**Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/**
URL статьи: **mathmod.esrae.ru/48-196**
**Ссылка для цитирования этой статьи:**
Патрин П.С., Дрогайцева О.В. Использование анализаторов трафика для улучшения работы сетей передачи данных // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2024. №2

УДК 004.042 DOI:10.24412/2541-9269-2024-4-10-19

# ИСПОЛЬЗОВАНИЕ АНАЛИЗАТОРОВ ТРАФИКА ДЛЯ УЛУЧШЕНИЯ РАБОТЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

П.С. Патрин[1], О.В .Дрогайцева[2]

[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, workpostoffice23@gmail.com
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, o.drogaytseva@gmail.com

# USING TRAFFIC ANALYZERS TO IMPROVE THE PERFORMANCE OF DATA NETWORKS

P.S. Patrin[1], O.V. Drogaytseva[2]

[1]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, workpostoffice23@gmail.com
[2]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, o.drogaytseva@gmail.com

**Аннотация:** В настоящей статье рассматриваются вопросы о теории телетрафика, принципах работы сетей передачи данных, представлены средства анализа сетевого трафика. В работе приведено рассмотрение наиболее популярных программных средств для анализа и мониторинга сетевого трафика, таких как Wireshark, EtherSensor и Plixer Scruinizer. Особое внимание уделено программному средству Wireshark, которое используется для анализа нагрузки на сеть и обеспечения качества обслуживания в различных локальных сетях. Приводятся примеры анализа нагрузок с использованием Wireshark и рекомендации для повышения качества обслуживания в локальных сетях.

**Ключевые слова:** анализ сетевого трафика, Wireshark, анализ нагрузки на пакетные сети.

**Abstract:** This article discusses the theory of teletraffic, the principles of data networks, and presents network traffic analysis tools. The paper analyzes the most popular software tools for analyzing and monitoring network traffic, such as Wireshark, EtherSensor, and Plixer Scruinizer. Particular attention is paid to the Wireshark software tool, which is used to analyze network load and ensure quality of service in various local networks. Examples of load analysis and recommendations for improving the quality of service in local networks are given.

**Keywords:** network traffic analysis, Wireshark, packet network load analysis.

**Введение в сети передачи данных.** Сети передачи данных – это совокупность различных устройств, соединенных между собой с помощью линий связи, которые предназначены для передачи информации в цифровом виде. Сети передачи данных формируют различный сетевой трафик:

1. Трафик данных – это трафик передачи файлов, электронной почты, документов.
2. Голосовой трафик – это трафик, по которому передаются голосовые сообщения (VoIP-трафик).
3. Мультимедийный трафик – это трафик, по которому передается потоковое видео.
4. Сигнальный трафик – это трафик, который служит для контроля и управления различными сетевыми устройствами.

Для эффективного управления различными данными и их нагрузкой на сеть передачи данных необходимо понимать устройство сети передачи данных. Этому посвящена теория телетрафика [1].

**Теория телетрафика.** Теория телетрафика берет свое начало из работ датского инженера А.К. Эрланга по расчету вероятности потерь телефонных вызовов на телефонной станции при определенном количестве соединительных линий. Теория телетрафика, в том числе, изучает оптимизацию ресурсов и анализ нагрузки на сеть передачи данных. В настоящее время теория телетрафика широко используется при построении и оптимизации вычислительных сетей с коммутацией пакетов [2].

**Коммутация пакетов.** Технология коммутации пакетов была разработана Управлением перспективных исследовательских проектов Министерства обороны США (DARPA) в 1989 г. и впервые применена при построении компьютерной сети ARPANET. Примерно в то же время в СССР велись аналогичные разработки, которые начались в 1970-х годах. Одним из известных проектов стала сеть «Огонек» [3].

Основой современных сетей является протокол IP (Internet Protocol). В сочетании с протоколом TCP (Transmission Control Protocol) образуют модель (стек) TCP/IP.

Стек TCP/IP изначально создавался для глобальных гетерогенных сетей (Интернет), где важна надежная передача информации. Преимущества TCP/IP – это способность фрагментировать сетевые пакеты, гибкая система адресации, разумное и экономное использование широковещательных пакетов. Недостатки TCP/IP – это высокие требования к аппаратной части и сложность администрирования.

Для поддержания работоспособности таких сетей необходим постоянный мониторинг и анализ сетевого трафика.

**Анализ сетевого трафика для управления нагрузкой.** Постоянный анализ сетевого трафика в сетях помогает обеспечить стабильную работу сети,

а также свести к минимуму перегрузки в сети. Основные функции анализа сетевого трафика:

1. Выявление проблемных мест в сети.
2. Оптимизация маршрутов передачи данных.
3. Формирование отчетов для дальнейшей диагностики.

Далее будут рассмотрены программные средства, которые автоматизируют процесс анализа сетевого трафика.

**Программные средства для анализа сетевого трафика.** Существует множество программных средств для анализа сетевого трафика, каждое из которых обладает своими уникальными функциями:

1. Wireshark [5] – это программное средство для захвата и анализа сетевого трафика, который активно используется как для образовательных целей, так и для устранения неполадок на компьютере или в сети. Wireshark работает практически со всеми протоколами модели OSI, обладает понятным для обычного пользователя интерфейсом и удобной системой фильтрации данных.
2. EtherSensor [6] – это программная платформа для анализа сетевого трафика в режиме реального времени, которая распознает такие объекты пользовательских и системных коммуникаций, как сообщения, файлы и сетевые события.
3. PlixerScrutinizer [7] – это программное средство, предназначенное для мониторинга и анализа сети. PlixerScrutinizer собирает и интерпретирует данные о каждой цифровой транзакции, а также формирует подробные отчёты о состоянии и безопасности сети.
4. JDSU NetworkAnalyzer – это масштабируемое программное средство, которое позволяет анализировать сеть и своевременно устранять неполадки в сети.

Среди всех представленных решений наиболее универсальным, функциональным и поддерживаемым программным средством является Wireshark. Также Wireshark позволяет анализировать более 1000 сетевых протоколов, выпускается по общедоступной лицензии GNU, имеет открытый исходный код и позволяет захватывать сетевые пакеты в реальном времени.

**Анализ сетевого трафика с использованием Wireshark**

Рассмотрим несколько практических примеров использования Wireshark для анализа сетевого трафика.

**Анализ загрузки сети**

При помощи анализа загрузки сети можно выявить пики нагрузки сети в течение дня. Это позволит спланировать меры по уменьшению нагрузки на сеть. Для того чтобы посмотреть график нагрузки на сеть в Wireshark, необходимо начать захват пакетов, а затем перейти на вкладку «Статистика» и выбрать «Графики ввода/вывода». График ввода/вывода Wireshark представлен на рис. 1.

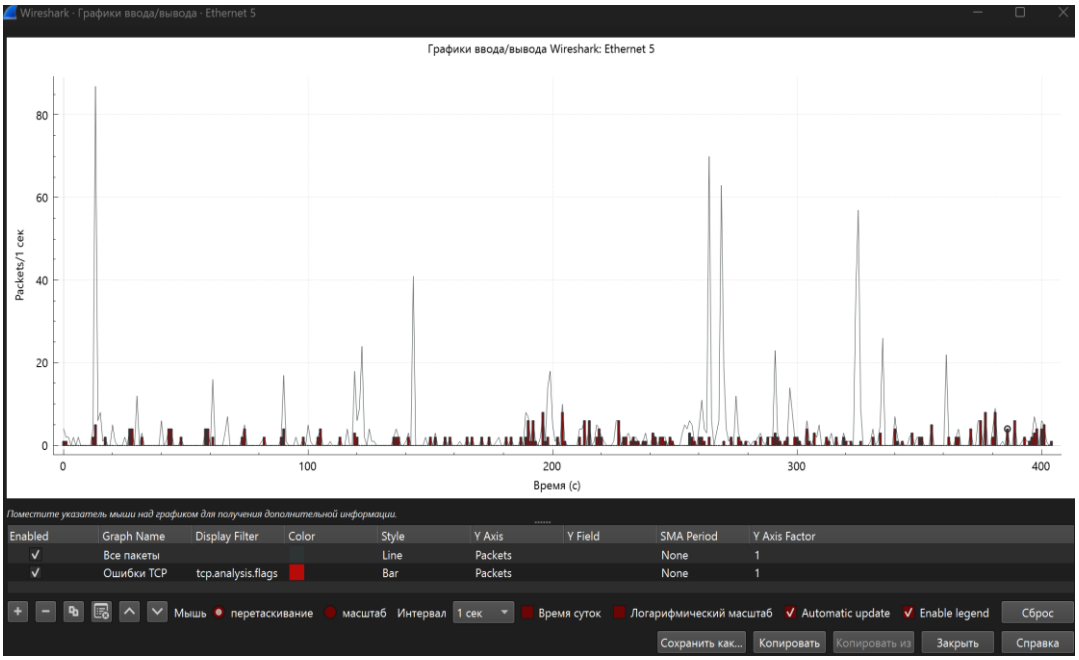


Рис. 1. График ввода/вывода Wireshark

## Поиск неисправностей

Для поиска сетевого трафика для конкретного IP-адреса или сетевого протокола в Wireshark используются фильтры. На рис. 2 представлены сетевые пакеты, отфильтрованные при помощи фильтра ip.addr == 192.168.189.19. Во втором столбце с названием «Time» находится временная метка сетевых пакетов. Большое время ожидания может указывать на проблемы с маршрутизацией или на перегрузку сети.

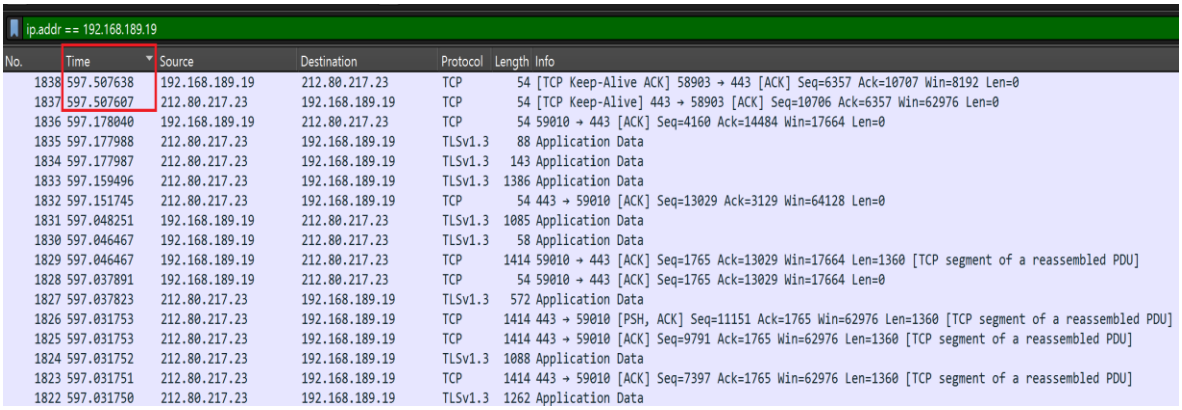


Рис. 2. Сетевые пакеты в Wireshark с фильтром ip.addr == 192.168.189.19

## Обнаружение нежелательного сетевого трафика

Также фильтры можно использовать для обнаружения подозрительного или нежелательного сетевого трафика в сети. Например, фильтр tcp.port == 22

можно использовать для анализа SSH-сессий, которые могут быть нежелательными для конкретной реализации сети. Wireshark предоставляет возможность сохранять сетевые пакеты в файл для последующего анализа сетевого трафика и выявления угроз безопасности. На рис. 3 представлены сетевые пакеты, отфильтрованные при помощи фильтра tcp.port == 22.

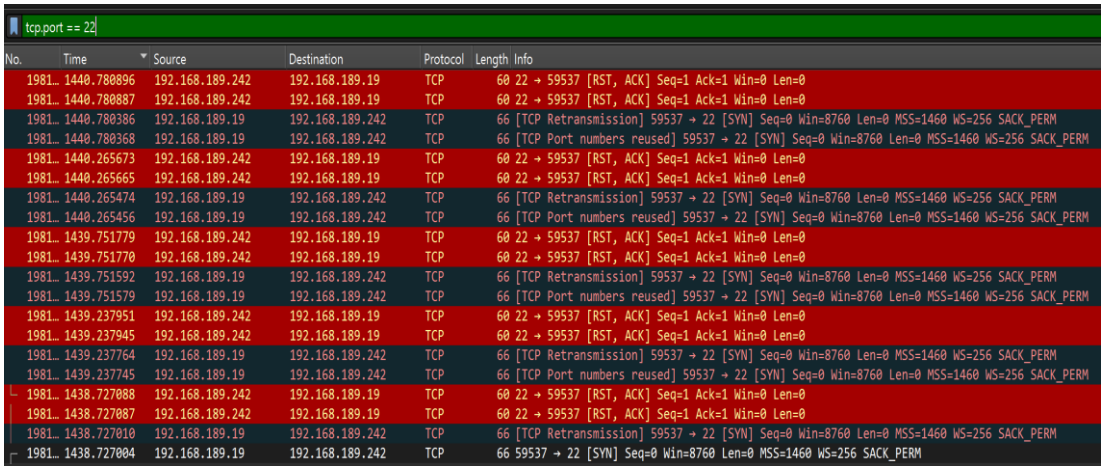


Рис. 3. Сетевые пакеты в Wireshark с фильтром tcp.port == 22

## Экспорт объектов из сетевого трафика

Для экспорта объектов из сетевого трафика в Wireshark применяется функция «Экспорт объектов». Wireshark анализирует HTTP потоки в сетевом трафике, которые были захвачены данным программным средством. Wireshark позволяет извлечь такие объекты, как файлы изображений, исполняемые файлы и другие объекты, которые можно передать по протоколу HTTP.

Чтобы воспользоваться функцией экспорта объектов из сетевого трафика, необходимо открыть вкладку «Файл», затем выбрать «Экспорт объектов» и перейти в раздел «HTTP», как показано на рис. 4. Все найденные файлы будут отображаться в новом окне, где можно будет сохранить выбранные файлы.

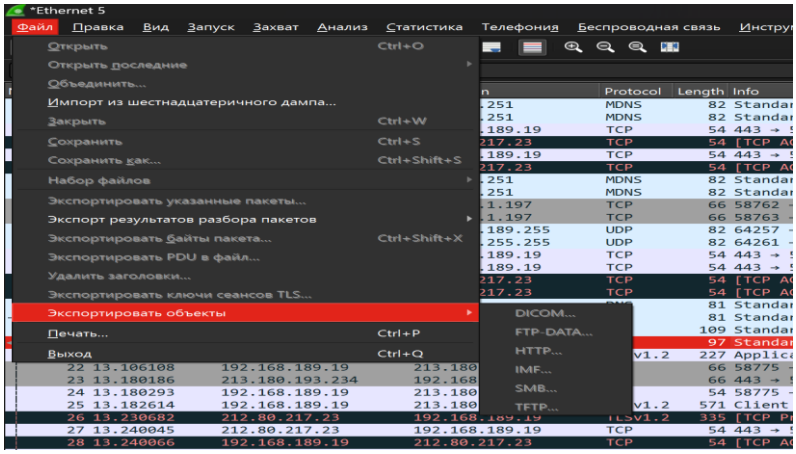


Рис.4. Экспорт объектов в Wireshark

Разберем подробнее поиск и возможное устранение ошибок, связанных, например, с сетевой задержкой.

Сетевая задержка (задержка в сети) - это задержка по времени при передаче запросов от компьютера к серверу в сети. Давайте выясним, как можно найти и убрать задержку в сети. Активность пользователя в сети – это запрос, а время отклика веб-страницы – это время, которое необходимо для ответа на этот запрос. Задержка по времени - это еще то время, которое сервер тратит на обработку и выполнение запроса. Следовательно, задержка по времени определяется как суммарный путь – это время для записи, обработки и получением пользователем запроса. Длительные задержки не приветствуются, так как они ухудшают процесс обмена данными с компьютером (пользователем).

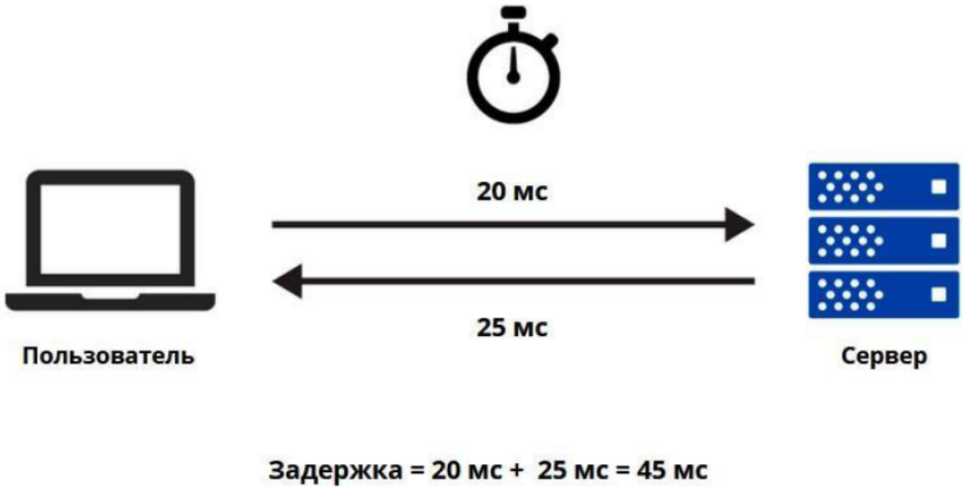


Рис. 5. Сетевая задержка

**Что может вызывать задержку?** Существует некоторое количество основных причин медленного сетевого подключения:

1. Большая задержка.
2. Зависимость приложений.
3. Потеря пакетов.
4. Перехватывающие устройства в сети.

Рассмотрим каждую из выше приведенных основных причин задержки в сети, а также рассмотрим, как можно исключить эти проблемы с помощью программы Wireshark.

**Большая задержка.** Понятие «большая задержка» - это время, которое требуется для передачи данных от одной точки к другой. Влияние «большой задержки» на передачу данных в сети очень большое. На диаграмме в качестве примера показано время кругового пути при загрузке файла по пути с высокой задержкой. Если время задержки кругового пути будет превышать одну секунду - это недопустимо!

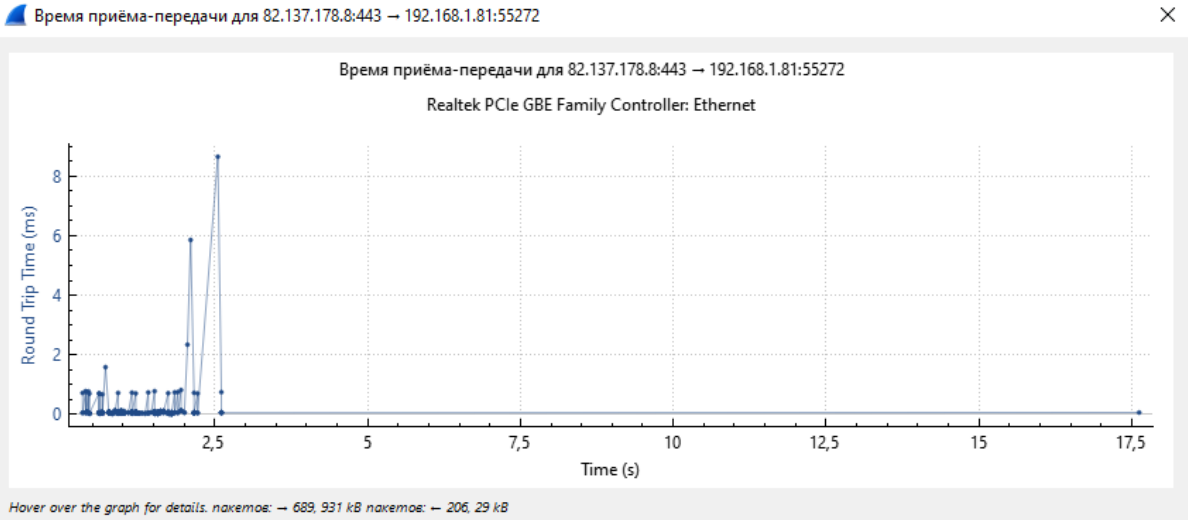


Рис. 6. Время пути

Программу Wireshark используют для расчета времени кругового пути, чтобы понять, что является причиной плохой работы протокола управления передачей TCP. Этот протокол используется для разных целей, например, для передачи данных, для просмотра веб-страниц и многого другого. В большинстве случаев операционную систему компьютера можно настроить так, чтобы в сети с большой задержкой она работала более эффективно.

**Зависимости приложений.** Некоторые приложения зависят от каких-то других приложений, процессов или обмена данными с другим хостом. Предположим, что приложение – это какая-то база данных, и оно зависит от подключения к другим серверам. В этом случае слабая производительность на «других серверах» может плохо повлиять на время загрузки приложения. Например, просмотр веб-страниц, но только при условии, что сервер ссылается на другие веб-сайты. Например, чтобы зайти на главную страницу сайта, вы должны сначала посетить 6 хостов, которые обеспечивают главную страницу рекламой и всем остальным.

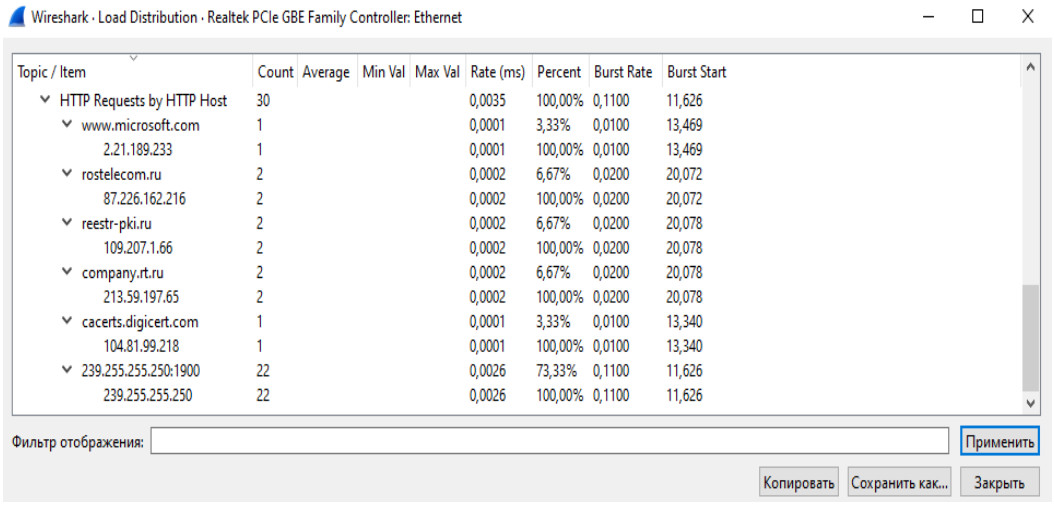


Рис. 7. Количество хостов

На приведенном выше рис. 7 показано окно «Load Distribution» в Wireshark. В нем отображается список всех серверов, которые использует главная страница сайта.

**Потеря пакетов.** Потеря пакетов – это самая часто встречающиеся проблема в сети. Потеря пакетов может происходить, когда пакеты неправильно доставляются от отправителя к получателю по сети Интернет. Например, пользователь посещает выбранный веб-сайт и начинает загружать с сайта информацию, потерянные пакеты вызывают их повторную передачу, что соответственно увеличивает скорость загрузки веб-файлов и замедляет процесс загрузки. Также, потеря пакетов оказывает негативное влияние на приложение, когда оно использует протокол TCP. Когда соединение обнаруживает потерянный пакет, то скорость передачи автоматически снижается, для того чтобы компенсировать сетевые проблемы. Далее скорость может постепенно восстанавливаться до более-менее приемлемого уровня до следующего потерянного пакета, что обязательно приведет снова к снижению скорости передачи данных.

Что же все-таки значит – «пакет потерян»? Вот если программа работает через протокол TCP, то потеря пакетов может быть обнаружена двумя способами. В первом случае получатель отслеживает пакеты по их порядковым номерам и тогда можно обнаружить отсутствующий пакет. В этом случае клиент делает три запроса на этот отсутствующий пакет (из-за двойного подтверждения), после этого он отправляется повторно. Во втором случае потерянный пакет обнаруживает отправитель, когда понимает, что получатель не подтвердил получение пакета, и после ожидания отправляет пакет данных повторно.

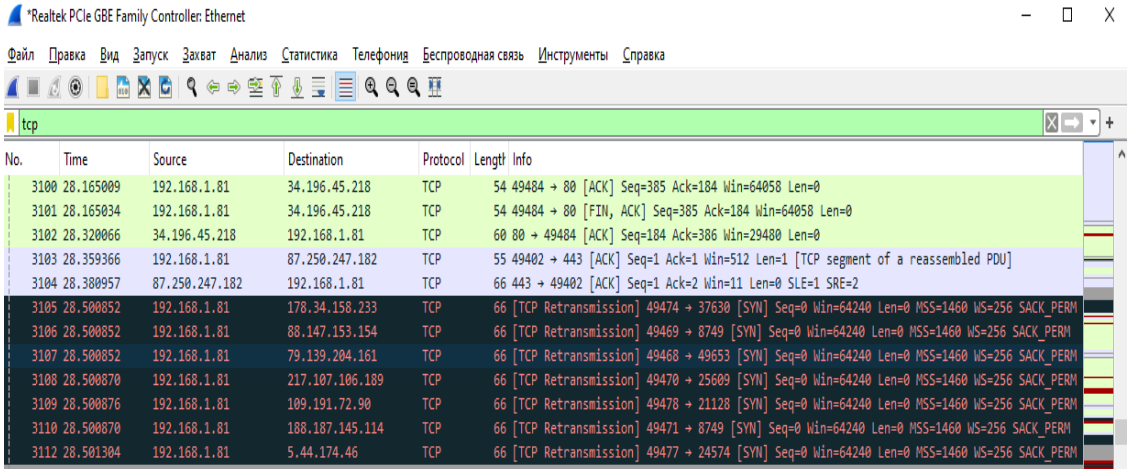


Рис. 8. Статистика пакетов

Wireshark показывает, что произошла перегрузка сети, а многократные подтверждения провоцируют повторную передачу трафика, который выделен другим цветом. Большое количество повторных подтверждений указывает на

то, что пакеты были потеряны, а также влияет на существенную задержку в сети. Для того чтобы повысить производительность сети, важно определить точное место потери пакетов. Когда Wireshark обнаруживает потерю пакетов, он начинает перемещается до тех пор, пока не найдет место потери пакетов. В данный момент это и есть та точка начала потери пакетов, которая указывает, на чем нужно сосредоточиться.

**Перехватывающие устройства.** Сетевые перехватчики – это коммутаторы, маршрутизаторы и брандмауэры, которые выбирают направления передачи данных. При потере пакетов эти устройства первыми необходимо проверить, потому что как раз они могли стать причиной потери. Например, если установлен приоритет трафика, то дополнительная задержка может возникнуть в потоке с низким уровнем приоритета.

**Заключение**

Для того чтобы эффективно управлять сетью, необходимо обеспечить должное качество обслуживания сети. Качество обслуживания достигается за счет передачи пакетов без их потерь, правильной маршрутизации данных, а также обеспечения корректной работы конечных сервисов и приложений. Использование анализаторов сетевого трафика, таких как Wireshark, позволяет предотвращать перегрузку сети, задержку в сети, следить за нежелательным трафиком в сети, повышать безопасность, а также улучшать качество обслуживания сети. Эти инструменты помогают в планировании и масштабируемости сети. Одним из перспективных направлений развития анализаторов трафика является интеграция с системами искусственного интеллекта, что позволит наиболее эффективно выявлять различные аномалии в сетевом трафике и корректно определять, а также прогнозировать нагрузку на сеть передачи данных.

## Литература

1. ГОСТ Р 56939-2016. Системы связи. Обеспечение качества обслуживания. Основные положения и требования. – М.: Стандартинформ, 2016.
2. Соловьев В.В. Теория телетрафика. Учебное пособие. – М.: Горячая линия – Телеком, 2019. – 384 с.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2013. – 960 с.
5. Wireshark User Guide. URL: https://www.wireshark.org/docs/ (дата обращения: 22.11.2024).
6. EtherSensor. URL: https://www.microolap.ru/products/ethersensor/ (дата обращения: 23.11.2024).
7. Plixer Scrutinizer Network Analyzer. URL: https://www.plixer.com/ (дата обращения: 23.11.2024).
8. Петухов С.Н. Программные средства анализа сетевого трафика. Учебное пособие. – М.: Финансы и статистика, 2020. – 156 с.

9. Козлов А.В. Сетевые технологии. Основы и анализ. – СПб.: БХВ-Петербург, 2021. – 320 с.
10. Савинков Д.Н., Федоров И.П. Практическое использование системы анализа трафика Wireshark. – М.: ДМК Пресс, 2022. – 112 с.