25th International Scientific Conference UNITECH

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025
GABROVO

АНАЛИЗ И ОПТИМИЗАЦИЯ НА МРЕЖОВИЯ ТРАФИК В РЕАЛНО ВРЕМЕ

Иван Златев*, Красен Ангелов, Боян Карапенев

Технически Университет, Габрово, България
**кореспондиращ автор: idzlatev78@gmail.com*

REAL-TIME NETWORK TRAFFIC ANALYSIS AND OPTIMIZATION

Ivan Zlatev*, Krasen Angelov, Boyan Karapenev

Technical University of Gabrovo, Bulgaria
**Corresponding author: idzlatev78@gmail.com*

Abstract
In the report, the methods, technologies, and algorithms for real-time network traffic analysis and optimization are examined. With the increasing demands for speed, reliability, and security in communication networks, traffic management has become a critical factor for the efficiency of IT infrastructure. The report presents modern approaches to monitoring, machine learning, Quality of Service (QoS), Software Defined Networking (SDN), as well as AI-based optimization

Keywords: SDN;QoS; NetFlow; Zabbix; Wireshark; tcpdump; nProbe;

ВЪВЕДЕНИЕ

В бързо развиващата се дигитална инфраструктура, където информационните потоци достигат мащаби от терабайти в секунда, управлението и оптимизацията на мрежовия трафик се превръщат в критичен фактор за надеждната работа на всички съвременни ИТ системи. С нарастването на броя на свързаните устройства, интернет услугите и облачните платформи, натоварването върху комуникационните канали и маршрутизиращите устройства се увеличава експоненциално. Това налага внедряването на интелигентни решения, които да позволят анализ и контрол в реално време.
Анализът в реално време на мрежовия трафик позволява не само подобряване на производителността и качеството на услугите (QoS), но и навременно откриване на аномалии, атаки, неефективно използване на ресурси и потенциални откази. Компаниите и институциите се стремят към пълна видимост върху своите мрежови операции, тъй като дори кратковременна загуба на свързаност може да доведе до сериозни финансови и оперативни последици.
Основната цел на настоящия доклад е да се изследват методите за анализ и оптимизация на мрежовия трафик в реално време, като се акцентира върху съвременни алгоритми, архитектури и инструменти – по-специално върху Cisco NetFlow и Zabbix като интегрирана платформа за наблюдение и управление.

1. Теоретично представяне на мрежовия трафик

1.1. Понятие за мрежов трафик

Мрежовият трафик представлява обемът от данни, който се предава през дадена мрежова инфраструктура за определен период от време. Този поток може да включва файлов трансфер, уеб заявки,

Print ISSN: 1313-230X, Online ISSN: 3033-1404

гласови пакети, видео стрийминг, телеметрични данни и други видове комуникации.

Мрежовият трафик може да се класифицира по различни признаци:

- **Тип на протоколите:** TCP, UDP, ICMP, HTTP, HTTPS, DNS и др.
- **Посока на комуникацията:** входящ, изходящ, междувъзлов, мултикаст.
- **Ниво на натоварване:** ниско, средно и високо.

Разбирането на структурата и динамиката на трафика е предпоставка за неговото ефективно управление. Например, HTTP/2 и QUIC променят начина, по който се използват TCP/UDP потоците, което от своя страна изисква нови методи за мониторинг и анализ.

1.2. Основни метрики за анализ на мрежовия трафик

При анализа на мрежовия трафик се използват ключови показатели, които определят неговото качество и ефективност:

- **Пропускателна способност (Throughput):** количеството данни, пренесени успешно за единица време.
- **Латентност (Latency):** времето, необходимо за достигане на пакета от източника до дестинацията.
- **Загуба на пакети (Packet loss):** процентът на изгубените пакети по пътя, показател за претоварване или проблеми в инфраструктурата.
- **Jitter:** вариацията във времето между последователни пакети — особено критична при VoIP и видео комуникации.
- **QoS показатели:** набор от метрики, които определят приоритетите на услугите в зависимост от бизнес изискванията.

Съвременните системи за мониторинг като Zabbix, NetFlow и Prometheus осигуряват непрекъснато измерване на тези параметри, което позволява динамична оптимизация и превенция на аномалии.

2. Методи за анализ на мрежовия трафик

2.1. Анализ на пакети

Пакетният анализ е класическият и най-прецизен метод за изследване на мрежовия трафик. При него всеки пакет, преминаващ през мрежовото устройство, се улавя и декодира. Инструменти като **Wireshark**, **tcpdump** и **nProbe** позволяват детайлна инспекция на заглавните полета, времеви отметки и протоколни взаимодействия.
Този подход е изключително ефективен при диагностика на конкретни проблеми, но при големи корпоративни мрежи изисква значителен процесорен и дисков ресурс. Поради това, в реалновременни среди, пакетният анализ често се използва в комбинация с потокови методи.

2.2. Поточен анализ (Flow-based monitoring)

Flow-базираните технологии като **Cisco NetFlow**, **IPFIX** и **sFlow** групират пакетите според общи атрибути — източник, дестинация, порт и протокол — и ги анализират като логически потоци. Предимството е, че се съкращава обемът от данни за обработка, като се запазва ключовата информация. Този подход е основа на съвременните решения за мрежова видимост и автоматична оптимизация.
NetFlow колекторите могат да обработват стотици хиляди потоци в секунда, което позволява динамично наблюдение

на 1000+ клиента при 10GbE интерфейси.

2.3. Статистически и машинно обучителни методи

С развитието на изкуствения интелект се налагат **ML-базирани методи** за откриване на отклонения и прогнози на натоварванията.

Примерни подходи:

- **K-means и DBSCAN** – клъстеризация на нормален и аномален трафик.
- **LSTM невронни мрежи** – предсказване на бъдещи стойности на натоварване.
- **Autoencoder** – откриване на необичайни модели на поведение.

Тези модели могат автоматично да сигнализират при подозрителна активност или да извършат корегиращи действия като пренасочване на потоци, ограничаване на скорости или промяна на приоритети.

3. Оптимизация на мрежовия трафик в реално време

3.1. Алгоритми за динамично маршрутизиране

Динамичното маршрутизиране позволява на мрежата да адаптира своите маршрути според текущите условия.

Най-често използвани са:

- **OSPF (Open Shortest Path First)** – определя най-краткия път чрез Dijkstra алгоритъм;
- **EIGRP (Enhanced Interior Gateway Routing Protocol)** – комбинира скорост и надеждност чрез многокритериална оценка;
- **SDN (Software Defined Networking)** – отделя контролния от транспортния слой и позволява централизирана оптимизация в реално време чрез контролери като OpenDaylight или ONOS.

3.2. Балансиране на натоварването

Load balancing е техника за равномерно разпределение на мрежовия трафик между множество сървъри, маршрути или услуги.
Методи като *Round Robin*, *Least Connections* и *Adaptive Load Balancing* гарантират, че нито един ресурс няма да бъде претоварен.
При анализа на трафика в реално време, балансирането може да се управлява автоматично чрез Zabbix triggers и SDN контролери.

3.3. QoS и приоритизация

Механизмите за **Quality of Service (QoS)** позволяват класифициране на трафика и приоритизиране на критични приложения като VoIP, видео стрийминг или SCADA системи.
Протоколи, като **DSCP (Differentiated Services Code Point)** и **CoS (Class of Service),** задават различни нива на приоритет, а рутерите обработват пакетите според тяхната важност.
В комбинация с NetFlow и Zabbix, администраторите могат в реално време да променят политики според наблюдаваните натоварвания.

4. Архитектури и инструменти за мониторинг на трафика в реално време

4.1. Архитектури за анализ

Модерните системи за мониторинг интегрират edge устройства, облачни решения и централизиран контрол. Архитектура включва четири слоя:

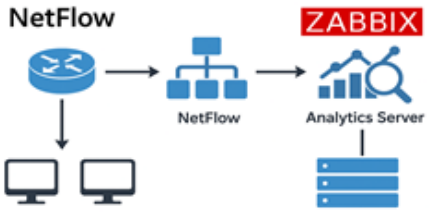
1. **Сензорен слой** – мрежови сонди и NetFlow агенти, разположени близо до източниците на трафик;
2. **Аналитичен слой** – сървъри, които обработват потоците в реално време (Apache Kafka, Flink);
3. **Контролен слой** – SDN контролер, който взема решения за пренасочване или ограничаване на трафика;
4. **Визуализационен слой** – Zabbix или ELK Stack за наблюдение и аларми.

4.2. Инструменти за наблюдение

Инструмент	Функционалност	Предимства
Wireshark	Подробен пакетен анализ	Безплатен, графичен интерфейс
nTopng	Поточен анализ и статистика	Работа в реално време, API интеграция
Zabbix / Prometheus	Централизиран мониторинг	Аларми, разширяемост, мащабируемост
Elastic Stack (ELK)	Анализ на логове и потоци	Висока гъвкавост и визуализация

Тази комбинация от инструменти покрива както детайлния анализ на пакети, така и статистическия мониторинг на инфраструктурно ниво.

5. Казус: Анализ и оптимизация трафика в мрежа на интернет доставчик



***Фиг. 1**. Схема на опитна постановка за анализ на трафика в реално време*

В рамките на средно голяма мрежа на Интернет доставчик в Община Трявна със 700 активни клиенти беше проведено изследване на реалновременния трафик чрез **NetFlow** и **Zabbix**. На фиг.1 е показана схемата на опитната постановка за анализиране на мрежовия трафик в реално време.

При направеното изследване резултатите показаха че:

- 35% от трафика е генериран от видеоконферентни приложения (Zoom, Teams);
- 20% — от облачни услуги (OneDrive, Google Drive);
- 15% — от уеб трафик.

След внедряване на QoS политика и механизми за балансиране на натоварването, средната латентност спадна с 27%, а загубата на пакети – с 19%.
В допълнение, Zabbix таблата за мониторинг визуализираха натоварването на интерфейсите в реално време, което позволи прецизно настройване на лимити и автоматично известяване при надвишаване на праговете.

6. Бъдещи тенденции и предизвикателства

6.1. Основни предизвикателства

- Експоненциален растеж на обема данни, което изисква оптимизация на съхранението и изчисленията;
- Нарастващ дял на **шифрован трафик (HTTPS, VPN)**, който затруднява дълбокия анализ;
- Спазване на стандарти за **сигурност и поверителност** (GDPR, ISO 27001);
- Необходимост от интеграция между различни платформи и протоколи.

6.2. Бъдещи направления

- **Интеграция на AIOps** – използване на изкуствен интелект за автоматично откриване и корекция на проблеми;
- **5G и Edge Computing** – локална обработка на трафика с минимална латентност;
- **Zero Trust архитектури** – нов модел на сигурност с динамично удостоверяване и микросегментация;
- **Федеративно обучение (Federated Learning)** – обучение на ML модели без централно съхранение на чувствителни данни.

ЗАКЛЮЧЕНИЕ

Анализът и оптимизацията на мрежовия трафик в реално време са критични аспекти от съвременните ИТ инфраструктури. Чрез комбиниране на традиционни методи за мониторинг с интелигентни алгоритми и автоматизация е възможно да се постигне висока ефективност, надеждност и сигурност на комуникационните системи.

В бъдеще, с навлизането на AI-базирани решения и самообучаващи се мрежи, управлението на трафика ще се превърне в напълно динамичен и адаптивен процес, способен да реагира мигновено на промените в мрежовата среда.

Благодарности:

Докладът се публикува във връзка с резултатите от изпълнение на дейностите по проект

№ НИП2025-17/2025. „Разработка и изследване на интелигентни методи за мониторинг и управление на IoT/5G- базирани комуникационни платформи и приложения“ към УЦНИТ при ТУ – Габрово.

ЛИТЕРАТУРА

[1] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[2] B. Claise, B. Trammell, and P. Aitken, “Specification of the IP Flow Information Export (IPFIX) Protocol,” RFC 7011, IETF, Sept. 2013.

[3] B. Claise, “Cisco Systems NetFlow Services Export Version 9,” RFC 3954, IETF, Oct. 2004.

[4] P. Phaal, S. Panchen, and N. McKee, “InMon sFlow Version 5,” sFlow.org, 2001 (rev. 2004).

[5] T. Auld, A. W. Moore, and S. F. Gull, “Bayesian Neural Networks for Internet Traffic Classification,” *IEEE Transactions on Neural Networks*, vol. 18, no. 1, pp. 223–239, Jan. 2007.

[6] A. W. Moore and K. Papagiannaki, “Toward the Accurate Identification of Network Applications,” in *Proc. Passive and Active Measurement (PAM)*, 2005, pp. 41–54.

[7] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools*. Springer, 2017.

[8] L. Deri and S. Mainardi, “ntopng: Next Generation Network Traffic Monitoring,” ntop.org White Paper, 2013.

[9] Zabbix SIA, *Zabbix 6.0 LTS Documentation*. Riga: Zabbix, 2024.

[10] The Apache Software Foundation, *Apache Flink Documentation (v1.18)*, ASF, 2024.