# Анализ влияния NAT на контрольные суммы TCP и UDP

Дунайцев Р.А. (СПбГУТ)

roman.dunaytsev@spbgut.ru

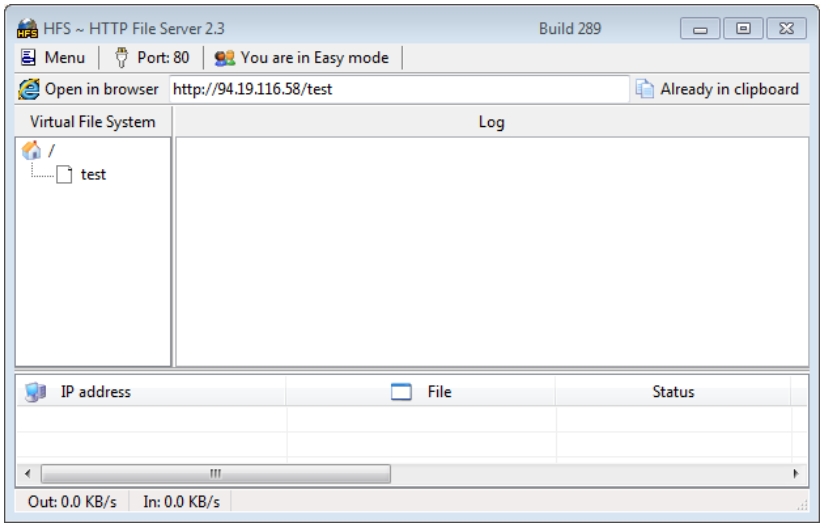
# Краткая теоретическая справка

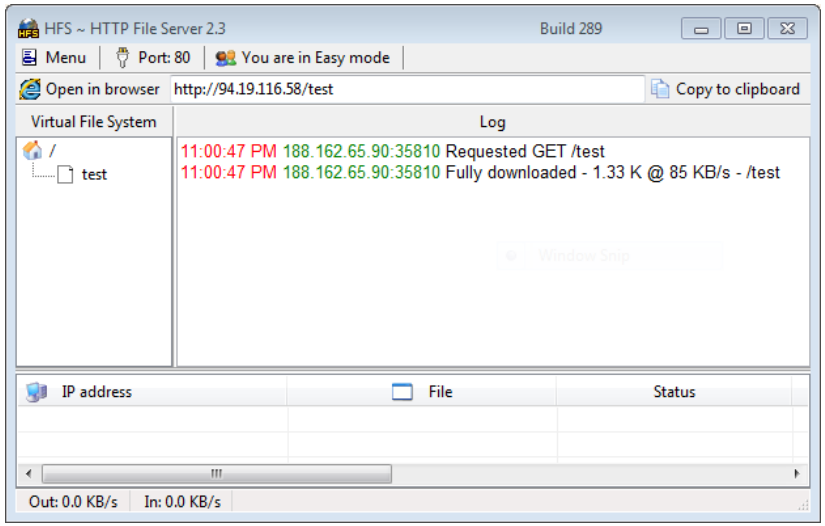
- IP-адрес считается глобально маршрутизируемым, если любой правильно настроенный маршрутизатор в сети Интернет может построить маршрут пакета так, что тот в конечном счете достигнет узла с этим IP-адресом. Для этого любой глобально маршрутизируемый адрес должен быть присвоен только одному узлу. Чтобы обеспечить уникальность глобально маршрутизируемых 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 маршрутизируемый IP-адрес. Обеспечивать уникальность таких адресов не требуется, потому что адреса не являются глобально маршрутизируемыми. В настоящее время NAT используется повсеместно, особенно в домашних сетях и сетях небольших организаций.

# Задание на дом

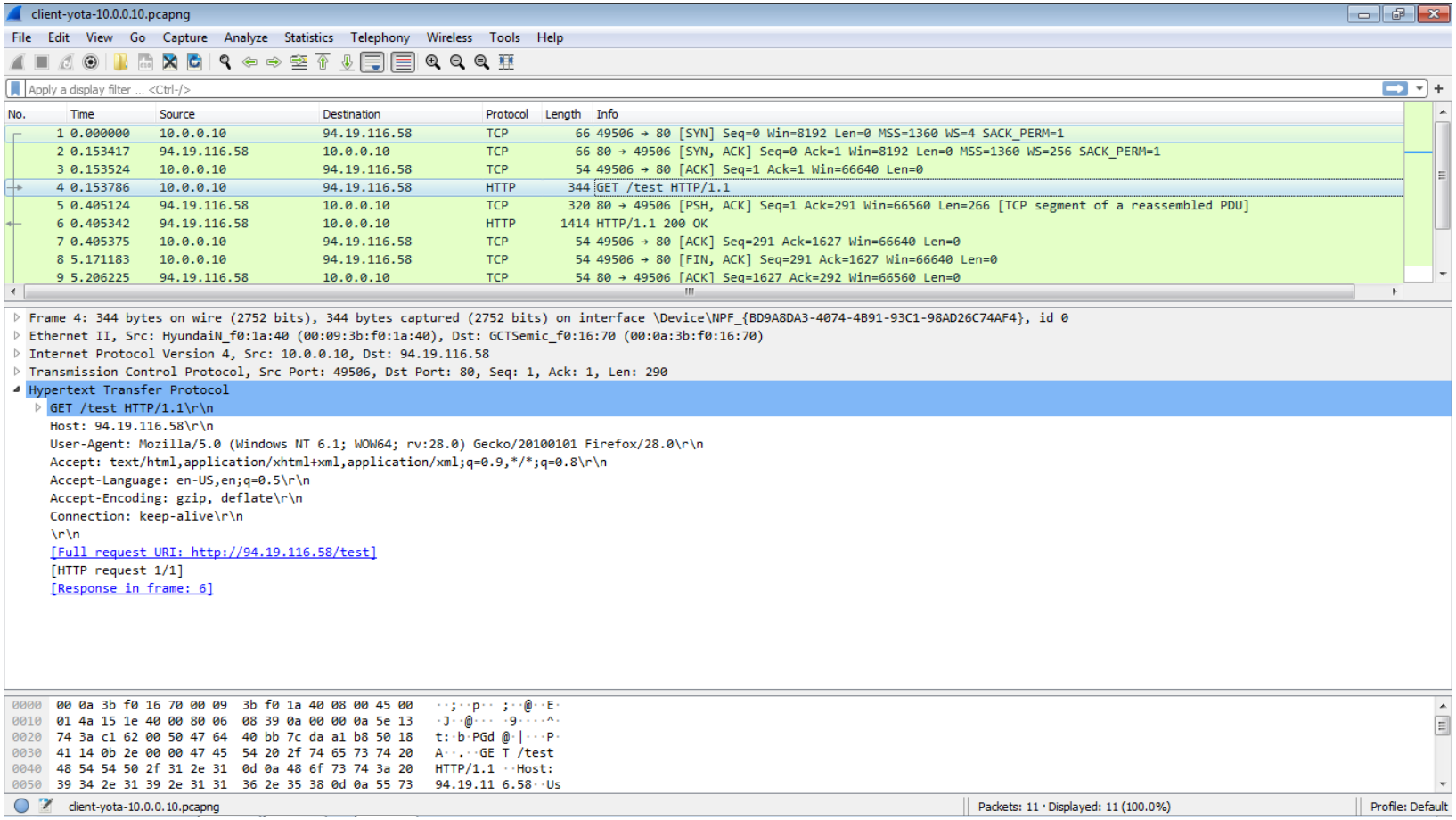
- Экспериментальным путем выяснить, пересчитываются ли контрольные суммы TCP при использовании NAT
  1) Найти 2 ПК, один с публичным IP-адресом (например, выдается некоторыми Интернет-провайдерами), а другой с частным IP-адресом
  2) Установить между ними TCP-соединение. В качестве сервера можно использовать 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

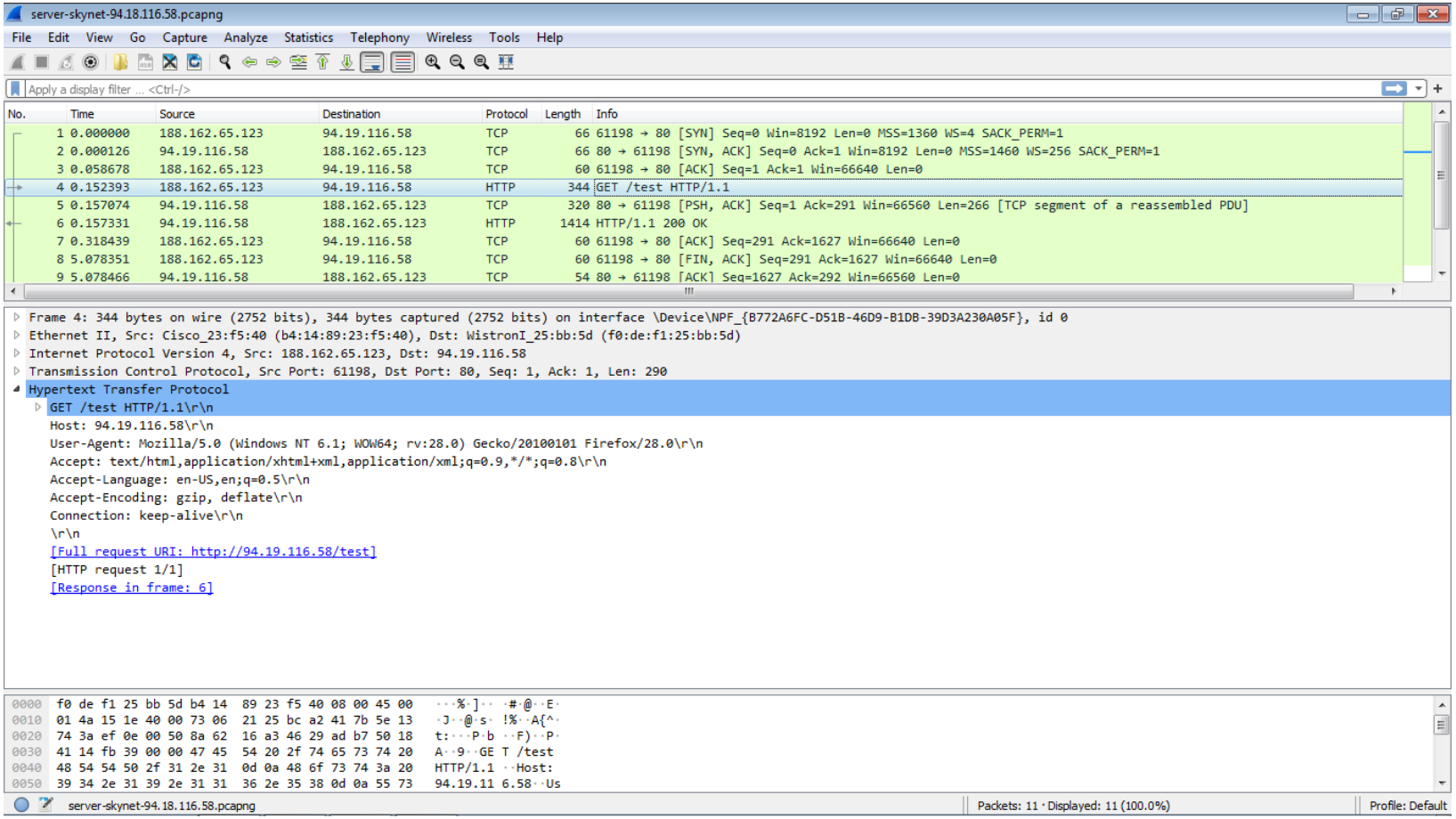


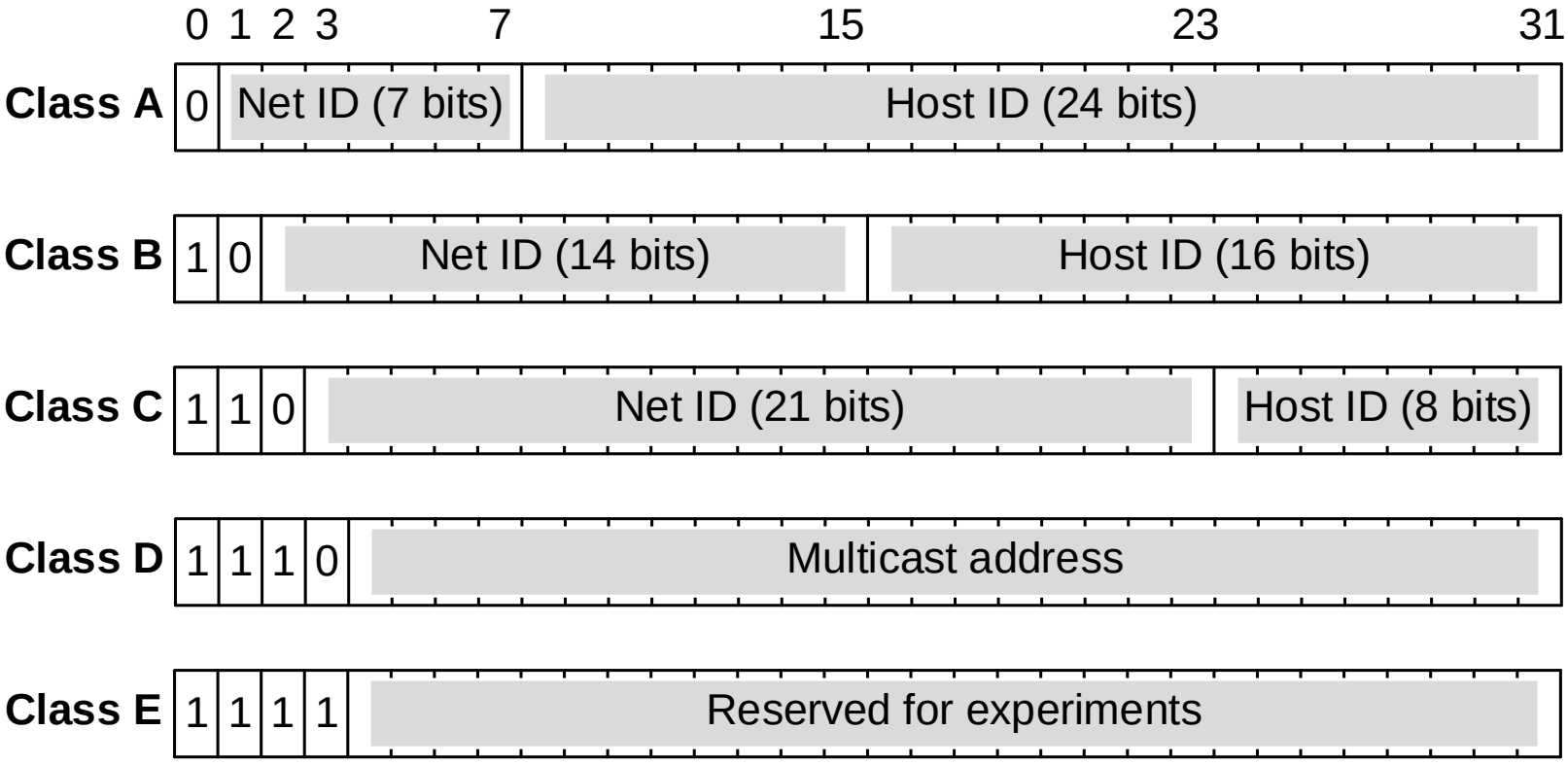
# Запрос GET на стороне клиента



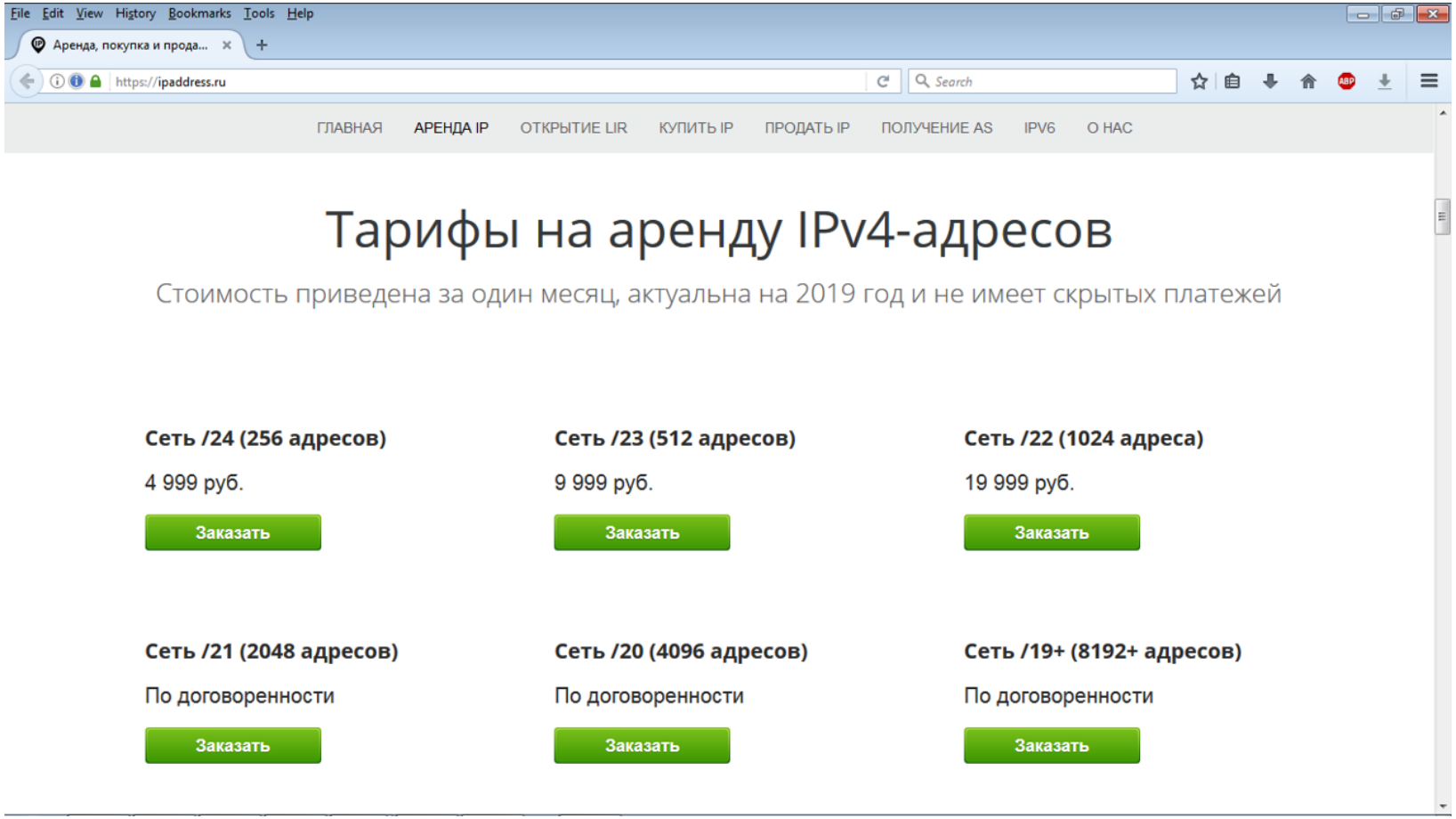
# Запрос GET на стороне сервера



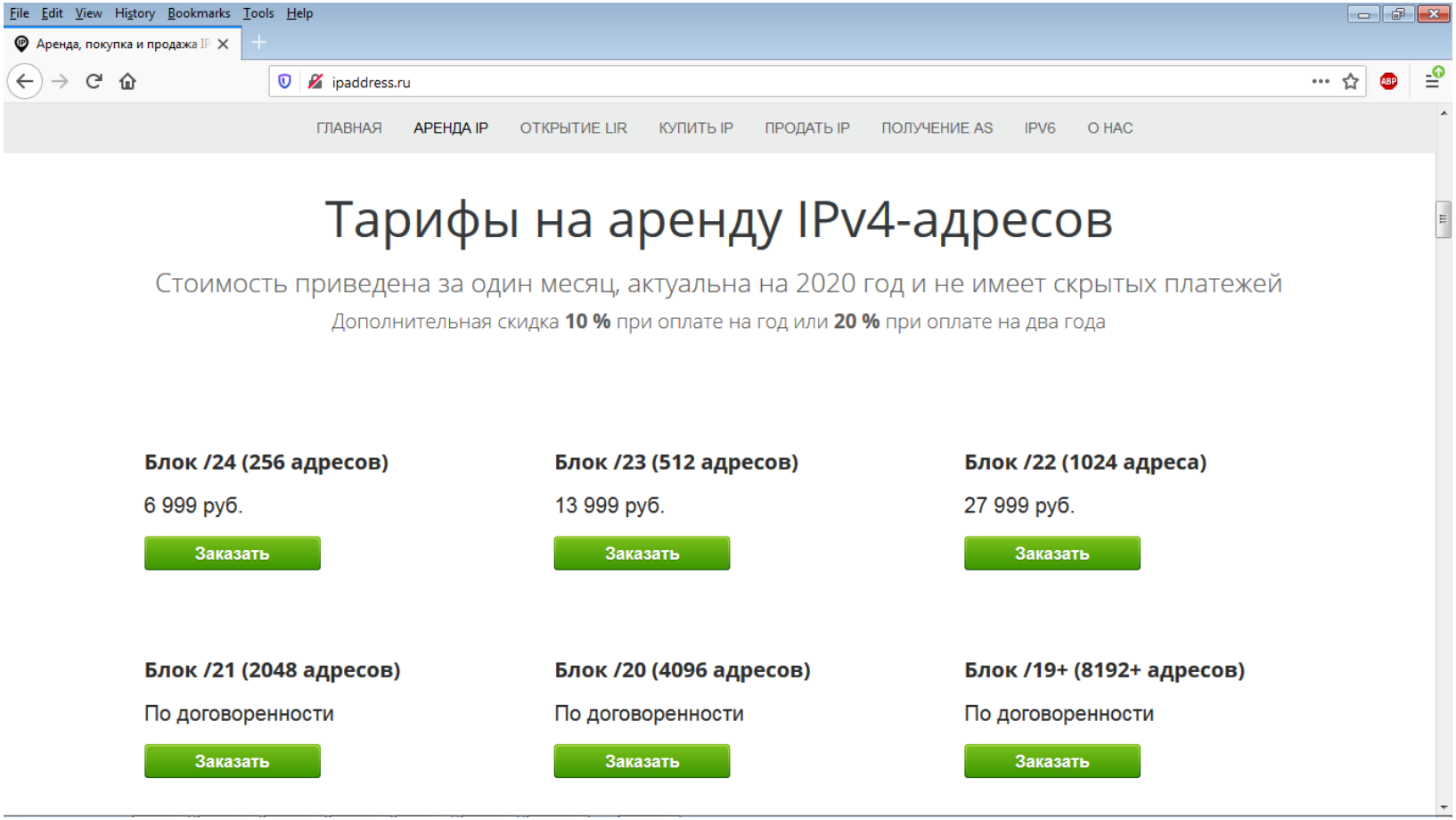
# Классовая адресация



# Публичные IP-адреса стоят денег



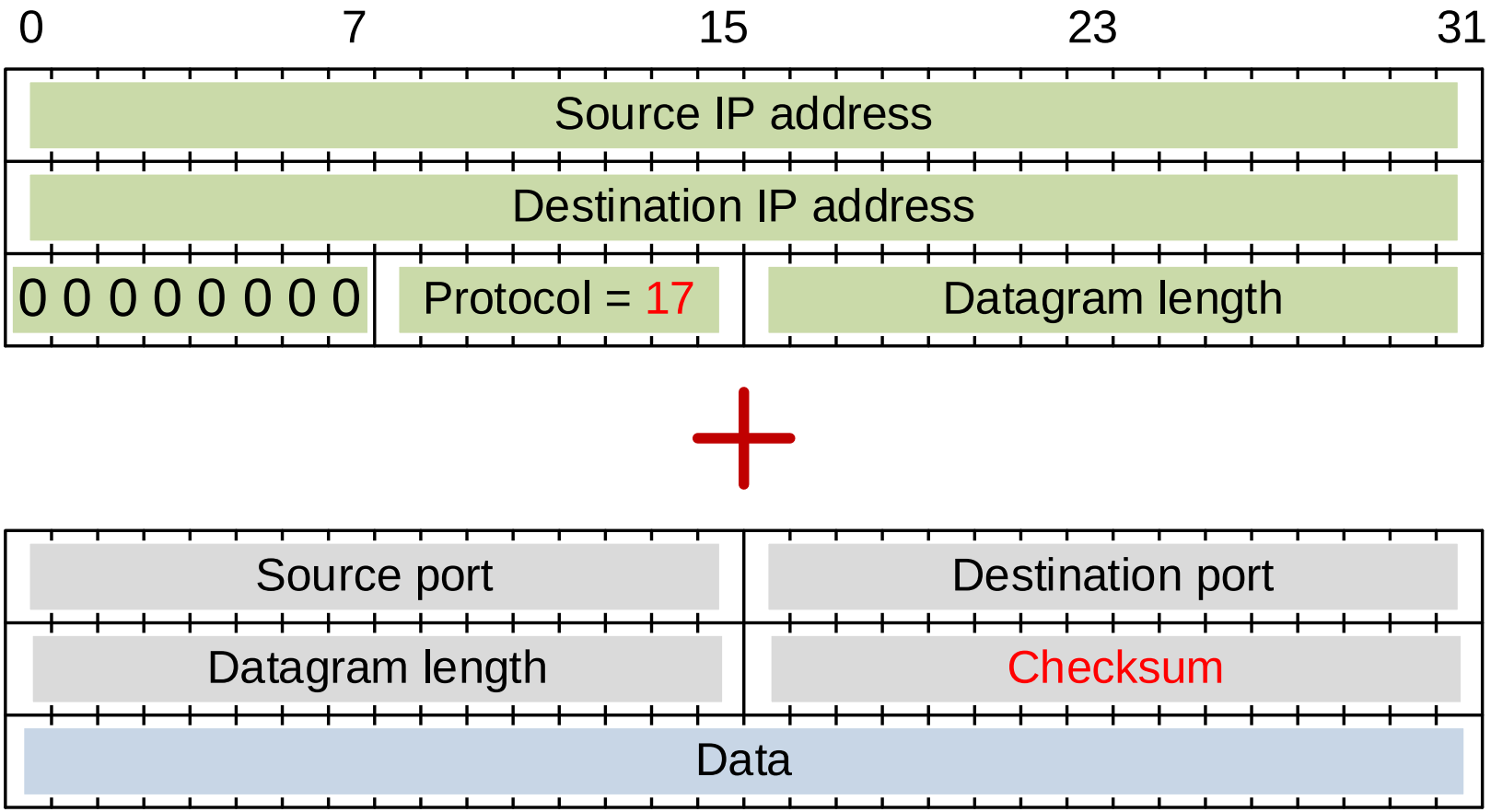
# И стоимость их аренды растет



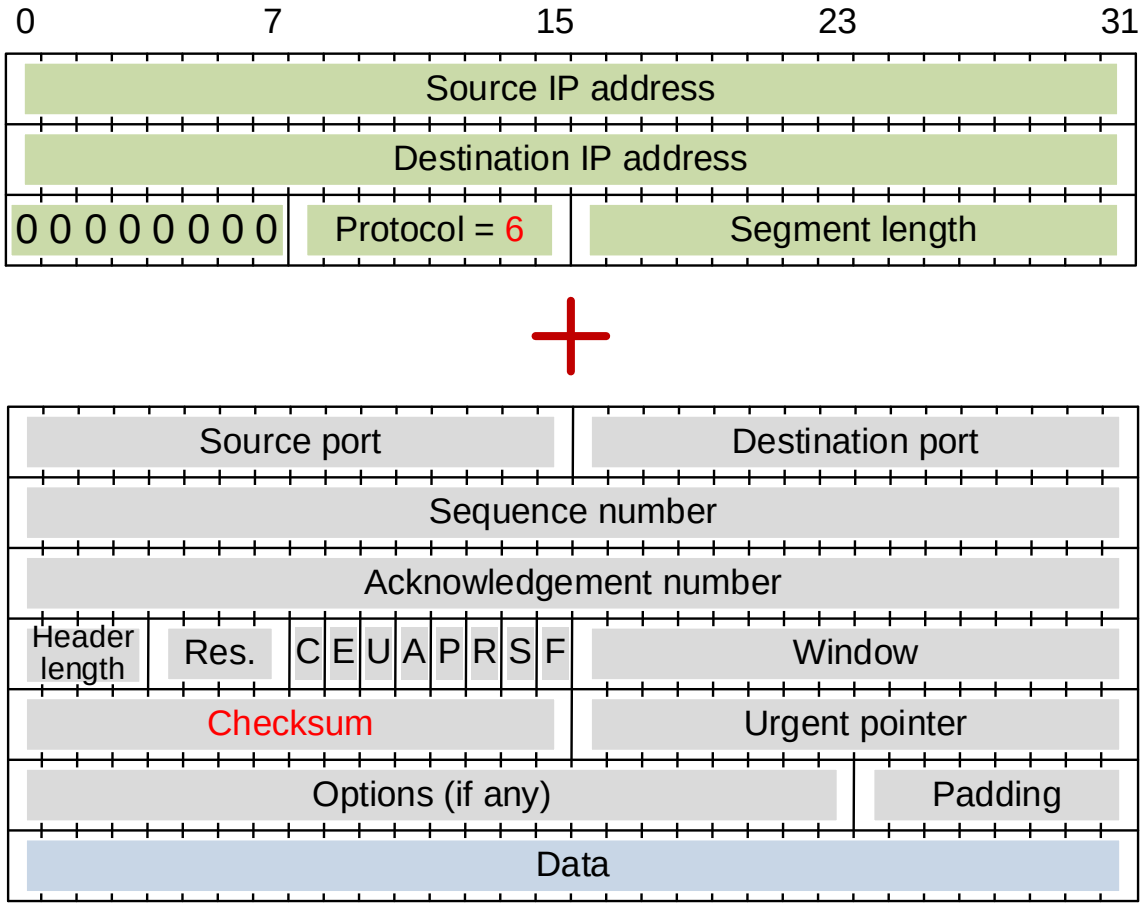
# Частные IP-адреса

- 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) |

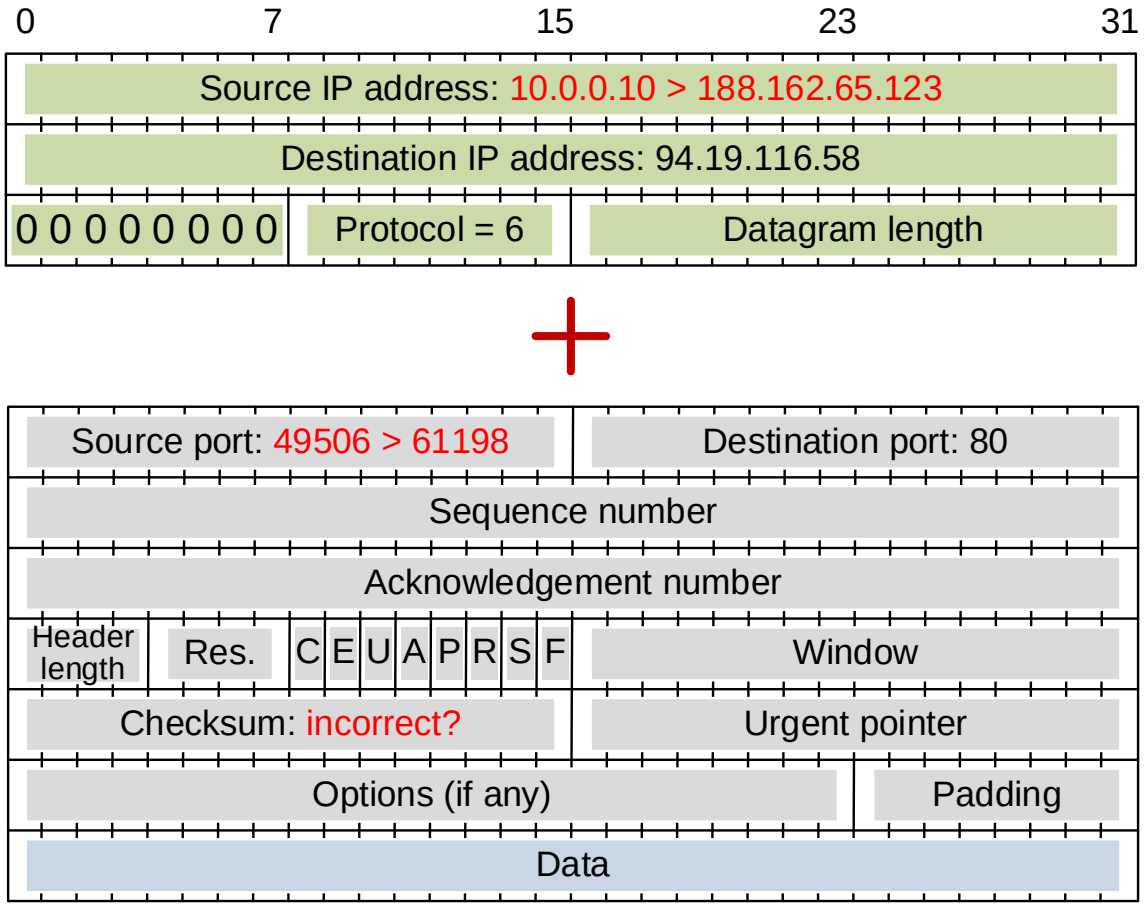
**Что видит клиент:**

| | | |
|---|---|---|
| 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)