Архипов Игорь Юрьевич
студент, 2 курс, факультет "Комплексная безопасность ТЭК"
Российский государственный университет нефти и газа (НИУ)
имени И. М. Губкина
Россия, г. Москва
Муляков Алексей Александрович
студент, 2 курс, факультет "Комплексная безопасность ТЭК"
Российский государственный университет нефти и газа (НИУ)
имени И. М. Губкина
Россия, г. Москва

ГЕНЕРАТОРЫ СЕТЕВОГО ТРАФИКА WAN / LAN ДЛЯ ТЕСТИРОВАНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ И СТРЕСС-ТЕСТИРОВАНИЯ СЕТИ. РАЗВЕРТЫВАНИЕ И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ

Аннотация: В данной статье рассмотрены принципы работы, развертывание и функциональные возможности генераторов сетевого трафика WAN/LAN, подчеркивая их критическую важность для объективной оценки производительности и устойчивости современных корпоративных сетей. Генераторы трафика – это специализированные аппаратные или программные решения, предназначенные для имитации реалистичного или экстремального сетевого потока данных с целью тестирования пропускной способности. Актуальность исследования обусловлена необходимостью выявления узких мест, проверки конфигураций оборудования и обеспечения соответствия сетей растущим требованиям к производительности и надежности. Современные генераторы трафика поддерживают моделирование разнообразных протоколов, что позволяет проводить комплексное тестирование как на физическом, так и на виртуальном уровне. Знание методик развертывания, настройки параметров генерации (интенсивность, размер пакетов, шаблоны) и анализа результатов тестирования позволяет сетевым инженерам и

администраторам гарантировать стабильность, производительность и отказоустойчивость инфраструктуры до ее ввода в промышленную эксплуатацию.

Ключевые слова: генераторы сетевого трафика, тестирование пропускной способности, стресс-тестирование, производительность сети, функциональное тестирование.

Abstract*:* This article discusses the principles of operation, deployment, and functionality of WAN/LAN network traffic generators, emphasizing their critical importance for an objective assessment of the performance and sustainability of modern corporate networks. Traffic generators are specialized hardware or software solutions designed to simulate realistic or extreme network data flow in order to test throughput. The relevance of the study is due to the need to identify bottlenecks, verify equipment configurations, and ensure that networks meet growing performance and reliability requirements. Modern traffic generators support modeling of various protocols, which allows for comprehensive testing at both the physical and virtual levels. Knowledge of deployment techniques, generation settings (intensity, packet size, templates), and analysis of test results allows network engineers and administrators to ensure the stability, performance, and fault tolerance of the infrastructure before it is put into commercial operation.

Keywords: network traffic generators, bandwidth testing, stress testing, network performance, functional testing.

Введение

В условиях постоянного роста объема передаваемых данных и ужесточения требований к качеству обслуживания (QoS) и отказоустойчивости корпоративных и операторских сетей, задача объективной оценки их реальной пропускной способности и устойчивости к нагрузке выходит на первый план. Планирование модернизации, проверка конфигурации, верификация сервисных соглашений (SLA) и подготовка к пиковым нагрузкам требуют использования специализированных

инструментов, способных детерминировано генерировать, контролировать и анализировать сетевой трафик. Ключевым инструментом для решения этих задач являются генераторы сетевого трафика – аппаратные или программные решения, предназначенные для эмуляции разнородного трафика, характерного для современных сетей передачи данных. В отличие от простых утилит проверки связности, такие генераторы позволяют создавать сложные, настраиваемые потоки данных с заданными параметрами (интенсивность, размер пакетов, типы протоколов, шаблоны нагрузки), что необходимо для проведения стресс-тестирования и определения «узких мест» инфраструктуры. Особую актуальность приобретает разделение тестовых сценариев для сегментов WAN (глобальная сеть) и LAN (локальная сеть). В сегменте LAN критически важна проверка максимальной производительности коммутационного оборудования, эффективности механизмов качества обслуживания (QoS), сегментации (VLAN) и фильтрации (ACL) под высокой нагрузкой. Для WAN-сегментов, часто имеющих ограниченную пропускную способность и подверженных задержкам и джиттеру, фокус смещается на тестирование туннельных решений (IPsec, DMVPN, SD-WAN), механизмов сжатия и оптимизации трафика, а также на проверку стабильности каналов связи в условиях длительной и неравномерной нагрузки.

Стресс-тестирование – это процесс проверки устойчивости системы или приложения при экстремальных или предельных условиях работы, чтобы оценить его способность справляться с нагрузками, превышающими обычные. Цель стресс-тестирования – выявить точки отказа системы, определить её пределы и убедиться, что она продолжает функционировать или корректно восстанавливается после перегрузки.[6]

Функциональное тестирование – процесс проверки, как работает программное обеспечение или система в соответствии с заданными требованиями. Главная цель – убедиться, что все функции программы выполняются так, как ожидалось.[7]

Объект исследования: генераторы сетевого трафика.

Предмет исследования: методы и инструменты генерации сетевого трафика (LAN/WAN) для тестирования производительности, пропускной способности и устойчивости сетевой инфраструктуры.

Цель исследования: установить генераторы сетевого трафика и провести различные тестирования.

Литературный обзор

Мы рассмотрели данную статью “WAN/LAN Network Traffic Generators for Bandwidth & Stress Testing” про генератор сетевого трафика Nping. Nping – инструмент с открытым исходным кодом для анализа ответов, управления временем отклика и генерации сетевых пакетов.

В данной статье рассмотрены основной функционал генератора сетевого трафика Nping. Но отсутствует упоминание о следующих важных аспектах:

1. Поддержка множества протоколов. Он может генерировать пакеты не только для ICMP (ping), но и для TCP, UDP, ARP, SCTP, позволяя тестировать ответы конкретных сервисов (например, отправляя TCP-пакет с флагом SYN).

2. Продвинутая настройка пакетов. Можно вручную задавать флаги TCP (SYN, ACK, RST, FIN и др.). Поля IP (TTL, идентификатор, фрагментацию). Случайные или полезные данные (payload). Скорость отправки и таймауты.[1]

В статье “Qperf - man pages section 1: User commands” мы рассмотрели генератор сетевого трафика Qperf, в ней приведено корректное, но не полное описание данного генератора сетевого трафика, не рассмотрены следующие важные моменты.

1. Богатый набор тестов (метрик) и параметров. Тесты: помимо tcp_bw (пропускная способность) и tcp_lat (задержка), есть множество других, например, udp_bw, udp_lat. Глубокие метрики: измеряет не только средние значения, но и время установки соединения, размеры окон (window size), загрузку CPU, что помогает находить узкие места.

2. Гибкость настройки тестов. Можно детально управлять параметрами: размером сообщений (--msg_size), длительностью теста (--t) и другими. [8]

В статье “Утилита iPerf: тестирование пропускной способности и скорости сети” описывается генератор сетевого трафика Iperf3, но в ней не указаны ключевые технические особенности, которые делают Iperf3 стандартом индустрии стресс-тестирования сетей.

1. Детальная аналитика и метрики. Iperf3 предоставляет не просто общую пропускную способность, но и интервальные отчеты с выводом статистики (bandwidth, jitter, loss) каждые N секунд, что позволяет видеть динамику и стабилизацию потока; расширенные TCP-метрики с отчетами о потерях пакетов (retransmits), размере окна (window size).

2. Продвинутые возможности и флаги. Обратный тест (-R): Клиент запрашивает у сервера отправку трафика к себе, что обходит проблемы с асимметричной маршрутизацией или настройками брандмауэра. Контроль битрейта UDP (-b) позволяет точно задать нагрузку (например, -b 100M для 100 Мбит/с) и измерить потери и джиттер. [2]

Таблица 1 – Сравнительная характеристика генераторов сетевого трафика

	Nping	Qperf	Iperf3
Требования к ВМ	ЦП - достаточно 1 ядра; ОЗУ - минимум 512 Мб	ЦП - достаточно 1 ядра; ОЗУ - минимум 1 Гб	ЦП - не менее 2 ядер при скорости в 10 Гбит/с, - не менее 4 ядер при скорости в 25 Гбит/с; ОЗУ - минимум 1 Гб
Уровни модели OSI, на которых работает	L3-4	L4	L4
Максимальная скорость генерируемого трафика	2 Гбит/с	20 Гбит/с	25 Гбит/с

Актуальная версия у производителя	7.98	0.4.11	3.19.1-alt1
Установленная пакетная версия	7.95	0.4.11	3.19.1-alt1

Гипотезы исследования

- Определить наиболее подходящий генератор сетевого трафика для стресс-тестирования сети.

Методы исследования

Тип исследования: экспериментальный, с элементами сравнительного анализа.

Характеристика выборки: тестовая сеть из коммутатора. А также включает узлы с установленными генераторами трафика (iPerf3, NPing, qperf), выступающие в роли клиентов и серверов.

Методы сбора и обработки данных: генерация тестовой нагрузки и анализ трафика в Wireshark.

Процедура эксперимента:

- Установка программного генератора Iperf3.
- Установка программного генератора Nping.
- Установка программного генератора Qperf.
- Проведение тестов.

Проведение эксперимента

После того, как мы ознакомились с принципами работы и установили программные генераторы сетевого трафика, перейдем к их функциональному

тестированию. Для этого развернем тестовый стенд, состоящий из коммутатора Cisco2960 и двух виртуальных машин, выполняющих роль клиента и сервера.

При выполнении эксперимента с использовался коммутатор Cisco2960. Топология сети указана на рисунке 1.

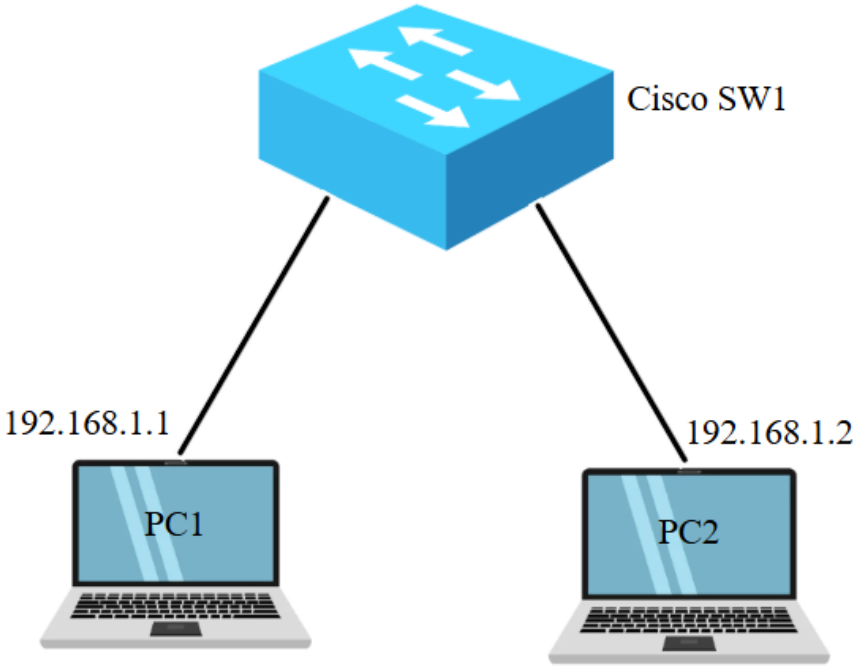

Рисунок 1 – Топология сети

Сначала установили генератор сетевого трафика qrepf. Далее на сервере, а именно на принимающей стороне ввели qperf, а на тестирующей стороне ввели qperf <ip_сервера> <тесты>.

Для начала провели базовый тест TCP на задержку и измерение пропускной способности. На клиенте ввели команду qperf 192.168.1.1 tcp_lat и qperf 192.168.1.1 tcp_bw. Клиент и сервер обмениваются короткими TCP-пакетами, чтобы измерить время круговой задержки (RTT) между ними. Результат представлен на рисунке 2 и 3.

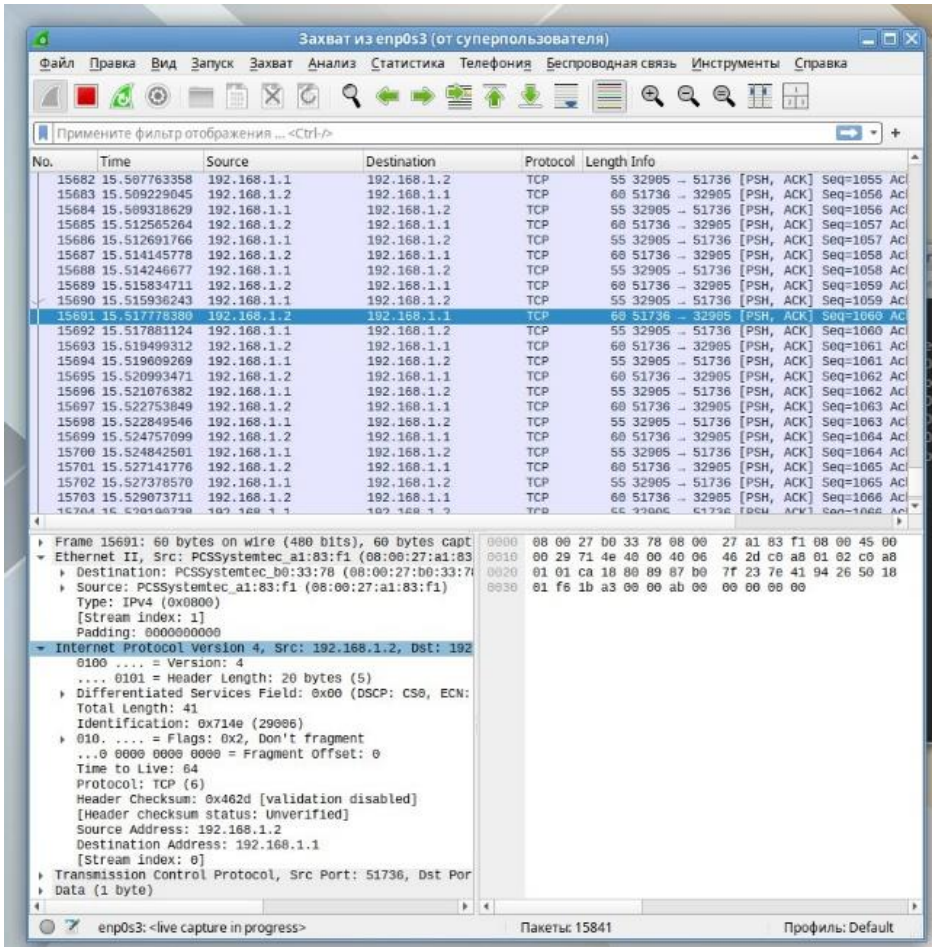

Рисунок 2 – Базовое тестирование qperf

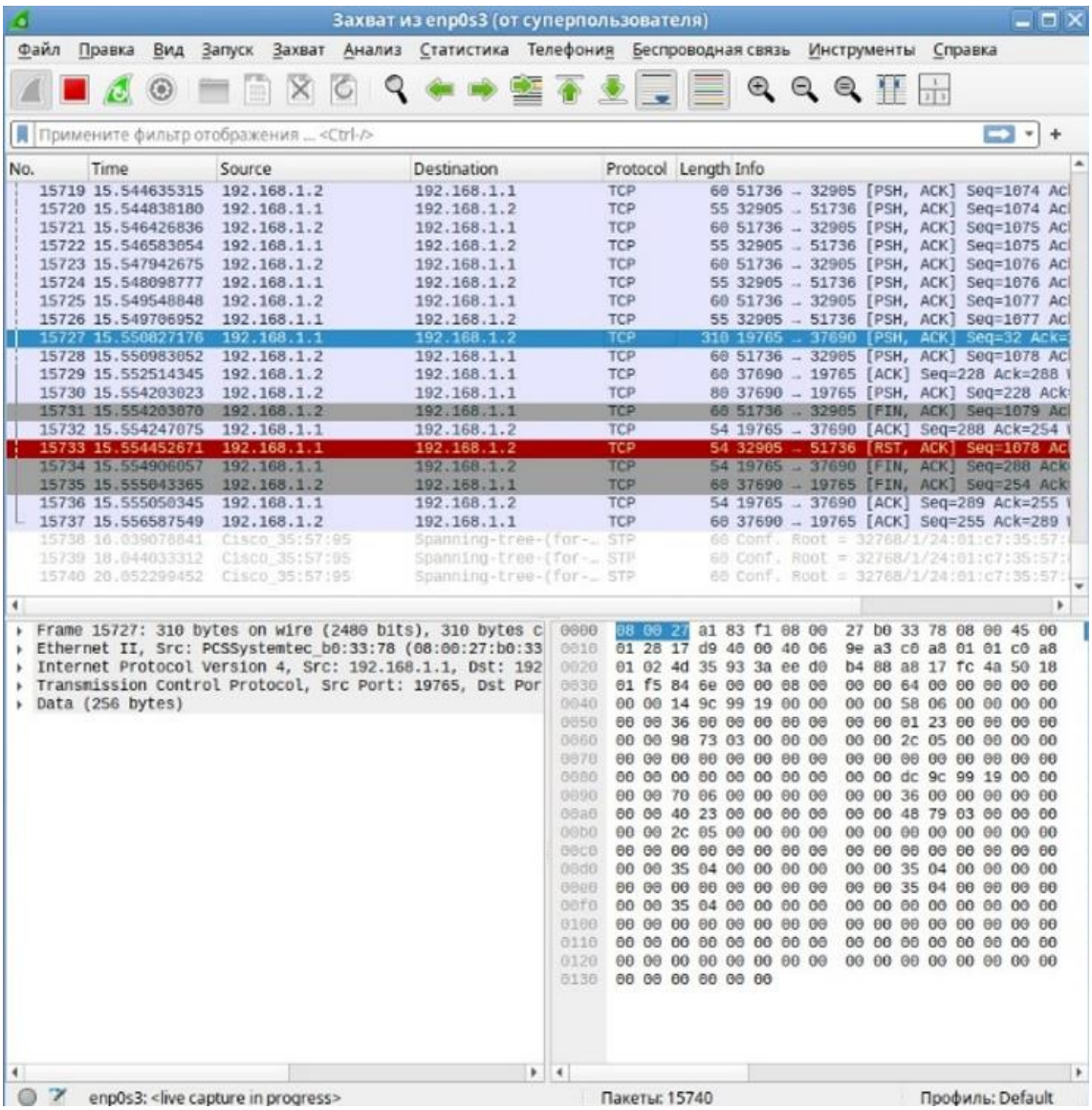

Рисунок 3 – Тестирование для измерения пропускной способности

На рисунке 4 зафиксирован момент пиковой нагрузки. По каналу 41023 - 51842 идут гигантские пакеты по 4 КБ данных каждый, в обоих направлениях, с минимальными паузами. Это и есть стресс-тест канала на максимальную скорость (tcp_bw).

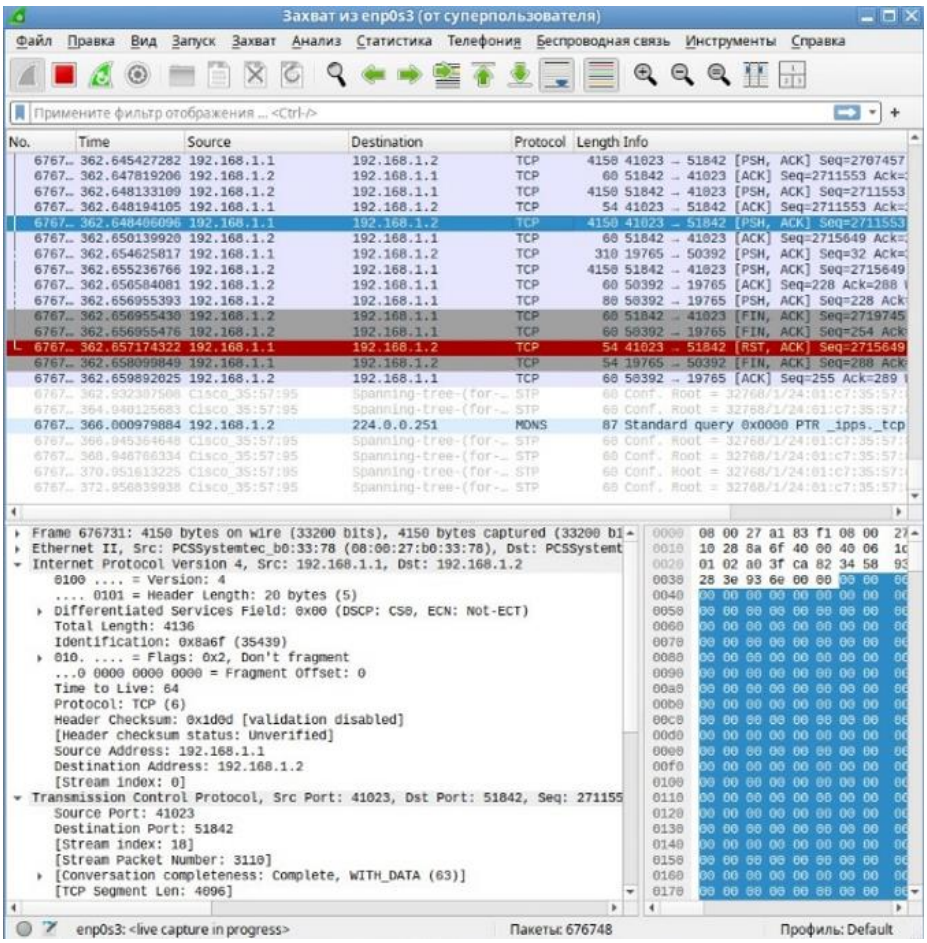

Рисунок 4 – Момент пиковой нагрузки с использованием qperf

Далее провели агрессивное нагрузочное стресс-тестирование UDP-канала на максимальную пропускную способность с использованием экстремально больших датаграмм, чтобы определить максимальную пропускную способность канала. Ввели команду qperf 192.168.1.1 udp_lat. Результат представлен на рисунке 5.

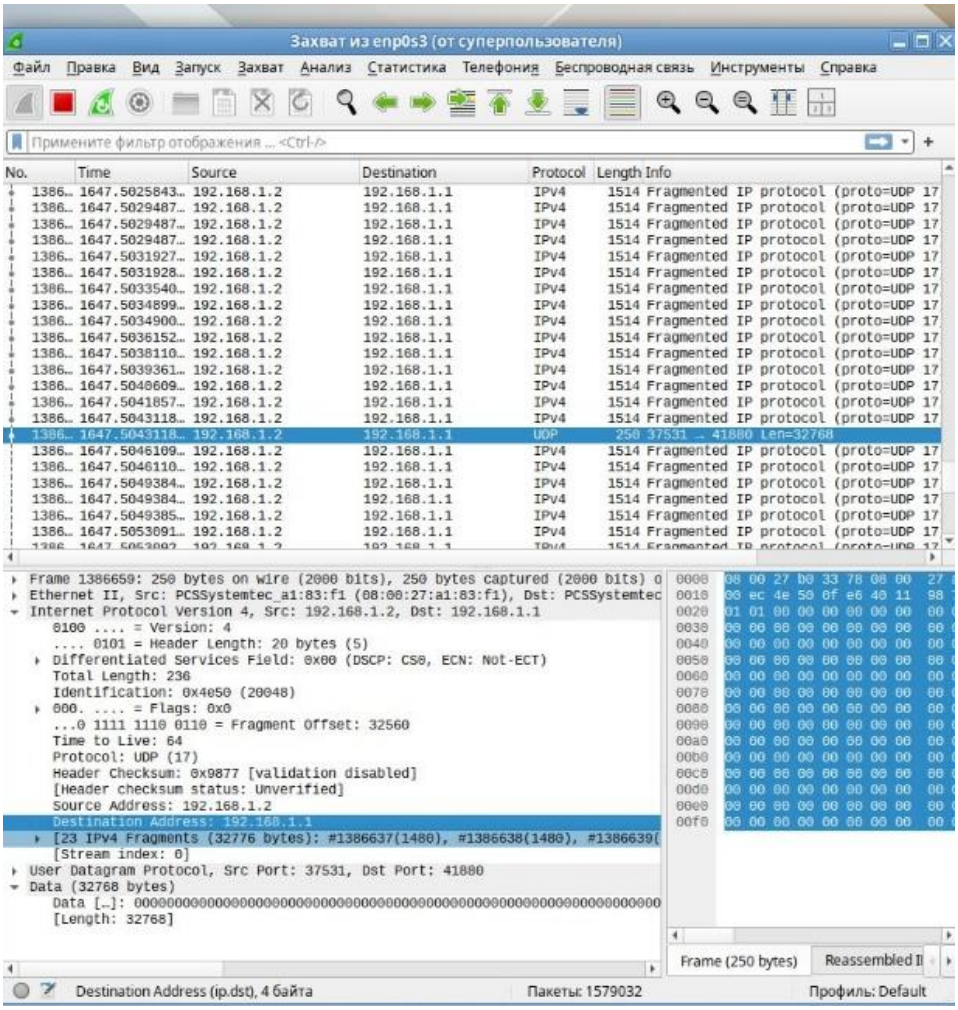

Рисунок 5 – Тестирование UDP-канала на пропускную способность

Далее командой qperf 192.168.1.100 -t 30 tcp_bw tcp_lat провели тест продолжительностью 30 секунд. На рисунке 6 представлен захват трафика во время проведения теста. В отличие от нагрузочных тестов, здесь наблюдается интенсивный обмен крайне малыми TCP-пакетами (55-69 байт).

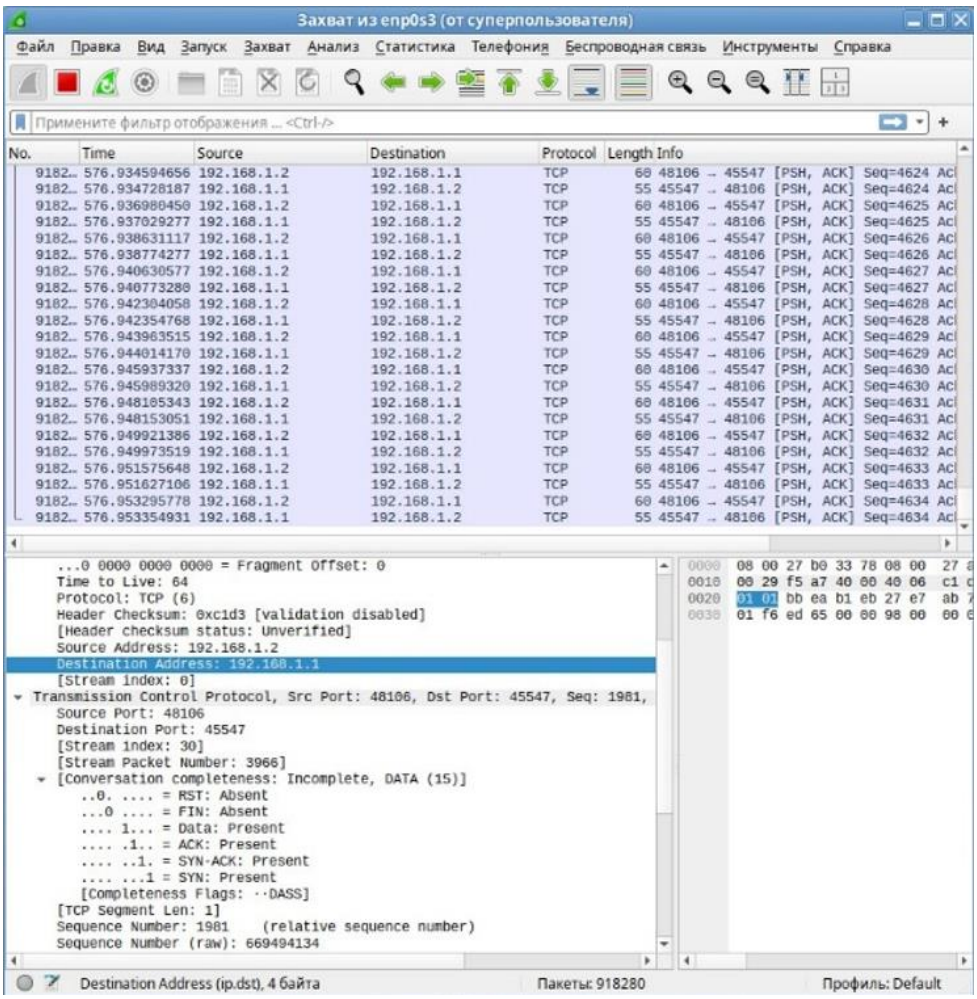

Рисунок 6 – Захват трафика во время проведения длительного теста

Далее установили другой генератор сетевого трафика iperf3.

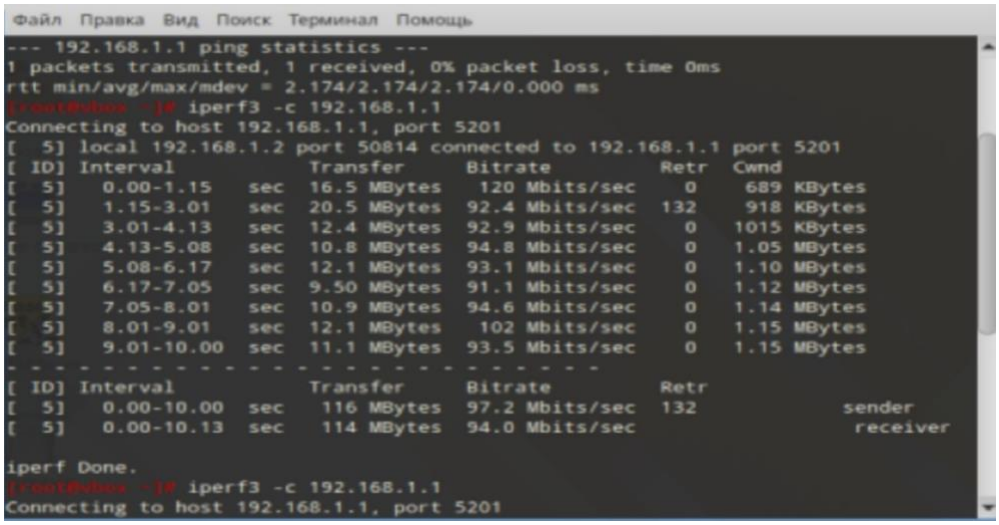

Рисунок 7 – Установленный iperf3

Iperf3. Для начала провели базовый тест на 10 секунд.

```
[root@vbox ~]# iperf3 -c 192.168.1.1
Connecting to host 192.168.1.1, port 5201
[  5] local 192.168.1.2 port 49002 connected to 192.168.1.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  14.0 MBytes   117 Mbits/sec    0    583 KBytes
[  5]   1.00-2.22   sec  13.4 MBytes  92.2 Mbits/sec  201    867 KBytes
[  5]   2.22-3.07   sec  9.88 MBytes  97.7 Mbits/sec    0    948 KBytes
[  5]   3.07-4.12   sec  10.8 MBytes  85.9 Mbits/sec    0   1.02 MBytes
[  5]   4.12-5.02   sec  11.0 MBytes   102 Mbits/sec  117    783 KBytes
[  5]   5.02-6.02   sec  10.9 MBytes  91.8 Mbits/sec    0    831 KBytes
[  5]   6.02-7.58   sec  17.6 MBytes  94.8 Mbits/sec    9    612 KBytes
[  5]   7.58-8.04   sec  5.50 MBytes   100 Mbits/sec    0    634 KBytes
[  5]   8.04-9.04   sec  11.2 MBytes  94.1 Mbits/sec    0    683 KBytes
[  5]   9.04-10.09  sec  11.0 MBytes  88.2 Mbits/sec    1    520 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.09  sec   115 MBytes  95.9 Mbits/sec  328             sender
[  5]   0.00-10.12  sec   113 MBytes  93.5 Mbits/sec                  receiver

iperf Done.
[root@vbox ~]#
```

Рисунок 8 – Клиент, базовый тест

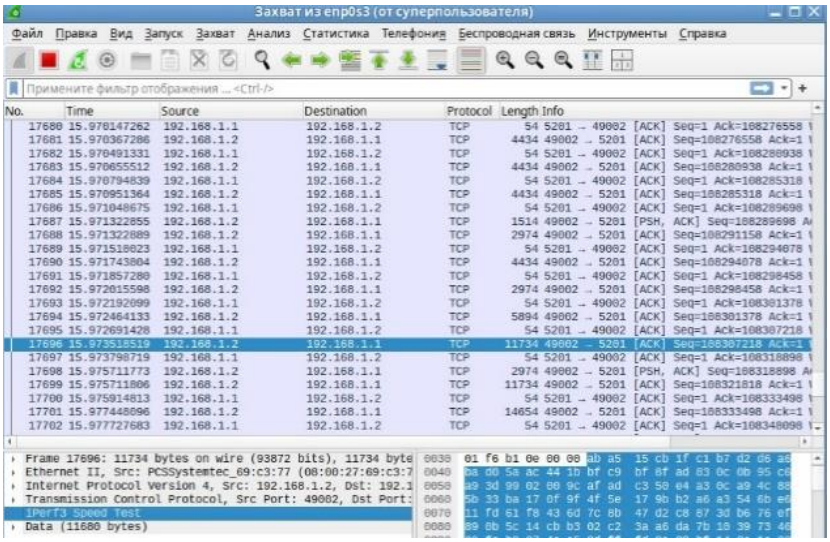

Рисунок 9 – Сервер, базовый тест (wireshark)

Далее же более длительный тест сети, на 30 секунд.

```
[root@vbox ~]# iperf3 -c 192.168.1.1 -t 30
Connecting to host 192.168.1.1, port 5201
[  5] local 192.168.1.2 port 36840 connected to 192.168.1.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.06   sec  14.6 MBytes   116 Mbits/sec    0    632 KBytes
[  5]   1.06-2.24   sec  13.4 MBytes  94.5 Mbits/sec    0   1.29 MBytes
[  5]   2.24-3.26   sec  11.1 MBytes  92.0 Mbits/sec    0   1.68 MBytes
[  5]   3.26-4.18   sec  10.8 MBytes  97.8 Mbits/sec    0   1.72 MBytes
[  5]   4.18-5.16   sec  9.88 MBytes  84.8 Mbits/sec  701   1.21 MBytes
[  5]   5.16-6.00   sec  9.50 MBytes  94.6 Mbits/sec    0   1.33 MBytes
[  5]   6.00-7.08   sec  12.4 MBytes  96.5 Mbits/sec  108   1.00 MBytes
[  5]   7.08-8.07   sec  10.1 MBytes  85.8 Mbits/sec  115    697 KBytes
[  5]   8.07-9.03   sec  11.1 MBytes  97.2 Mbits/sec    8    570 KBytes
[  5]   9.03-10.00  sec  9.50 MBytes  81.8 Mbits/sec    0    606 KBytes
[  5]  10.00-11.00  sec  12.1 MBytes   102 Mbits/sec    0    627 KBytes
[  5]  11.00-12.04  sec  10.9 MBytes  87.7 Mbits/sec    0    639 KBytes
[  5]  12.04-13.19  sec  12.2 MBytes  89.8 Mbits/sec    0    643 KBytes
[  5]  13.19-14.02  sec  9.50 MBytes  95.7 Mbits/sec    0    643 KBytes
[  5]  14.02-15.01  sec  9.38 MBytes  79.3 Mbits/sec    0    643 KBytes
[  5]  15.01-16.83  sec  20.4 MBytes  94.0 Mbits/sec    0    656 KBytes
[  5]  16.83-17.16  sec  4.00 MBytes   100 Mbits/sec    0    660 KBytes
```

Рисунок 10 – Клиент, тест на 30 секунд

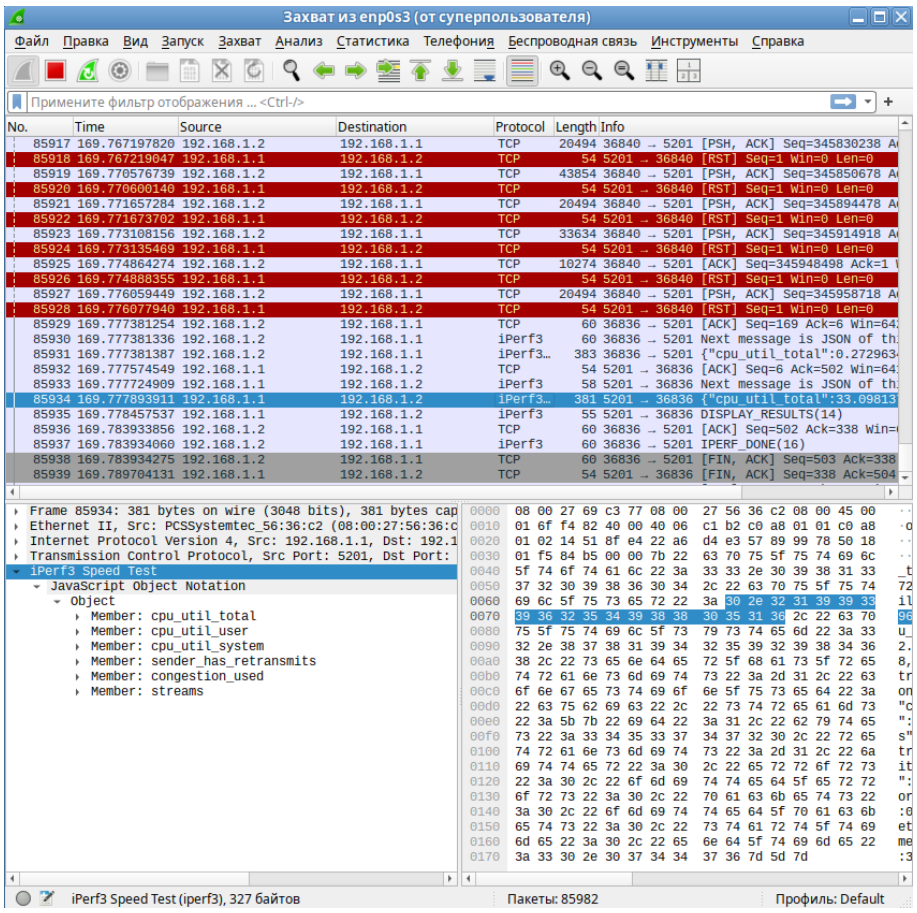

Рисунок 11 – Сервер, тест на 30 секунд (wireshark)

Поменяли местами роли, проведя тест в обратном направлении (сервер отправляет данные клиенту).

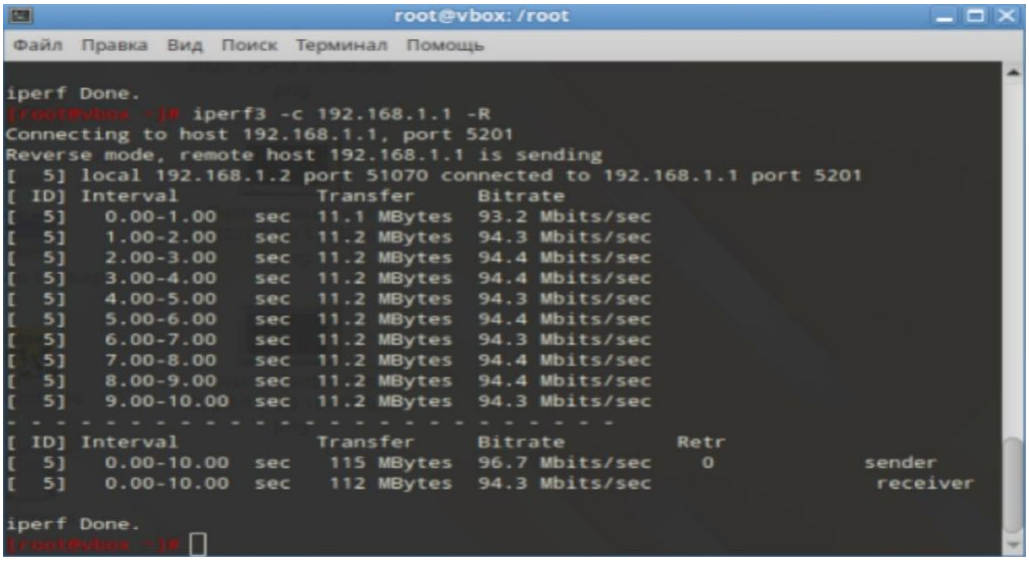

Рисунок 12 – Клиент, тест в обратном направлении

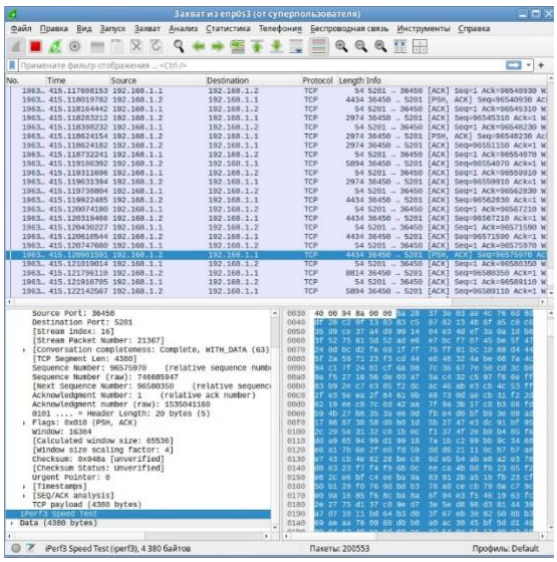

Рисунок 13 – Сервер, тест в обратном направлении (wireshark)

Далее попробовали провести тестирование на 60 секунд с параллельными потоками для полного использования канала.

```
[root@vbox ~]# iperf3 -c 192.168.1.1  -t 60 -P 4 -i5
Connecting to host 192.168.1.1, port 5201
[  5] local 192.168.1.2 port 42934 connected to 192.168.1.1 port 5201
[  7] local 192.168.1.2 port 42940 connected to 192.168.1.1 port 5201
[  9] local 192.168.1.2 port 42942 connected to 192.168.1.1 port 5201
[ 11] local 192.168.1.2 port 42956 connected to 192.168.1.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-6.64   sec  20.0 MBytes  25.3 Mbits/sec    0    873 KBytes
[  7]   0.00-6.64   sec  23.1 MBytes  29.2 Mbits/sec    0   1.04 MBytes
[  9]   0.00-6.64   sec  25.0 MBytes  31.6 Mbits/sec    0   1.13 MBytes
[ 11]   0.00-6.64   sec  20.2 MBytes  25.6 Mbits/sec    0    908 KBytes
[SUM]   0.00-6.64   sec  88.4 MBytes   112 Mbits/sec    0
- - - - - - - - - - - - - - - - - - - - - - - - -
[  5]   6.64-11.39  sec  10.9 MBytes  19.2 Mbits/sec    0   1.22 MBytes
[  7]   6.64-11.39  sec  13.5 MBytes  23.9 Mbits/sec    0   1.33 MBytes
[  9]   6.64-11.39  sec  13.6 MBytes  24.1 Mbits/sec    0   1.33 MBytes
```

Рисунок 14 – Клиент, тест на 60 секунд с параллельными потоками

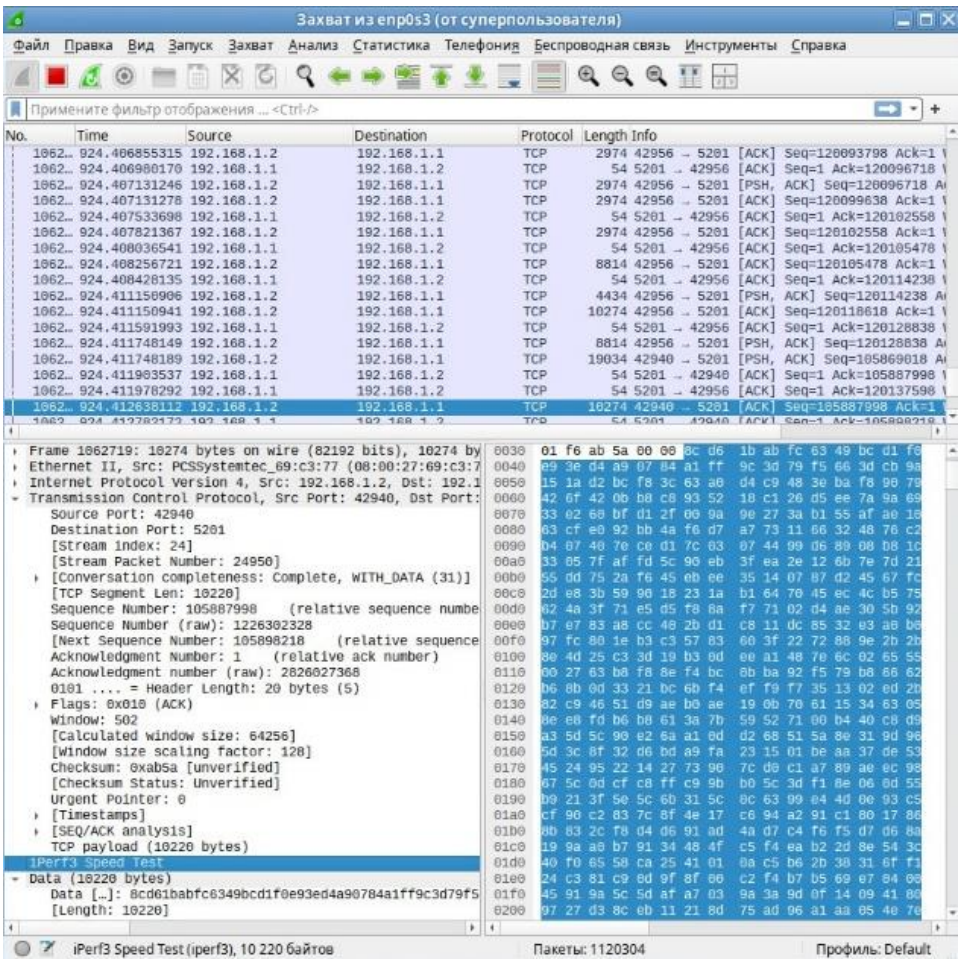

Рисунок 15 – Сервер, тест на 60 секунд с параллельными потоками (wireshark)

Также провели длительное стресс-тестирование сети на 300 секунд.

```
[  5] 285.00-286.00 sec  11.4 MBytes  95.5 Mbits/sec
[  5] 286.00-287.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 287.00-288.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 288.00-289.00 sec  11.4 MBytes  95.4 Mbits/sec
[  5] 289.00-290.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 290.00-291.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 291.00-292.00 sec  11.4 MBytes  95.3 Mbits/sec
[  5] 292.00-293.00 sec  11.2 MBytes  94.5 Mbits/sec
[  5] 293.00-294.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 294.00-295.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 295.00-296.00 sec  11.2 MBytes  94.4 Mbits/sec
[  5] 296.00-297.00 sec  11.2 MBytes  94.3 Mbits/sec
[  5] 297.00-298.00 sec  11.2 MBytes  94.5 Mbits/sec
[  5] 298.00-299.00 sec  11.4 MBytes  95.4 Mbits/sec
[  5] 299.00-300.00 sec  11.2 MBytes  94.3 Mbits/sec
[  5] 300.00-301.00 sec  11.4 MBytes  95.4 Mbits/sec
[  5] 301.00-301.08 sec   768 KBytes  84.3 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-301.08 sec  3.32 GBytes  94.7 Mbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201 (test #14)
-----------------------------------------------------------
```

Рисунок 16 – Стресс-тест на 300 секунд

Проверили пропускную способность при изменении размера окна TCP.

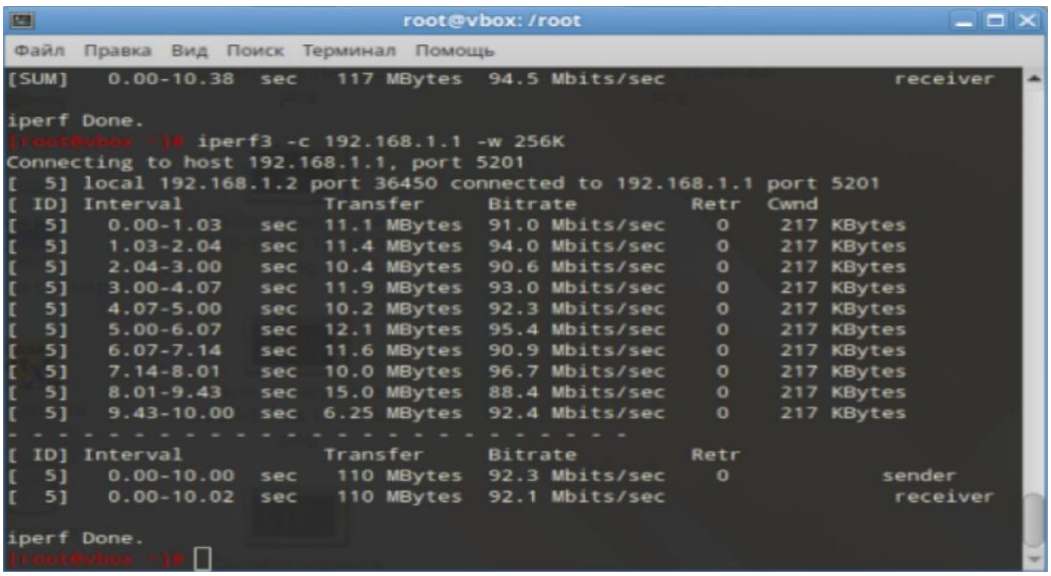

Рисунок 17 – Клиент, тест с изменением окна TCP

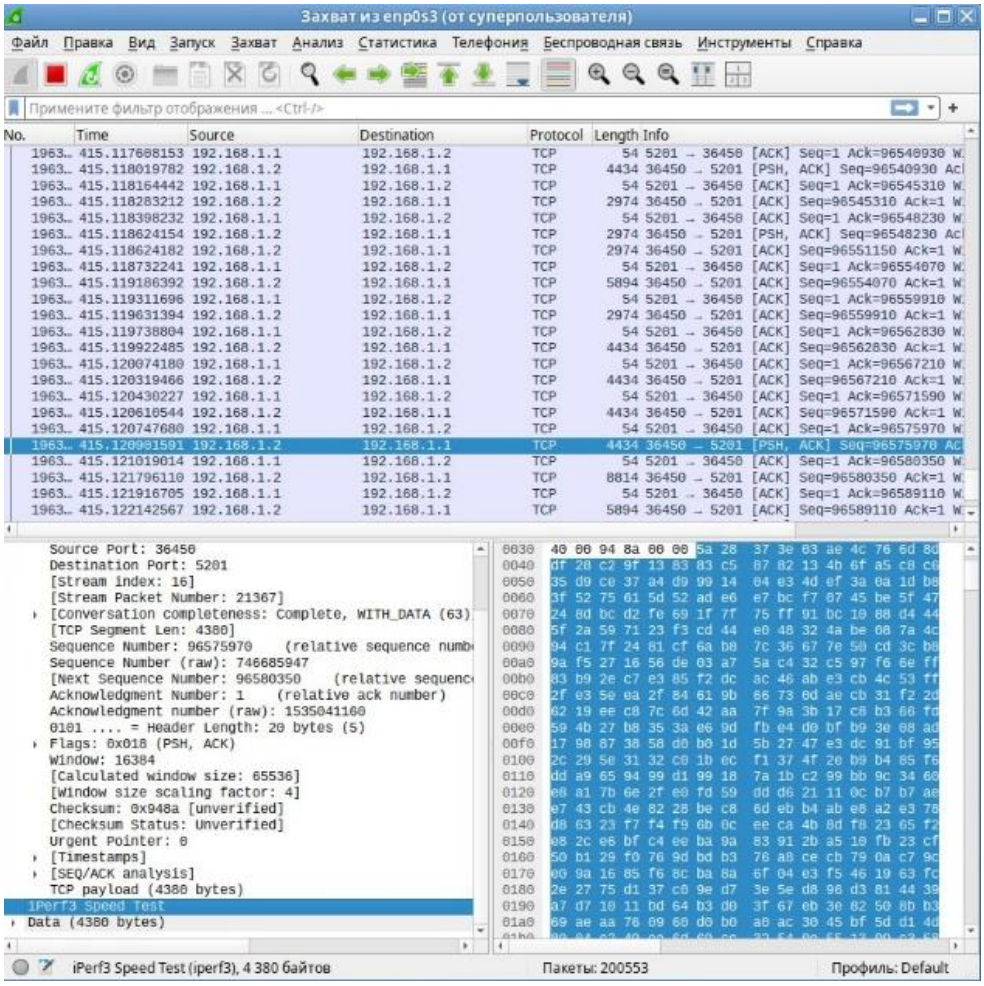

Рисунок 18 – Сервер, тест с изменением окна TCP (wireshark)

Далее провели тестирование сети с максимальной скоростью UDP-трафика. Результат представлен на рисунках 19-20.

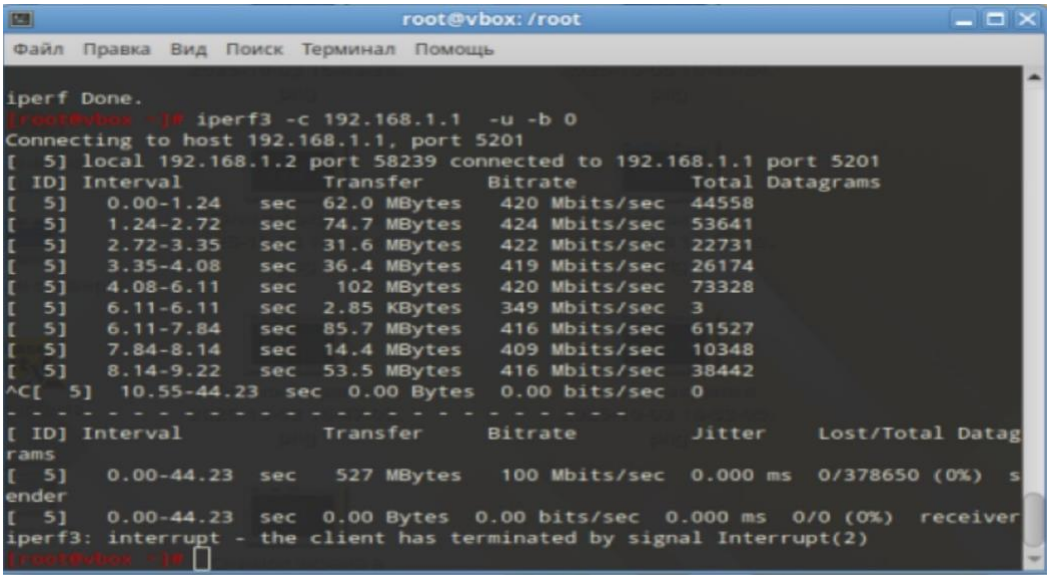

Рисунок 19 – Клиент, тест с максимальной скоростью UDP-трафика

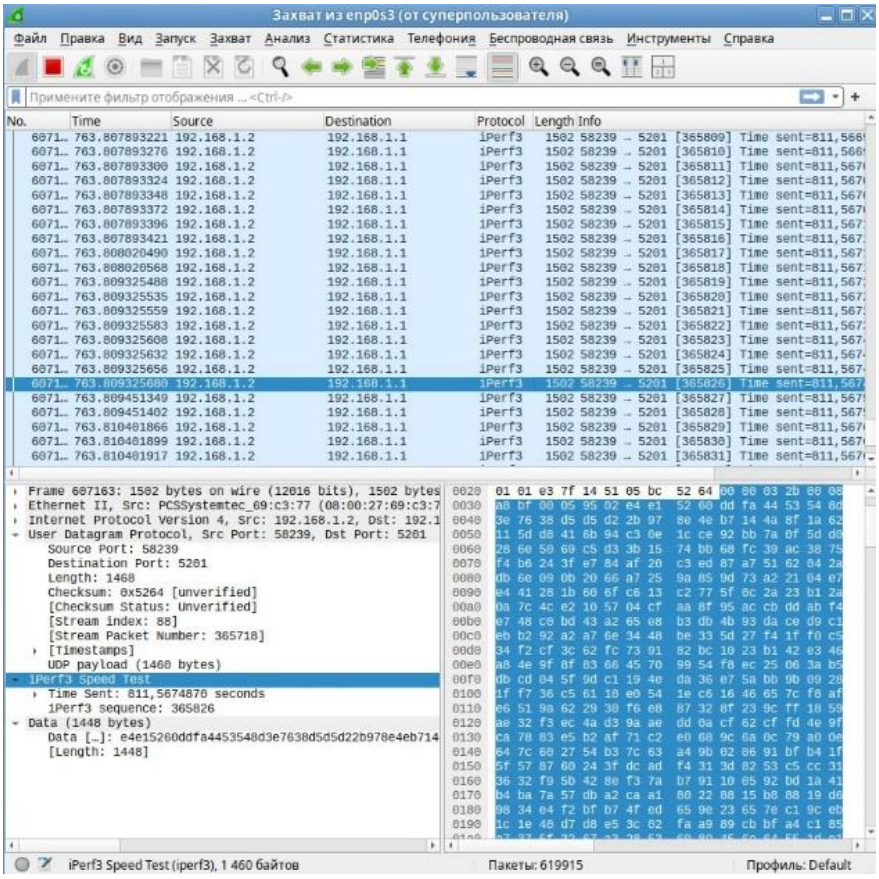

Рисунок 20 – Сервер, тест с максимальной скоростью UDP-трафика (wireshark)

Nping. Провели стресс-тестирование TCP трафиком, использовали команду nping --tcp -p 80 --flags syn --rate 5000 --count 0 192.168.1.1.

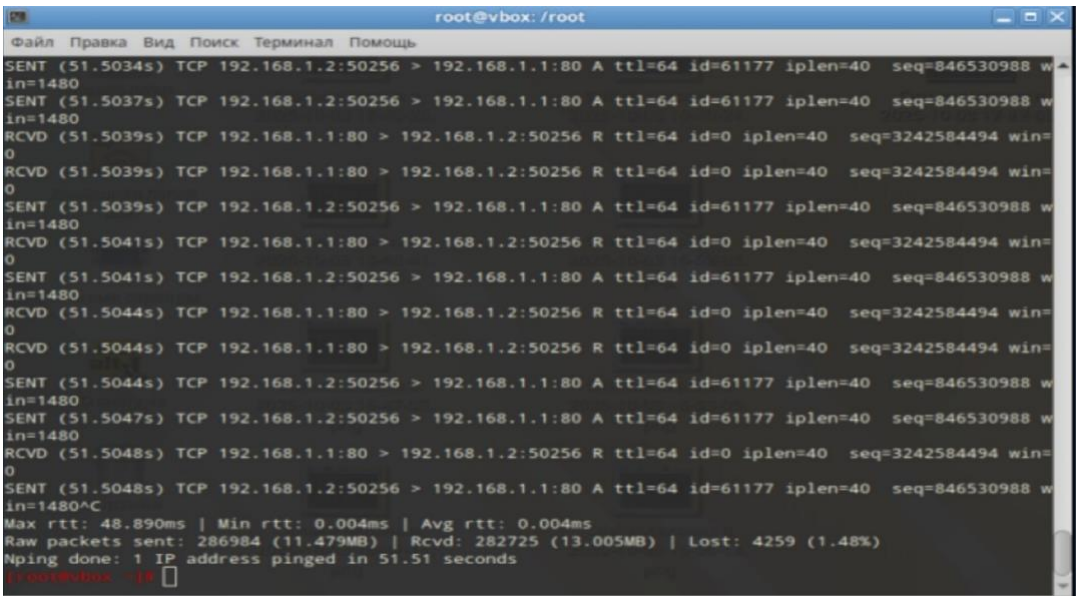

Рисунок 21 – Клиент, тест

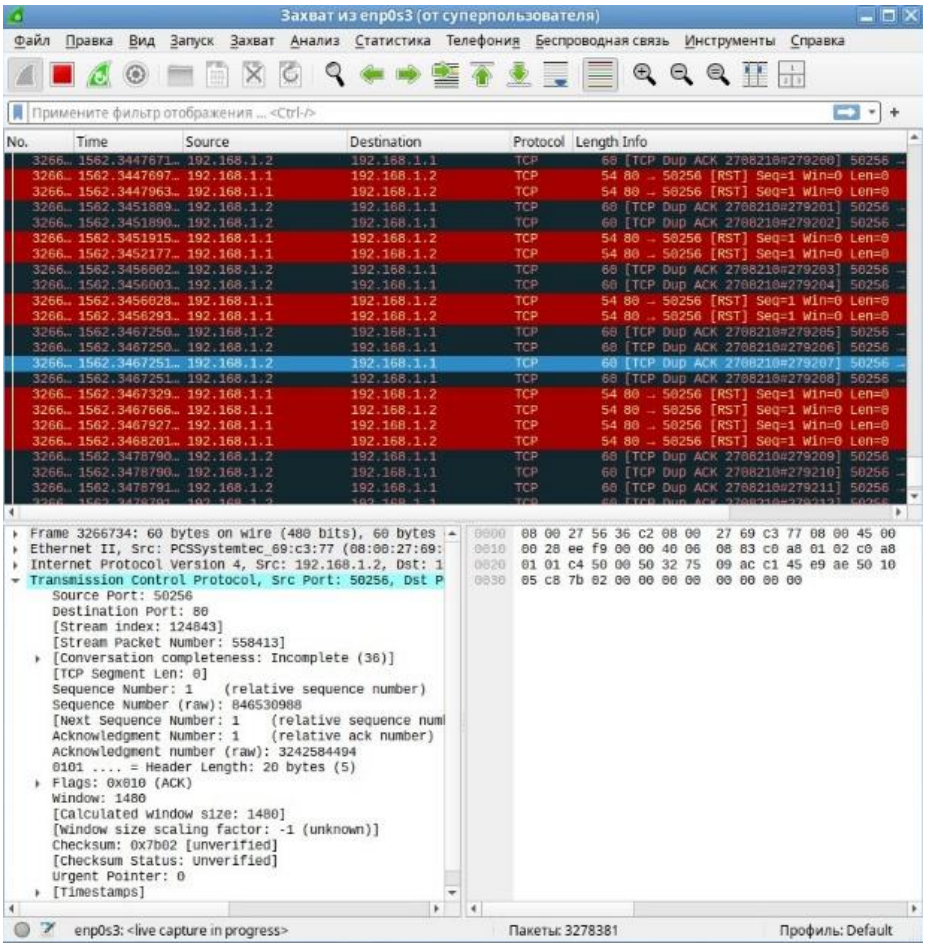

Рисунок 22 – Сервер, стресс-тестирование TCP трафиком

Далее сменили флаг на ack, использовали команду nping --tcp -p 80 --flags ack --rate 500 --count 10000 192.168.1.1.

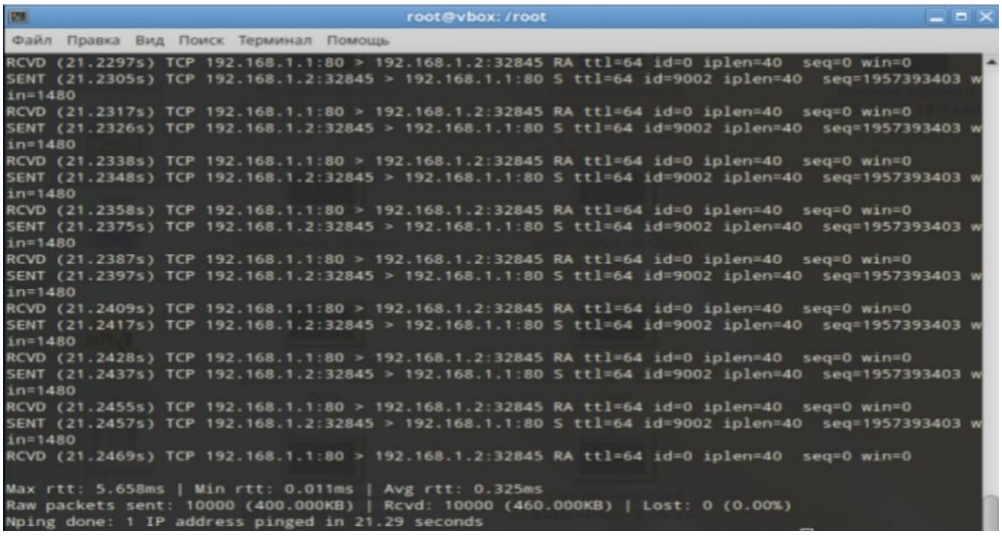

Рисунок 23 – Клиент, тест с измененным на ack флагом

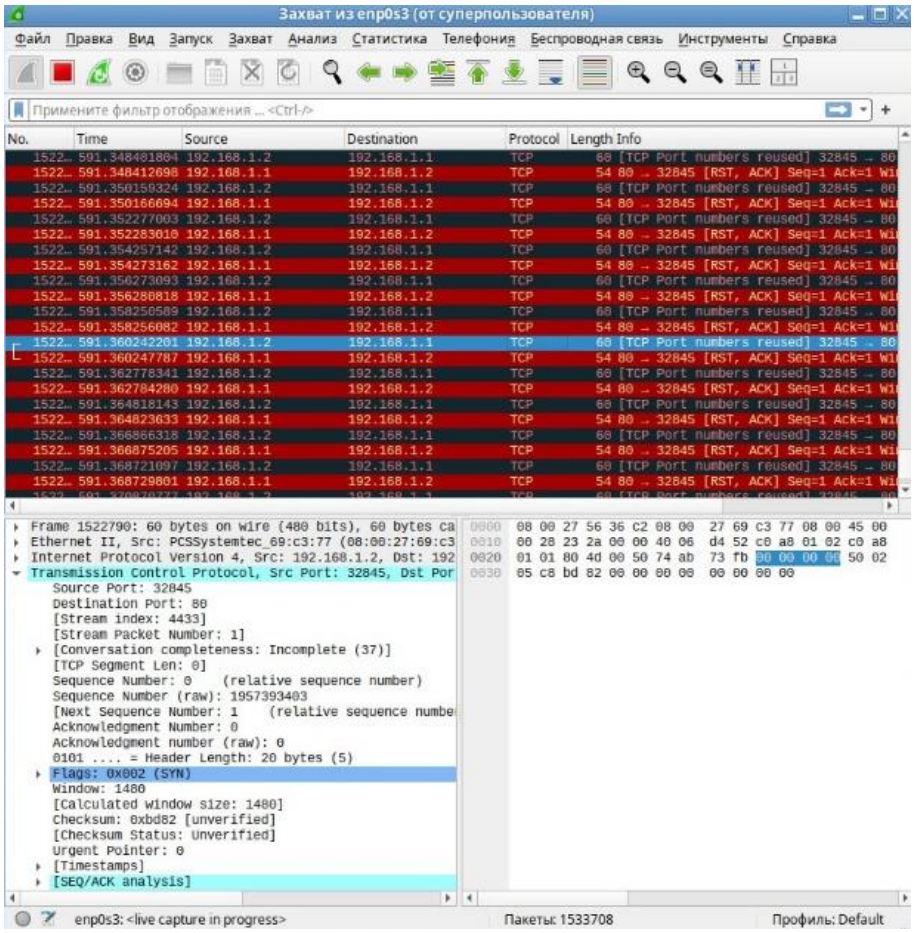

Рисунок 24 – Сервер, тест с измененным на ack флагом (wireshark)

Так как Nping работает и на L3, попробуем генерировать напрямую пакеты, использую команду nping --icmp --rate 1000 --count 1000 192.168.1.1.

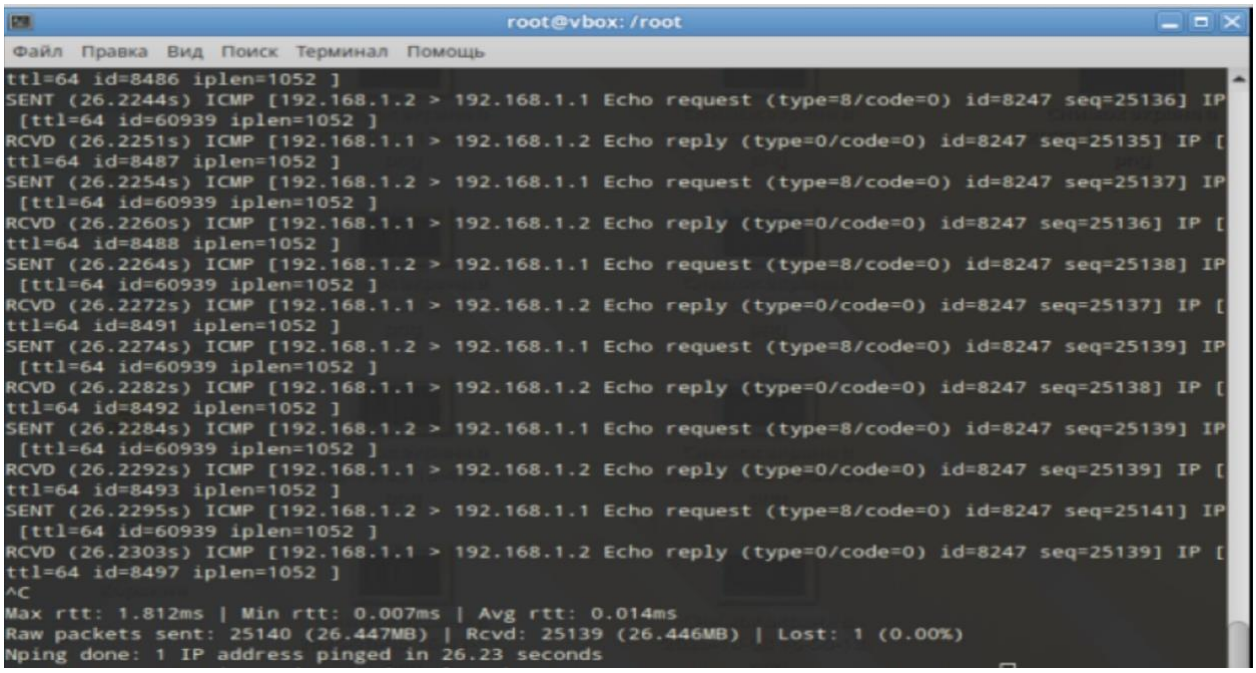

Рисунок 25 – Клиент, генерация пакетов

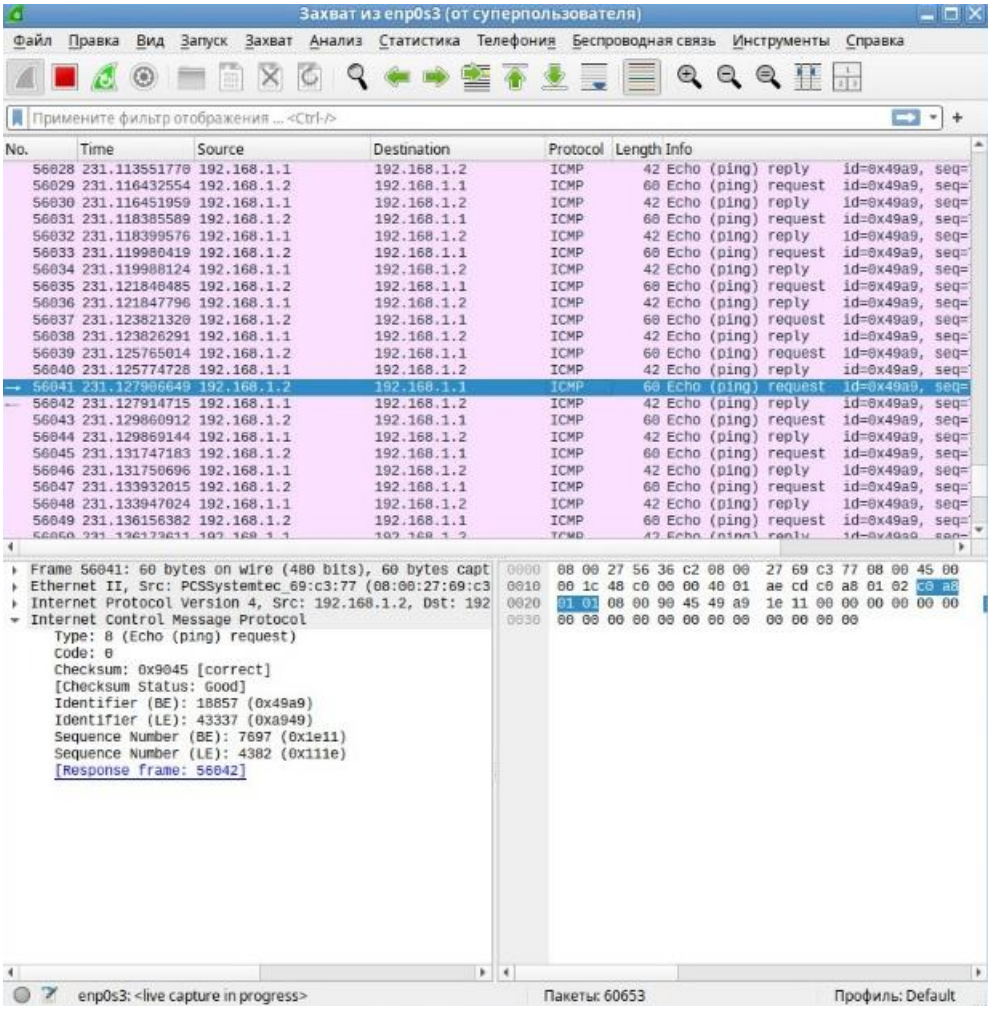

Рисунок 26 – Сервер, тест с генерацией пакетов (wireshark)

Заключение

Таблица 2 – Результаты тестирования пропускной способности

Iperf		Nping		Qperf	
Время тестирования, с	Пропускная способность, МБит/с	Время тестирования, с	Пропускная способность, МБит/с	Время тестирования, с	Пропускная способность, МБит/с
10	97	10	2,3	10	86
60	96	60	2,0	60	83
300	93	90	1,8	300	81
Стресс-тестирование сети					
+		-		+	

В ходе исследования были рассмотрены и применены инструменты для генерации сетевого трафика: Nping, Iperf3 и Qperf. Эксперименты по развертыванию и функциональному тестированию подтвердили их эффективность для оценки пропускной способности как в сегментах LAN, так и в условиях эмуляции WAN-соединений. Nping продемонстрировал возможности по формированию низкоуровневого трафика и проверке доступности, Iperf3 зарекомендовал себя как универсальное и мощное средство для измерения пропускной способности TCP/UDP, а qperf предоставил детальную метрику задержек и производительности.

Выдвинутая гипотеза подтвердилась: наилучший генератор для тестирования пропускной способности – Iperf3 и Qperf, потому что, они обладают высокой мощностью, что подходит для стресс-тестирования, а Nping не подходит, потому что он обладает недостаточно высокой скоростью генерируемого трафика.

Таким образом, сравнительный анализ рассмотренных генераторов трафика и их применение является необходимым этапом для валидации конфигурации сети, планирования её масштабирования и обеспечения отказоустойчивости.

Литература

1. WAN/LAN Network Traffic Generators for Bandwidth & Stress Testing URL: https://www.netadmintools.com/wan-and-lan-network-traffic-generators/

2. Утилита iPerf: тестирование пропускной способности и скорости сети URL:https://winitpro.ru/index.php/2014/11/05/testirovanie-propusknoj-sposobnosti-seti-s-iperf/

3. Инструмент оценки производительности сети Linux (IPERF, QPERF) URL: https://russianblogs.com/article/66693950724/

4.Введение в iperf URL: https://yamadharma.github.io/ru/teaching/simulation-networks/lab/mininet-iperf-intro/

5. Утилита nping: тестирование пропускной способности и скорости сети URL: https://infosecportal.ru/soft/nping/

6. Стресс-тестирование URL: https://serverspace.ru/support/glossary/stress-testirovanie/

7. Функциональное тестирование URL: https://ibs-qa.ru/media/chto-takoe-funktsionalnoe-testirovanie/

8. Qperf - man pages section 1: User commands URL: https://docs.oracle.com/cd/E88353_01/html/E37839/qperf-1.html

9. НОРМИРОВАНИЕ ПОКАЗАТЕЛЕЙ ПРИ ОРГАНИЗАЦИИ КИБЕРПОЛИГОНА ПО СЕТЕВЫМ ТЕХНОЛОГИЯМ Уймин А.Г. В книге: Нефть и газ - 2024. Тезисы докладов 78-ой Международной молодежной научной конференции. Москва, 2024. С. 1253-1254.