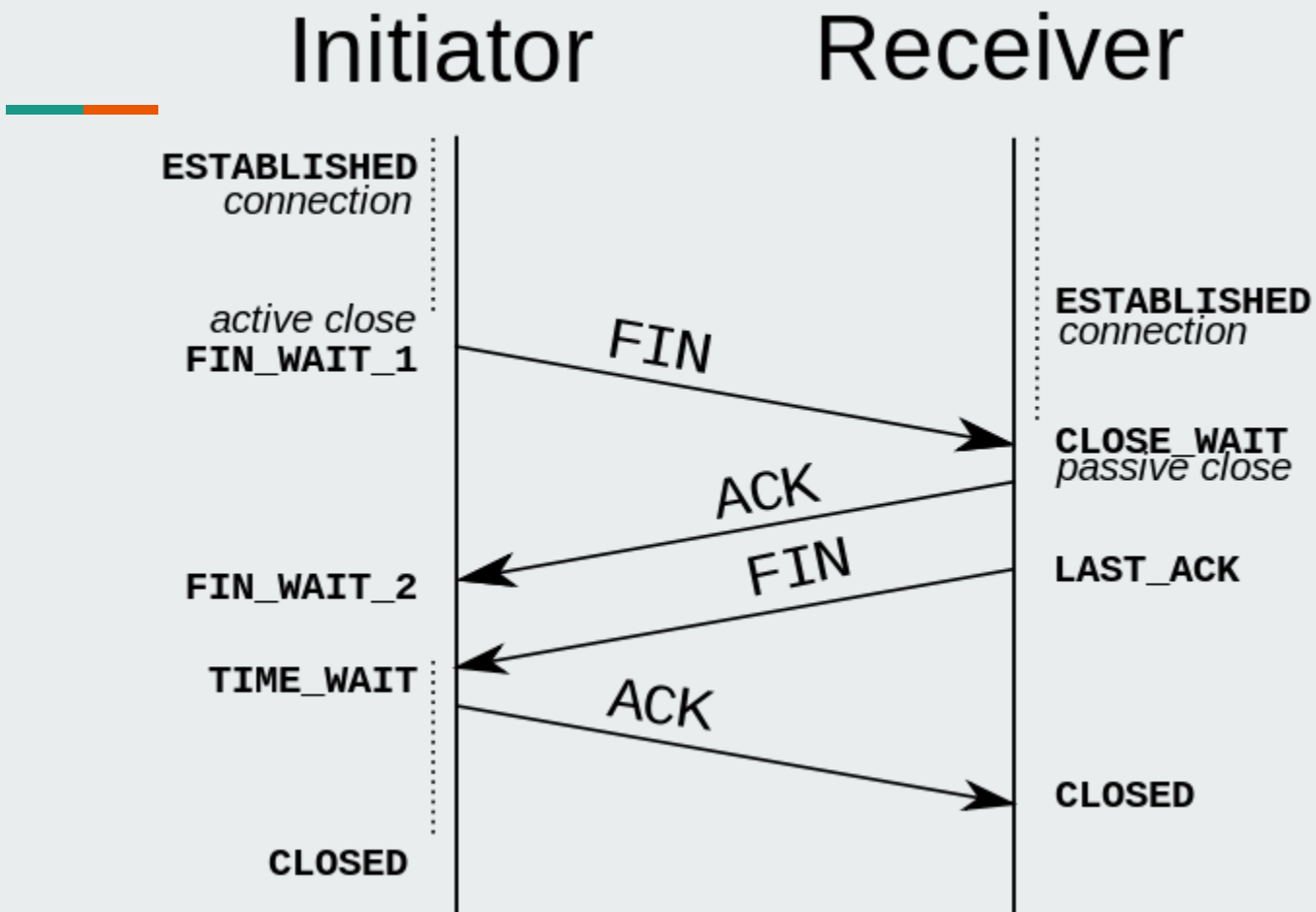
TCP и UDP

Transmission control Protocol
User Datagram Protocol

Жизненный цикл



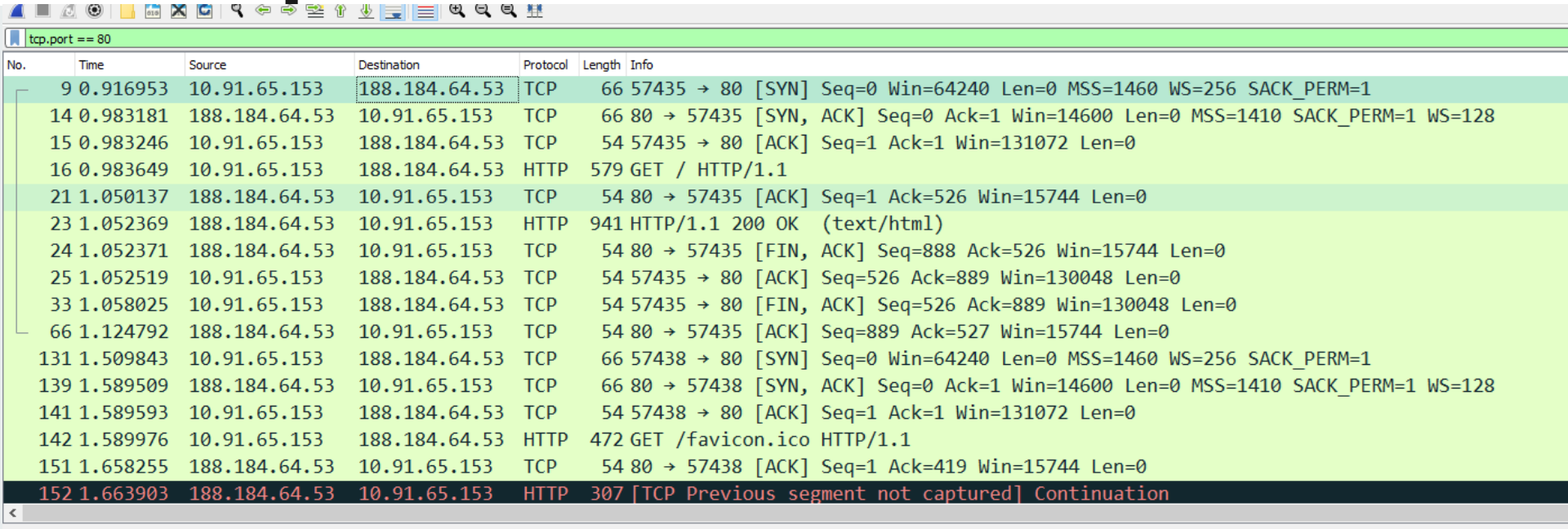
Установление соединения



Задача 3

Расчехлить WireShark
Поставить фильтр tcp.port == 80
Открыть сайт info.cern.ch
Остановить WireShark
Посмотреть последовательность установления TCP-соединения

help



tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
9	0.916953	10.91.65.153	188.184.64.53	TCP	66	57435 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	0.983181	188.184.64.53	10.91.65.153	TCP	66	80 → 57435 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1410 SACK_PERM=1 WS=128
15	0.983246	10.91.65.153	188.184.64.53	TCP	54	57435 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
16	0.983649	10.91.65.153	188.184.64.53	HTTP	579	GET / HTTP/1.1
21	1.050137	188.184.64.53	10.91.65.153	TCP	54	80 → 57435 [ACK] Seq=1 Ack=526 Win=15744 Len=0
23	1.052369	188.184.64.53	10.91.65.153	HTTP	941	HTTP/1.1 200 OK (text/html)
24	1.052371	188.184.64.53	10.91.65.153	TCP	54	80 → 57435 [FIN, ACK] Seq=888 Ack=526 Win=15744 Len=0
25	1.052519	10.91.65.153	188.184.64.53	TCP	54	57435 → 80 [ACK] Seq=526 Ack=889 Win=130048 Len=0
33	1.058025	10.91.65.153	188.184.64.53	TCP	54	57435 → 80 [FIN, ACK] Seq=526 Ack=889 Win=130048 Len=0
66	1.124792	188.184.64.53	10.91.65.153	TCP	54	80 → 57435 [ACK] Seq=889 Ack=527 Win=15744 Len=0
131	1.509843	10.91.65.153	188.184.64.53	TCP	66	57438 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
139	1.589509	188.184.64.53	10.91.65.153	TCP	66	80 → 57438 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1410 SACK_PERM=1 WS=128
141	1.589593	10.91.65.153	188.184.64.53	TCP	54	57438 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
142	1.589976	10.91.65.153	188.184.64.53	HTTP	472	GET /favicon.ico HTTP/1.1
151	1.658255	188.184.64.53	10.91.65.153	TCP	54	80 → 57438 [ACK] Seq=1 Ack=419 Win=15744 Len=0
152	1.663903	188.184.64.53	10.91.65.153	HTTP	307	[TCP Previous segment not captured] Continuation

```
> Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{701B32A9-5C9E-4B64-A7D0-0B124E39D26D}, id 0
> Ethernet II, Src: IntelCor_b9:6d:06 (d0:ab:d5:b9:6d:06), Dst: Routerbo_26:15:9c (cc:2d:e0:26:15:9c)
> Internet Protocol Version 4, Src: 10.91.65.153, Dst: 188.184.64.53
> Transmission Control Protocol, Src Port: 57435, Dst Port: 80, Seq: 0, Len: 0
```

Воспользуйтесь функцией Follow > tcp stream

ICMP

Протокол ping-a

обслуживание функции контроля правильности работы сети. С его помощью передаются всякого рода, низкоуровневые сводки, с раскроенными неправильностями во время сетевых связей

Заголовок в 4 байта - первый байт определяет тип пакета, второй - код операции, третий и четвёртый представляют собой контрольную сумму.

Задача 4

Выполните следующие команды:

ping -t 3 ya.ru

ping -A ya.ru

ping -w 2 5.5.5.5

Telnet

Устаревший протокол, для обмена текстовыми данными

подключитесь к info.cern.ch
отправьте запрос GET из задачи №3
получите ответ и сравните его с тем, что был в 3 задании

Задача 5

подключитесь через **netcat** на адрес 188.130.155.122 и tcp-порт 6000
посмотрите на трафик в WireShark (фильтр **tcp.port == 6000**)
переподключитесь на udp-порт 6000
сравните запись трафика

FTP

Протокол передачи данных, можно управлять из консоли, например

```
nc ftp.mcafee.com 21
220 Welcome to ProXad FTP server
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
pwd
257 "/" is the current directory
```

Команды FTP

ABOR	ADAT	ALLO	APPE	AUTH	CDUP	CLNT	CWD
DELE	EPRT	EPSV	FEAT	HASH	HELP	LIST	MDTM
MFMT	MKD	MLSD	MLST	MODE	NLST	NOOP	NOP
OPTS	PASS	PASV	PBSZ	PORT	PROT	PWD	QUIT
REST	RETR	RMD	RNFR	RNTO	SITE	SIZE	STOR
STRU	SYST	TYPE	USER	XCUP	XCWD	XMKD	XPWD
XRMD							

Задача 6

Запустите WireShark
Откройте **ftp://ftp.uni-erlangen.de/** в браузере
Побродите по FTP, запишите трафик
Скачайте пару файлов
Остановите WireShark, после этого сделайте фильтр: **ftp-data**
Сохраните себе данные файлы ещё раз
Проверьте, есть ли файлы в
File > Export objects > HTTP

Задача 7 и 8

сайт root-me.org
раздел Network
Задачи
- Telnet - authentication
- FTP - authentication

HTTP

Протокол, позволяющий получать различные ресурсы, например HTML-документы

Типы запросов

GET - получить
PUT - создать
POST - отправить (форму)
PATCH - изменить
DELETE – удалить
OPTIONS – получить заголовки от сервера (инфа про то, как будет построена коммуникация с сервером)

Номера ответов

200 - OK
204 - No Content
301 - Moved Permanently
401 - Unauthorized
403 - Forbidden
405 - Not Allowed
502 - Bad Gateway
418 – I’m a teapot
…

Значения

1XX – Информативы
2XX – Все ок
3XX – Перенаправление
4XX – Ошибка на стороне браузера клиента
5XX – Ошибка на стороне сервера

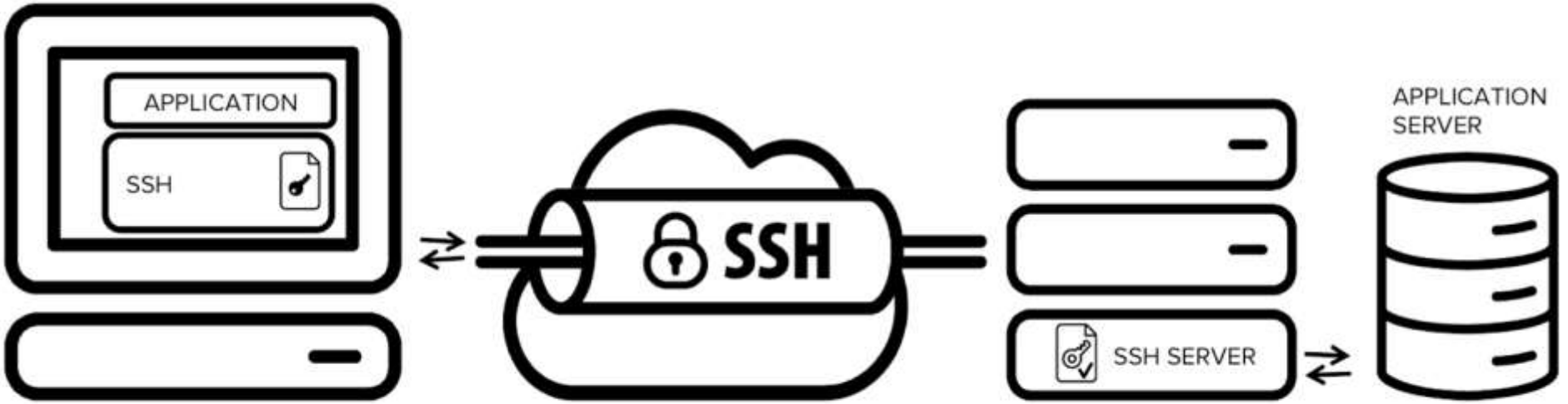
Заголовки HTTP

User-Agent
Accept
Authorizations
Cache-Control
Content-Type
ETag

Задача 9

Откройте любой сайт по HTTP (например http://eng.rzd.ru/)
Заранее включите WireShark
Поставьте фильтр по http
Посмотрите заголовки запроса и ответа (например, через **follow > Tcp Stream** (или HTTP-stream)

SSH



Secure SHell - защищенный протокол для удаленного доступа к компьютерам. Через SSH можно выполнять операции в командной строке компьютера, который физически находится в другом месте. Иными словами, SSH — это дистанционная командная строка. Визуально вы работаете на своем компьютере, но в реальности — на другом. Отличная замена telnet.

Установление соединения