

# Анализ влияния NAT на контрольные суммы TCP и UDP

Дунайцев Р.А. (СПбГУТ)

[roman.dunaytsev@spbgut.ru](mailto:roman.dunaytsev@spbgut.ru)

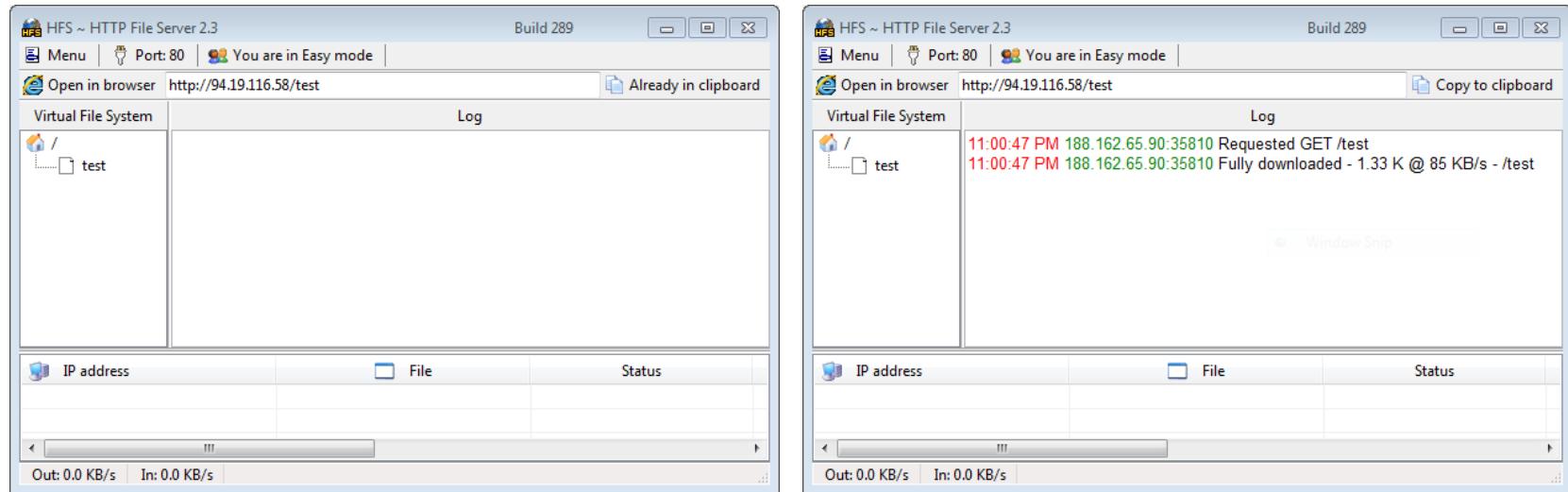
# Краткая теоретическая справка

- IP-адрес считается глобально маршрутизуемым, если любой правильно настроенный маршрутизатор в сети Интернет может построить маршрут пакета так, что тот в конечном счете достигнет узла с этим IP-адресом. Для этого любой глобально маршрутизуемый адрес должен быть присвоен только одному узлу. Чтобы обеспечить уникальность глобально маршрутизуемых адресов, организация IANA (Internet Assigned Numbers Authority) и ее филиалы распределяют отдельные блоки IP-адресов между крупными организациями, такими как корпорации, университеты и Интернет-провайдеры, которые затем могут передавать эти адреса своим сотрудникам и клиентам, гарантируя уникальность каждого адреса. Так как IPv4 имеет лишь 32-битное адресное пространство, теоретически существует 4.294.967.296 глобальных IP-адресов. Из-за стремительного роста числа сетевых устройств и особенностей распределения IP-адресов организацией IANA это количество оказалось недостаточным. К счастью, благодаря механизму преобразования сетевых адресов (**Network Address Translation, NAT**) существует возможность подключения к сети Интернет целой подсети, имея единственный глобальный IP-адрес. Чтобы настроить NAT, каждому узлу в этой подсети нужно присвоить локально маршрутизуемый IP-адрес. Обеспечивать уникальность таких адресов не требуется, потому что адреса не являются глобально маршрутизуемыми. В настоящее время NAT используется повсеместно, особенно в домашних сетях и сетях небольших организаций.

# Задание на дом

- Экспериментальным путем выяснить, пересчитываются ли контрольные суммы TCP при использовании NAT
  - 1) Найти 2 ПК, один с публичным IP-адресом (например, выдается некоторыми Интернет-провайдерами), а другой с частным IP-адресом
  - 2) Установить между ними TCP-соединение. В качестве сервера можно использовать бесплатную и не требующую установки программу HFS <https://www.rejetto.com/hfs/>
  - 3) С помощью Wireshark собрать пакеты этого TCP-соединения на той и другой стороне (т.е. захват трафика должен выполняться **одновременно как на клиенте, так и на сервере**)
  - 4) Сравнить контрольную сумму **одного и того же** TCP-сегмента, захваченного Wireshark при отправке клиентом и получении сервером. Для сравнения лучше использовать TCP-сегмент с HTTP-запросом GET, как уникальный и легко узнаваемый
  - 5) В качестве альтернативы эксперимент можно провести с UDP
  - 6) К отчету приложить собранные Wireshark пакеты!

# HFS ~ HTTP File Server



# Запрос GET на стороне клиента

client-yota-10.0.0.10.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.10	94.19.116.58	TCP	66	49506 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
2	0.153417	94.19.116.58	10.0.0.10	TCP	66	80 → 49506 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1360 WS=256 SACK_PERM=1
3	0.153524	10.0.0.10	94.19.116.58	TCP	54	49506 → 80 [ACK] Seq=1 Ack=1 Win=66640 Len=0
4	0.153786	10.0.0.10	94.19.116.58	HTTP	344	GET /test HTTP/1.1
5	0.405124	94.19.116.58	10.0.0.10	TCP	320	80 → 49506 [PSH, ACK] Seq=1 Ack=291 Win=66560 Len=266 [TCP segment of a reassembled PDU]
6	0.405342	94.19.116.58	10.0.0.10	HTTP	1414	HTTP/1.1 200 OK
7	0.405375	10.0.0.10	94.19.116.58	TCP	54	49506 → 80 [ACK] Seq=291 Ack=1627 Win=66640 Len=0
8	5.171183	10.0.0.10	94.19.116.58	TCP	54	49506 → 80 [FIN, ACK] Seq=291 Ack=1627 Win=66640 Len=0
9	5.206225	94.19.116.58	10.0.0.10	TCP	54	80 → 49506 [ACK] Seq=1627 Ack=292 Win=66560 Len=0

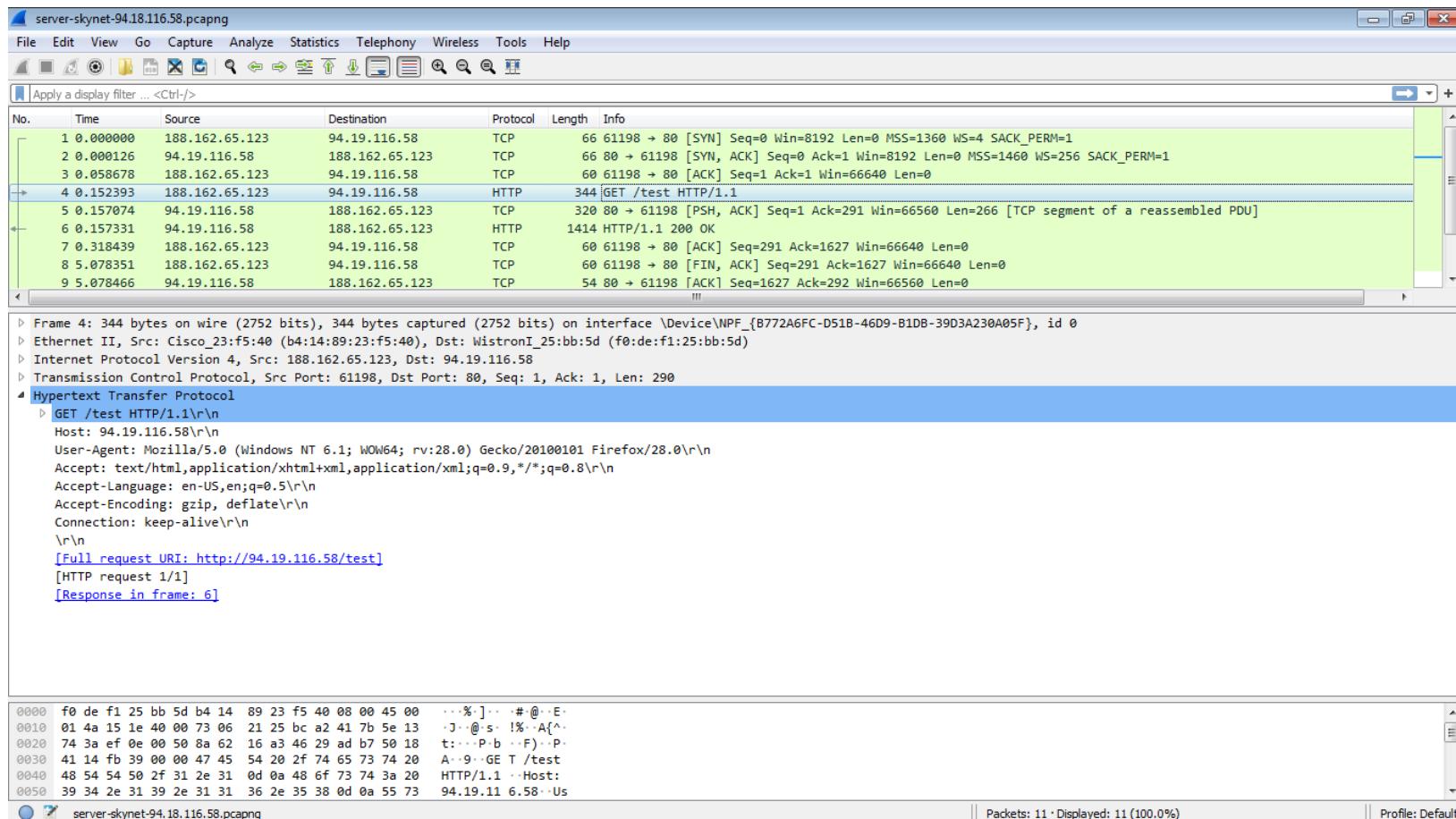
Frame 4: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF\_{BD9A8DA3-4074-4B91-93C1-98AD26C74AF4}, id 0  
Ethernet II, Src: HyundaiIn\_f0:1a:40 (00:09:3b:f0:1a:40), Dst: GCTSemic\_f0:16:70 (00:0a:3b:f0:16:70)  
Internet Protocol Version 4, Src: 10.0.0.10, Dst: 94.19.116.58  
Transmission Control Protocol, Src Port: 49506, Dst Port: 80, Seq: 1, Ack: 1, Len: 290

Hypertext Transfer Protocol  
GET /test HTTP/1.1\r\nHost: 94.19.116.58\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n\r\n[Full request URI: http://94.19.116.58/test]  
[HTTP request 1/1]  
[Response in frame: 6]

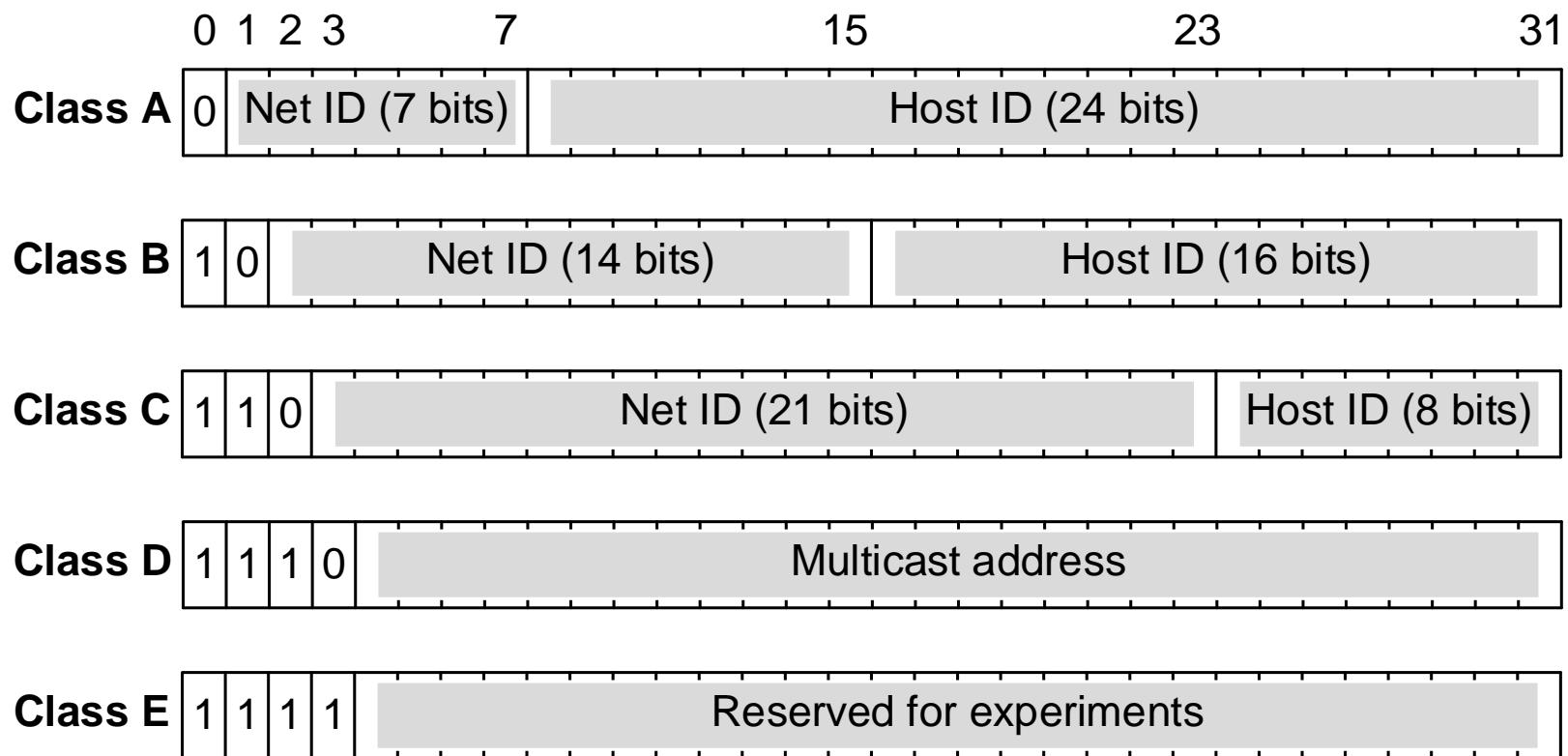
0000 00 0a 3b f0 16 70 00 09 3b f0 1a 40 08 00 45 00 ..; p.. ;:@ E.  
0010 01 4a 15 1e 40 00 80 06 08 39 0a 00 00 0a 5e 13 J:@... 9...^.  
0020 74 3a c1 62 00 50 47 64 40 bb 7c da a1 b8 50 18 t:b PGd @ | ..P.  
0030 41 14 0b 2e 00 00 47 45 54 20 2f 74 65 73 74 20 A...GE T /test  
0040 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:  
0050 39 34 2e 31 39 2e 31 31 36 2e 35 38 0d 0a 55 73 94.19.116.58..Us

Packets: 11 · Displayed: 11 (100.0%) | Profile: Default

# Запрос GET на стороне сервера



# Классовая адресация



# Публичные IP-адреса стоят денег

File Edit View History Bookmarks Tools Help

Аренда, покупка и продажа IP-адресов https://ipaddress.ru

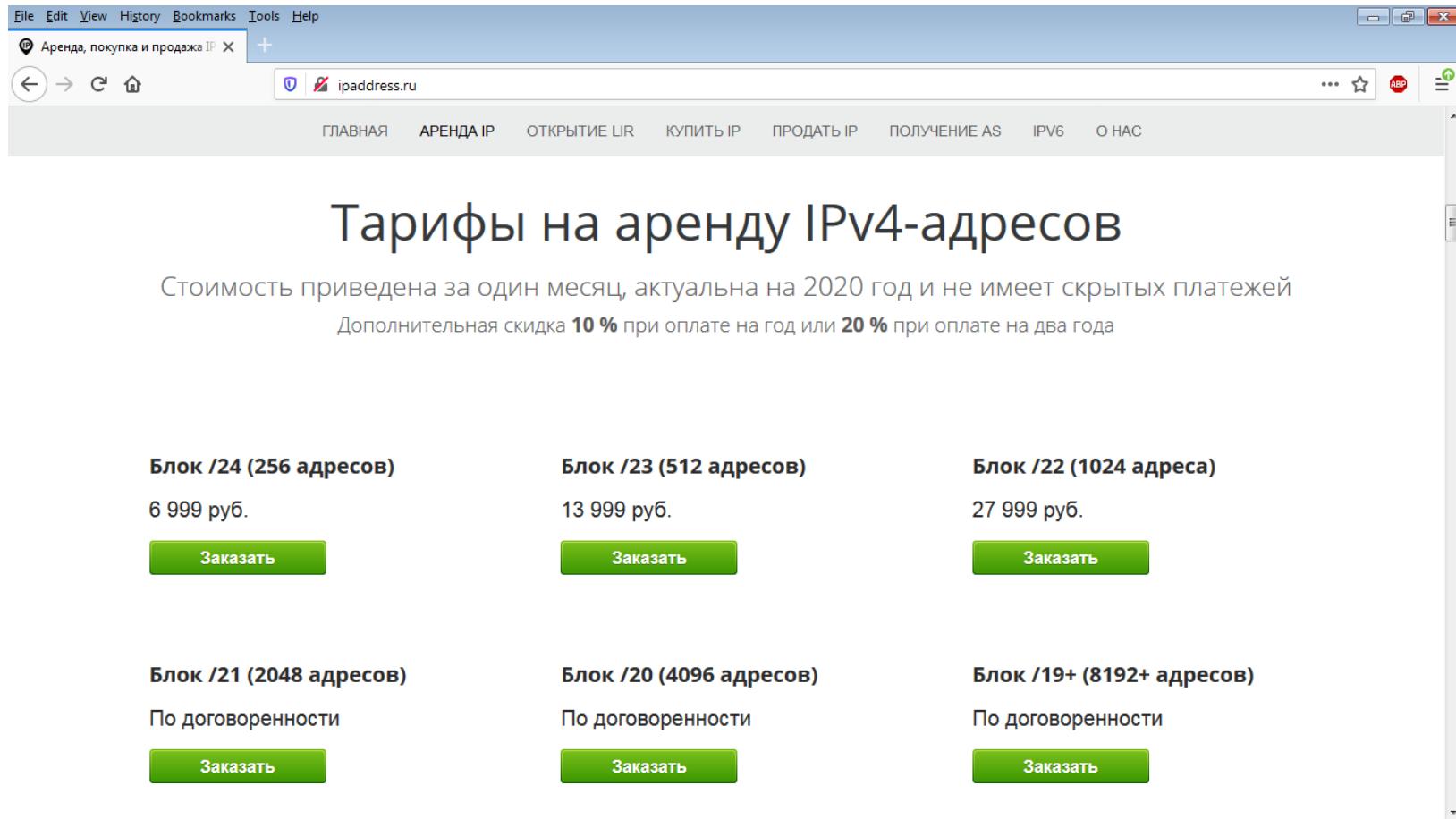
ГЛАВНАЯ АРЕНДА IP ОТКРЫТИЕ LIR КУПИТЬ IP ПРОДАТЬ IP ПОЛУЧЕНИЕ AS IPV6 О НАС

## Тарифы на аренду IPv4-адресов

Стоимость приведена за один месяц, актуальна на 2019 год и не имеет скрытых платежей

<b>Сеть /24 (256 адресов)</b> 4 999 руб. <a href="#">Заказать</a>	<b>Сеть /23 (512 адресов)</b> 9 999 руб. <a href="#">Заказать</a>	<b>Сеть /22 (1024 адреса)</b> 19 999 руб. <a href="#">Заказать</a>
<b>Сеть /21 (2048 адресов)</b> По договоренности <a href="#">Заказать</a>	<b>Сеть /20 (4096 адресов)</b> По договоренности <a href="#">Заказать</a>	<b>Сеть /19+ (8192+ адресов)</b> По договоренности <a href="#">Заказать</a>

# И стоимость их аренды растет



File Edit View History Bookmarks Tools Help

Аренда, покупка и продажа IP X +

ipaddress.ru

ГЛАВНАЯ АРЕНДА IP ОТКРЫТИЕ LIR КУПИТЬ IP ПРОДАТЬ IP ПОЛУЧЕНИЕ AS IPV6 О НАС

## Тарифы на аренду IPv4-адресов

Стоимость приведена за один месяц, актуальна на 2020 год и не имеет скрытых платежей

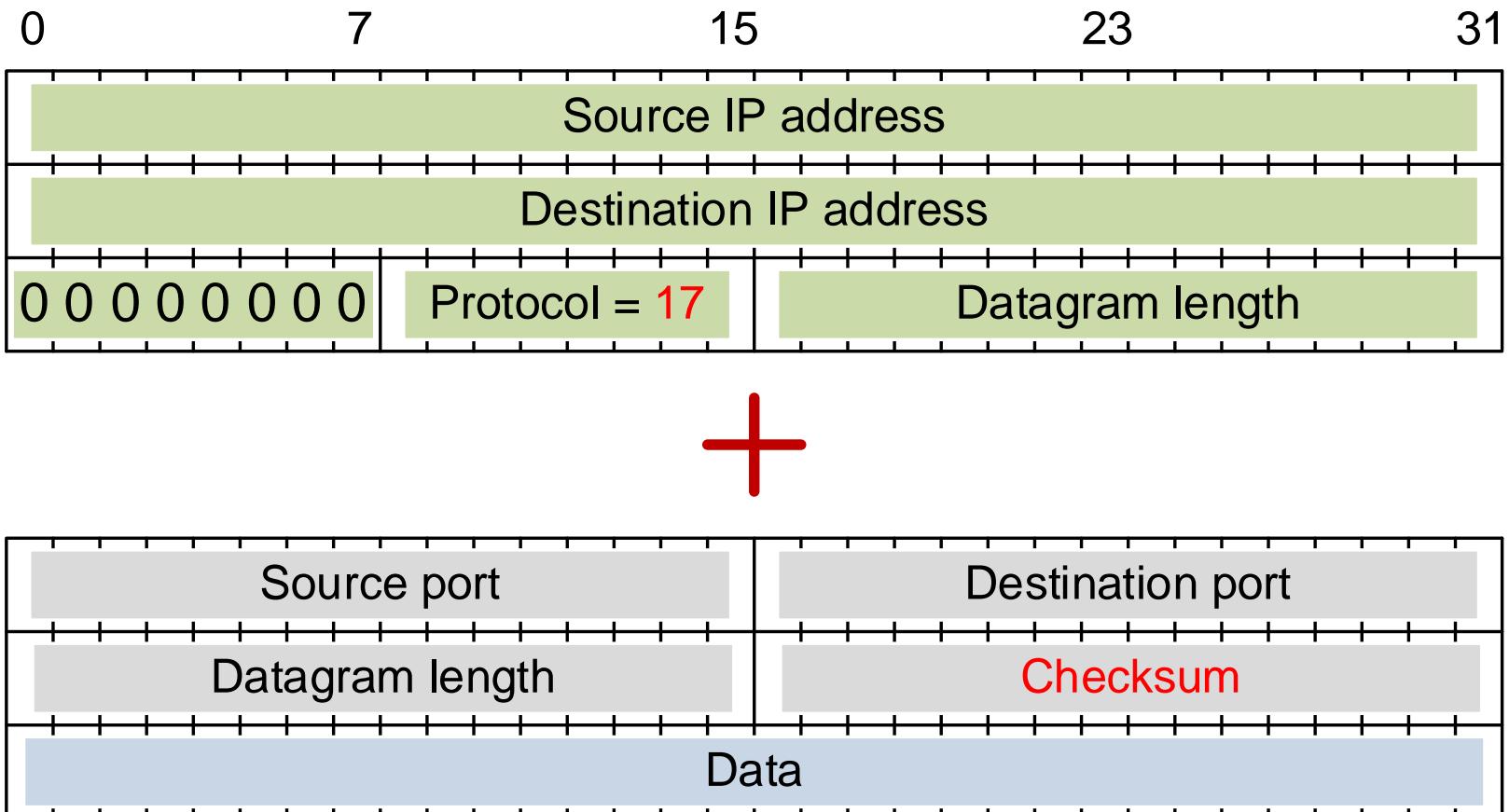
Дополнительная скидка **10 %** при оплате на год или **20 %** при оплате на два года

<b>Блок /24 (256 адресов)</b> 6 999 руб. <a href="#">Заказать</a>	<b>Блок /23 (512 адресов)</b> 13 999 руб. <a href="#">Заказать</a>	<b>Блок /22 (1024 адреса)</b> 27 999 руб. <a href="#">Заказать</a>
<b>Блок /21 (2048 адресов)</b> По договоренности <a href="#">Заказать</a>	<b>Блок /20 (4096 адресов)</b> По договоренности <a href="#">Заказать</a>	<b>Блок /19+ (8192+ адресов)</b> По договоренности <a href="#">Заказать</a>

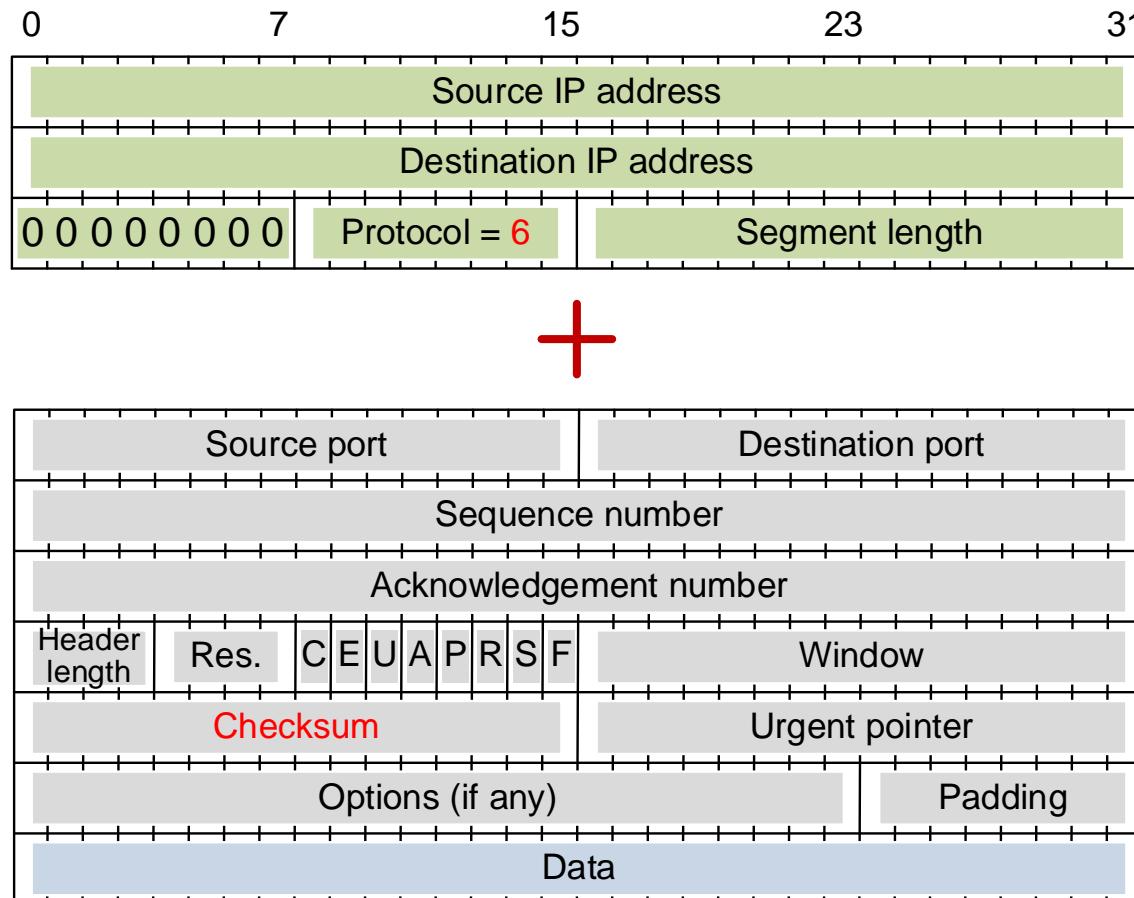
# Частные IP-адреса

- 10.0.0.0 – 10.255.255.255 (маска подсети /8)
- 172.16.0.0 – 172.31.255.255 (маска подсети /12)
- 192.168.0.0 – 192.168.255.255 (маска подсети /16)

# Контрольная сумма UDP



# Контрольная сумма TCP



# Пример TCP-соединения с NAT

Клиент	NAT	Сервер
10.0.0.10 (49506)	188.162.65.123 (61198)	94.19.116.58 (80)

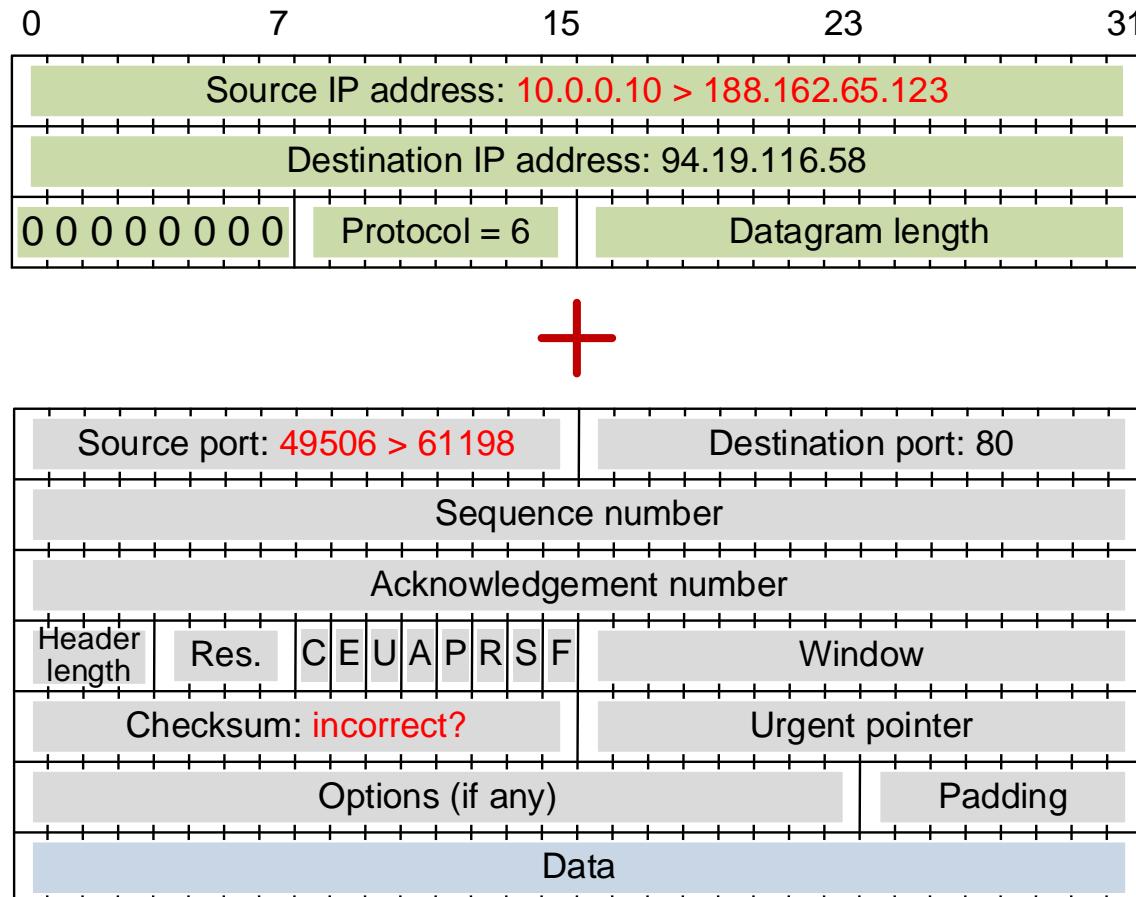
**Что видит клиент:**

10.0.0.10 (49506)	>	94.19.116.58 (80)
----------------------	---	----------------------

**Что видит сервер:**

188.162.65.123 (61198)	>	94.19.116.58 (80)
---------------------------	---	----------------------

# Как быть с контрольной суммой?



# Пересчитывать или отказаться?

- При использовании NAT происходит замена локально маршрутизируемого IP-адреса (т.н. частный/внутренний/серый) на глобально маршрутизируемый (т.н. публичный/внешний/белый)
- Для возможности обратного преобразования часто также меняется и номер порта клиента (**Port Address Translation, PAT**)
- Поскольку исходная контрольная сумма рассчитывалась для прежних значений, подобная замена делает ее неверной и такой TCP-сегмент или UDP-дейтаграмма получателем будет отброшены как ошибочные
- Следовательно, необходимо либо пересчитывать контрольную сумму TCP и UDP всякий раз, когда пакет проходит через NAT туда или обратно, либо отказаться от использования контрольных сумм в TCP и UDP, как это сделано в IPv6 (ее там просто нет)