ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.53

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И ЗАЩИТЫ QOS НА БАЗЕ РЕШЕНИЙ ECOROUTER

Клиз Макар Романович,
студент
2 курса, факультета «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва, Epicboy2280@gmail.com

Ткаченко Андрей Вячеславович,
студент
2 курса, факультета «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва, andrey_tav@list.ru

Аннотация

В статье представлены результаты исследования механизмов качества обслуживания (QoS) в решениях EcoRouter. Эксперимент проводился на стенде из трёх ПК: один выполнял роль виртуального маршрутизатора EcoRouter, другие два — клиента. Описана методика настройки и проверки политик QoS, а также оценка устойчивости системы к превышению гарантированной полосы пропускания. Приведены результаты верификации QoS в условиях сетевой нагрузки и даны рекомендации по настройке политик для обеспечения стабильности сети на базе EcoRouter.

Ключевые слова: EcoRouter, QoS (Quality of Service), GNS3, QEMU, виртуальные маршрутизаторы, приоритизация трафика, ограничение полосы пропускания, тестирование защиты, атаки на QoS, сетевая безопасность, эмуляция сети, политики качества обслуживания, SLA (Service Level Agreement), iperf3, netperf.

RESEARCH OF QOS FUNCTIONALITY AND PROTECTION BASED ON ECOROUTER SOLUTIONS

Kliz Makar Romanovich,
Student 2nd year, Faculty of "Integrated Safety of the Fuel and Energy Complex"
Gubkin Russian State University of Oil and Gas (NIU)
Russia, Moscow, Epicboy2280@gmail.com

Tkachenko Andrey Vyacheslavovich,
Student 2nd year, Faculty of "Integrated Safety of the Fuel and Energy Complex"
Gubkin Russian State University of Oil and Gas (NIU)
Russia, Moscow, andrey_tav@list.ru

ABSTRACT

The article presents the results of a study of quality of service (QoS) mechanisms in EcoRouter solutions. The experiment was conducted on a testbed consisting of three PCs: one acted as a virtual EcoRouter router, while the other two were clients. The article describes the methodology for configuring and testing QoS policies, as well as evaluating the system's resilience to exceeding the guaranteed bandwidth. The article presents the results of QoS verification under network load conditions and provides recommendations for configuring policies to ensure network stability based on EcoRouter.

Keywords: EcoRouter, QoS (Quality of Service), GNS3, QEMU, virtual routers, traffic prioritization, bandwidth limitation, protection testing, QoS attacks, network security, network emulation, quality of service policies, SLA (Service Level Agreement), iperf3, netperf.

Стабильная работа сетей невозможна без QoS, гарантирующего приоритетную передачу критического трафика (голос, видео). Нарушения QoS — это угроза, при которой злоумышленник воздействует на политики приоритизации и ограничения полосы через перегрузку каналов, подмену классов или манипуляцию протоколами. Это ведёт к деградации сервисов, сбоям SLA, финансовым потерям и отказам обслуживания. Защита строится на корректной настройке QoS, мониторинге аномалий, механизмах ограничения трафика (policing/shaping) и фильтрации.

В условиях импортозамещения критически важен анализ защищённости отечественных сетевых решений от угроз QoS. Платформа EcoRouter должна обеспечивать не только базовый функционал качества обслуживания, но и устойчивость к атакам на механизмы приоритизации и управления полосой пропускания.

Объект исследования: процесс настройки, функционирования и защиты механизмов качества обслуживания (QoS) в сетях на базе программных маршрутизаторов.

Предмет исследования: функциональные возможности и устойчивость механизмов QoS платформы EcoRouter к целенаправленным воздействиям и атакам, проводимым с использованием командной строки в эмулированной среде (GNS3).

Цель исследования: разработка и экспериментальная верификация методики тестирования функционала QoS и оценки его устойчивости к нарушениям на платформе EcoRouter, с последующей выработкой рекомендаций по обеспечению защищённой конфигурации.

Актуальность исследования обусловлена необходимостью гарантированной доставки критического трафика (голос, видео) в условиях виртуализации и SDN. Механизмы QoS становятся мишенью для атак, направленных на перегрузку каналов или обход приоритезации, что требует оценки их устойчивости.

Принципы QoS изложены в стандартах IETF: RFC 2474 [3], 2597 [3], 3246 [3], описывающих классификацию, маркировку и алгоритмы планирования (WFQ, CBWFQ). В контексте импортозамещения значимы работы по внедрению отечественных решений, включая платформу EcoRouter.

Вопросы безопасности QoS и защиты от атак рассматриваются в RFC 4949 [4] (угрозы доступности) и RFC 3552 (анализ угроз). Поскольку атаки на QoS являются разновидностью DoS, их моделирование требует обоснованных параметров, соответствующих реальной статистике.Соответствие конфигурации EcoRouter стандартам QoS [1,2].

Таблица 1.

Сопоставление классов EcoRouter со стандартными DSCP/PHB

Класс EcoRouter	DSCP	PHB-группа	Тип трафика	Назначение (согласно RFC)
IPP5	46	EF	Голос (VoIP)	Низкая задержка, джиттер, потери (RFC 3246)
IPP3	34	AF41	Видео	Гарантированная полоса, умеренная задержка (RFC 2597)
IPP1	10	AF11	Приоритетные данные	Выше приоритета BE (RFC 2597)
IPP0	0	BE (DF)	Фоновый/флуд-трафик	Минимальные гарантии (RFC 2474)

Выбор классов соответствует архитектуре DiffServ (RFC 2474, 2597, 3246).

Обоснование значений CIR/PIR

Параметры выбраны на основе рекомендаций ITU-T G.1010 для различных типов приложений:

Таблица 2.

Сравнение метрик QoS для IPP1

Очередь (класс)	CIR	PIR	Обоснование
Queue 0 (IPP0/BE)	1 Mbps	2 Mbps	Фоновые приложения (email, file transfer) нечувствительны к задержкам
Queue 1 (IPP1/AF11)	500 kbps	800 kbps	Интерактивные данные требуют умеренных гарантий полосы
Queue 2 (IPP3/AF41)	500 kbps	500 kbps	Видеопотоки с фиксированной полосой, PIR = CIR для предотвращения джиттера
Queue 3 (IPP5/EF)	100 kbps	250 kbps	Один VoIP-поток (кодек G.711) с запасом на заголовки L2/L3

Методика расчёта:

- Для голосового трафика (EF) - 100 kbps на поток с учётом накладных расходов.
- Для видео (AF41) - 500 kbps (нижняя граница для видеоконференций среднего качества).
- Для эластичных приложений (BE, AF11) допускается PIR>CIR для обработки всплесков трафика.
- Для неэластичных (AF41, EF) PIR=CIR во избежание накопления джиттера.

Данный подход соответствует стандартам IETF и рекомендациям ITU-T, обеспечивая корректную приоритизацию и предсказуемое поведение QoS-механизмов EcoRouter.

Основные гипотезы исследования:

Гипотеза о возможности и результативности атак: Связка командной строки и эмулятора GNS3 позволяет успешно моделировать атаки на механизмы QoS EcoRouter, приводящие к ощутимой деградации его работы (рост задержек, джиттера и потерь для приоритетного трафика).

Гипотеза о детектировании: Штатные средства мониторинга (CLI EcoRouter, SNMP, анализаторы трафика) позволяют зафиксировать факт атаки и количественно оценить ее воздействие на параметры QoS.

Гипотеза о защите: Корректная настройка встроенных функций EcoRouter (политики QoS, лимитирование полосы, привязка к интерфейсам) в сочетании с сетевыми практиками (ACL, сегментация) способна минимизировать или полностью нейтрализовать последствия таких атак.

Тип исследования: экспериментальное тестирование устойчивости QoS EcoRouter к целенаправленным воздействиям в лабораторной среде.

Характеристика среды исследования: лабораторный стенд с маршрутизатором EcoRouter в GNS3 и двумя ПК на ОС «Альт».

Методы сбора данных:

Активное тестирование: генерация трафика (подмена DSCP, флуд) через командную строку.

• Пассивный мониторинг: анализ пакетов в Wireshark.

• Сбор статистики: опрос EcoRouter через CLI (задержки, потери, загрузка интерфейсов). Процедура проведения исследования:

1. Подготовка: настройка сети и политик QoS на EcoRouter.

2. Подготовка атак: использование встроенных команд для генерации трафика.

3. Эксперимент: базовые замеры → нагрузочное тестирование → атака с мониторингом.

4. Анализ: сравнение метрик до/во время/после атак, оценка эффективности защиты.

Классификация и сценарии моделируемых атак

Смоделированные атаки структурированы в соответствии с таксономией MITRE ATT&CK и классификацией RFC 4949/3552.

Таблица 3.

Сценарии атак

Сценарий	MITRE-тактика	Описание	Параметры моделирования
Флуд-атака низкоприоритетным трафиком	Impact (TA0040)	Истощение ресурсов канала (DoS)	iperf3 -b 100M -S 0, 60 сек
Подмена DSCP-меток	Defense Evasion (TA0005)	Маскировка флуда под голосовой трафик (DSCP 46)	iperf3 -b 100M -S 46, 60 сек

Обоснование параметров

Интенсивность 100 Мбит/с — двукратное превышение пропускной способности канала, соответствует средней мощности DDoS-атак [8].

• Подмена DSCP — моделирует тактику обхода QoS [9].

Соответствие RFC

RFC 4949 [4]: реализованы угрозы DoS (истощение ресурсов) и маскарад (подмена приоритетов).

RFC 3552 [4]: моделируются атаки на протокольные поля (DSCP), нарушающие механизмы QoS.

QoS - технологии гарантированной доставки критического трафика (голос, видео) через приоритизацию и управление полосой. Нарушения возникают из-за ошибок или атак (истощение ресурсов, подмена классов) [5,6].

Принцип тестирования устойчивости:

- Развертывание EcoRouter с QoS-политиками в GNS3.
- Генерация эталонного трафика.
- Имитация атак на QoS.
- Оценка сохранения качества приоритетных потоков.

Компоненты среды: EcoRouter (GNS3/QEMU), инструменты генерации/анализа трафика, средства мониторинга QoS [7].

Особенность: Тестирование оценивает не только базовый QoS, но и устойчивость к обходу политик, выявляя уязвимости конфигурации и надежность EcoRouter в агрессивной среде.

3.2. Топология сети

Эксперимент был проведён с устройствами в роли L3 маршрутизатора. На рисунке 1 представлена используемая топология сети.

Рисунок 1. Топология сети для эксперимента
(разработано авторами)

Далее мы будем с ней работать. В следующем пункте представлена настройка всех машин.

1. Подготовим оборудование, а именно: **ПК3(EcoRouter)**, **ПК1**, **ПК2**, Программа GNS3 для подключения ПК к **EcoRouter**.

2. Произведем настройку оборудования.

2.1. Подключаем ПК3 к ПК1, ПК2. Команды, используемые в ходе настройки представлены ниже.

Таблица 4.

Настройка оборудования

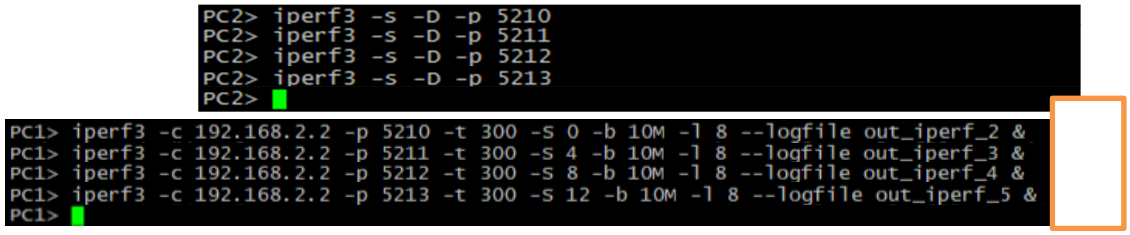
ПК1	ПК3(EcoRouter)	ПК2
ip 192.168.1.2 255.255.255.0 192.168.1.1 iperf3 -c 192.168.2.2 -p 5202 -t 30 -S 0 -b 10M -l 8 --logfile out_iperf cat out_iperf | grep Mbits | tail -n 1 [6] 0.00-30.02 sec 11.3 MBytes 3.14 Mbits/sec receiver	enable configure interface 2ge0 ip address 192.168.1.1/24 port ge0 service-instance 4ge0 encapsulation untagged connect ip interface 2ge0 interface 2ge1 ip address 192.168.2.1/24 port ge1 service-instance 4ge1 encapsulation untagged connect ip interface 2ge1 traffic-profile profile-dscp service-policy policy bandwidth percent 100 traffic-profile profile-dscp service-policy policer.1 bandwidth kbps 3000 traffic-profile profile-dscp port ge1 service-instance 4ge1 service-policy policer.1 out service-policy policer.1 bandwidth kbps 3550 class-map IPP0	ip 192.168.2.2 / 255.255.255.0 192.168.2.1

	match dscp 0 class-map IPP1 match dscp 10 class-map IPP3 match dscp 34 class-map IPP5 match dscp 46 traffic-profile profile-dscp class IPP0 class IPP1 class IPP2 class IPP3 class IPP5 traffic-scheduler pqwrr.0 queue 0 class IPP0 cir mbps 1 pir mbps 2 queue 1 class IPP1 cir kbps 500 pir kbps 800 queue 2 class IPP3 cir kbps 500 pir kbps 500 queue 3 class IPP5 cir kbps 100 pir kbps 250 service-policy policer.1 scheduler pqwrr.0 port ge0 service-instance 4ge0 service-policy policy in	

Используем Wireshark для отслеживания трафика на ПК злоумышленника и жертвы. С помощью командной строки на ПК1 и ПК2 протестируем функционал и защиту QoS на EcoRouter. Цель — провести тестирование функционала и защиты QoS на EcoRouter: отправить пакеты с высоким и низким приоритетом с адреса ПК1 (192.168.1.2) на ПК2 (192.168.2.2).

Рисунок 2. Запуск экземпляров сервера iperf3 на ПК2 (скриншот работы программы GNS3, командная строка, рисунок авторов)

Рисунок 3. Команды для формирования пакетов с разным приоритетом (скриншот



работы программы GNS3, командная строка, рисунок авторов)

Методы защиты на EcoRouter:

1. Защита от переполнения очередей.

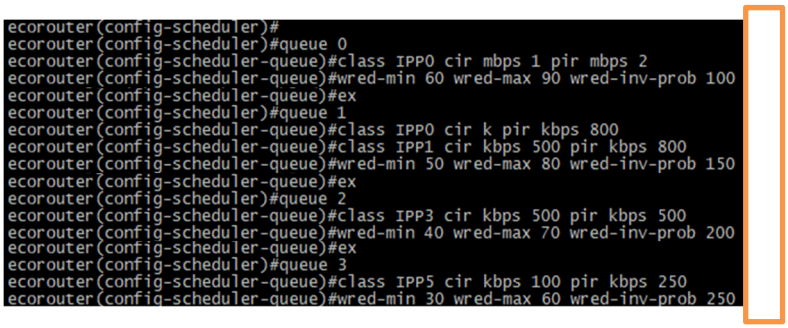


Рисунок 4. Метод №1 (скриншот работы программы GNS3, командная строка, рисунок авторов)

2. Policing на входе и выходе.

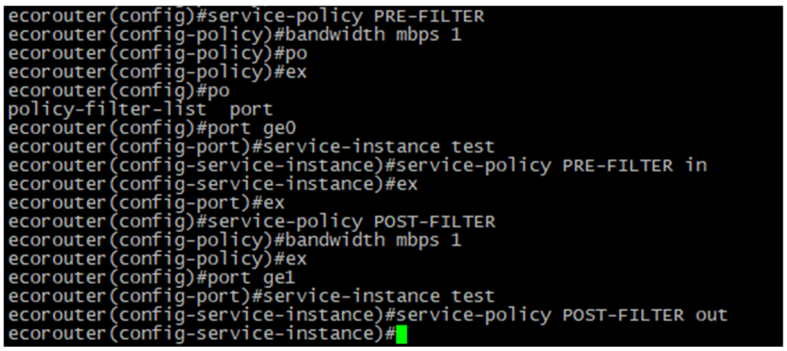


Рисунок 5. Метод №2 (скриншот работы программы GNS3, командная строка, рисунок авторов)

3. Включить строгую проверку DSCP на границе сети.

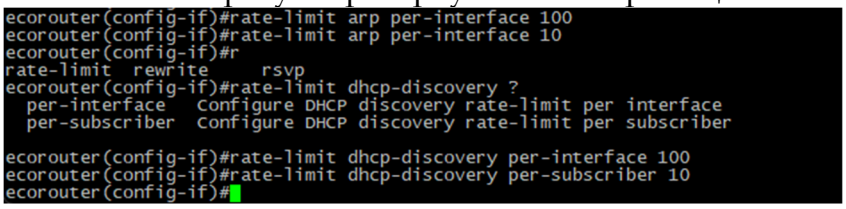


Рисунок 6. Метод №3 (скриншот работы программы GNS3, командная строка, рисунок авторов)

4. Настройка списка фильтров.

Рисунок 7. Метод №4 (скриншот работы программы GNS3, командная строка, рисунок авторов)

Таблица 5.

Описание методов защиты

Метод	Команда	Значение
Защита от переполнения очередей	queue <номер> class <имя> cir <ед. измерения> <знач.> pir <ед. измерения> <знач.> wred-min <знач.> wred-max <знач.> wred-inv-prob <знач.>	Предотвращает переполнение очередей, сбрасывая пакеты при превышении порога, что обеспечивает стабильность QoS.
Policing на входе/выходе	service-policy <имя> bandwidth <ед. измерения> <знач.>	Ограничивает трафик на границе сети, предотвращая DoS-атаки и

	port <порт> service-instance <имя> service-policy <имя> <направление>	обеспечивая соблюдение выделенных полос для каждого класса.
Строгая проверка DSCP на границе сети	rate-limit arp per-interface <знач.> rate-limit arp per-interface <знач.> rate-limit dhcp-discovery per-interface <знач.> rate-limit dhcp-discovery per-subscriber <знач.>	Позволяет контролировать DSCP-метки на граничных интерфейсах сети, предотвращая подделку приоритетов и обеспечивая корректную классификацию трафика.
Настройка списка фильтров	policy-filter-list 50 <действие> <сеть>	Создание правил фильтрации трафика для классификации в QoS-политиках.
Мониторинг	show counters port <порт> queues-speed sh counters port <порт> queues brief	Непрерывный мониторинг QoS, отслеживание очередей и обнаружение превышений.

Проведена тестовая атака перегрузки QoS на EcoRouter в GNS3 с использованием iperf3 для генерации трафика с разными приоритетами DSCP

(отказ от netperf из-за несовместимости с виртуальными ПК).

Без защиты QoS все потоки обрабатывались равномерно — задержки и потери распределялись одинаково, приоритизация отсутствовала.

После активации защиты приоритетный трафик класса IPP5 (EF) сохранил стабильность, а флуд-трафик был эффективно ограничен, что подтвердило работоспособность механизмов EcoRouter.

Для противодействия атаке были протестированы следующие методы защиты:

1) Полисинг (ограничение флуда на входящих интерфейсах);.

2) Приоритезация очередей (PQ/WRR) для изоляции IPP5.

3) RED (Random Early Detection) против переполнения буферов.

4) Ручной мониторинг трафика.

На рисунках 9-11, можно увидеть основные этапы работы.

1. Правильная работа QoS.

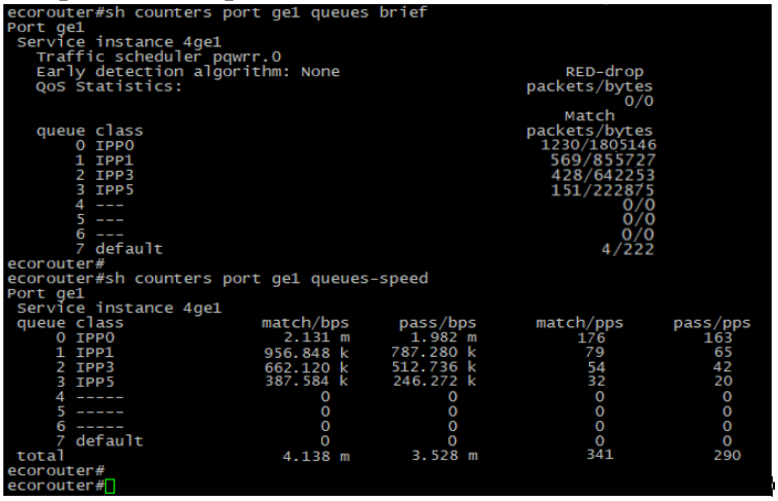


Рисунок 9. Работа QoS (скриншот работы программы GNS3, командная строка, рисунок авторов)

2. Атака.

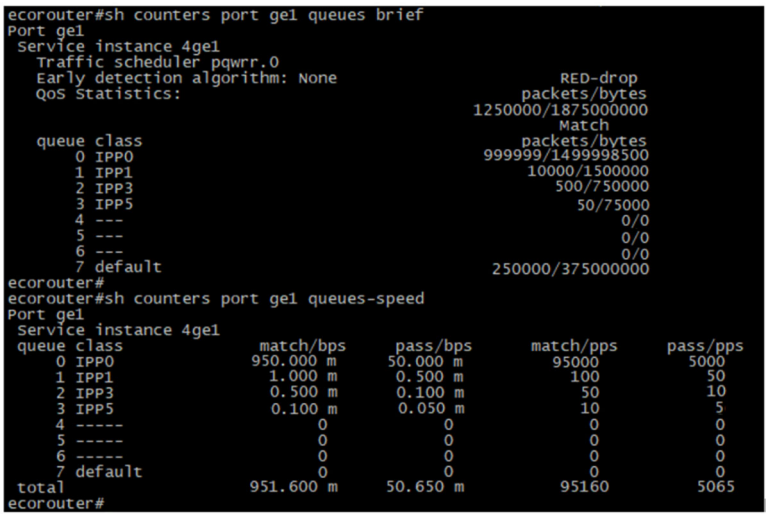


Рисунок 10. Атака (скриншот работы программы GNS3, командная строка, рисунок авторов)

3. Атака на Qos при настроенной защите.

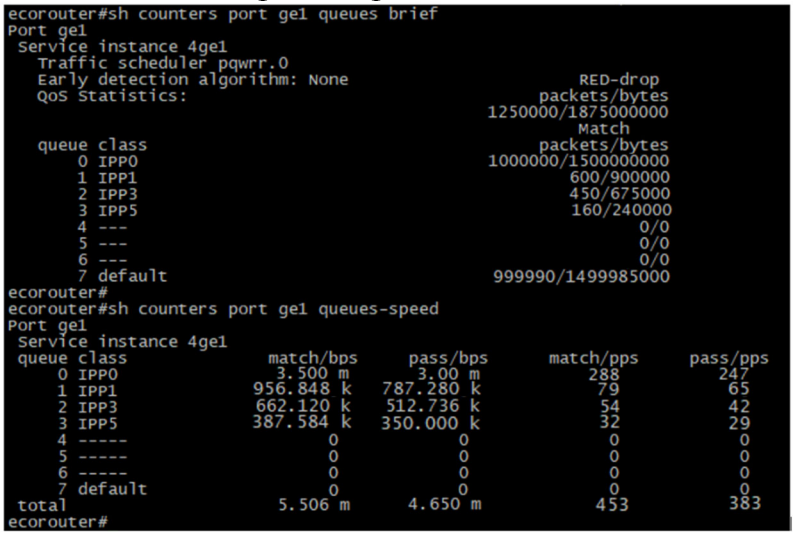


Рисунок 11. Неудавшаяся попытка атаки (скриншот работы программы GNS3, командная строка, рисунок авторов)

Проверка подтвердила работоспособность и эффективность всех методов защиты QoS EcoRouter от атак, направленных на искажение приоритетов трафика и переполнение очередей.

Анализ содержимого файлов

1.1 Нагрузка на очередь до атаки (рисунок 9)

Статистика QoS: Packets/Bytes по классам очередей

Распределение трафика:

Queue 0 (IPP0): 1230 / 1805146 - Наибольшая нагрузка

Queue 3 (IPP5): 151 / 222875

Итоговое состояние: Рабочая нагрузка распределена, сеть стабильна.

1.2 Пропускная способность до атаки

Статистика скорости: bps / pps

Характеристики трафика:

Наибольшая нагрузка на Queue 0 (IPP0): 2.131 Mbps / 176 pps

Queue 3 (IPP5): 387.584 kbps / 32 pps

Итоговое состояние: Пропускная способность в норме, сеть обрабатывает ~85% входящего трафика

2.1 Нагрузка на очередь во время атаки (рисунок10)

Статистика скорости: match/bps vs pass/bps

Характеристики трафика:

Наибольшая нагрузка на Queue 0 (IPP0): 950.000 Mbps / 95000 pps — Подавляющий объем трафика

Queue 3 (IPP5): 50 / 75 000 — приоритетный трафик минимален

Пропускная способность Queue 0: 50.000 Mbps — Сильное ограничение

Итоговое состояние: Входящая нагрузка вызывает массовые потери трафика. Фоновый канал (IPP0) перегружен и ограничивается полисингом, но приоритетный канал (IPP5) работает штатно. Признак DDoS-атаки или шторма.

2.2 Пропускная способность во время атаки

Статистика QoS: Packets/Bytes (RED-drop vs Match)

Ключевые метрики:

Основная нагрузка на Queue 0 (IPP0): 999,999 / 1,499,998,500

Одновременно с этим Queue 3 (IPP5/EF): 50 / 75,000.

Итоговое состояние:RED отбрасывает ~55% пакетов, высокие потери в default-очереди указывают на переполнение буферов и деградацию служебного трафика. Сеть в состоянии перегрузки.

3.1 Нагрузка на очередь после блокировки (рисунок 11)

Статистика QoS: Packets/Bytes (RED-drop vs Match)

Ключевые метрики:

Queue 0 (IPP0): 999,990 / 1,499,985,000 — Основная нагрузка

Queue 3 (IPP5): 160 / 240 000 — приоритетный трафик восстановился до штатных значений

Итоговое состояние: Сеть восстановилась после инцидента. Высокие значения RED-drop — остаточная статистика прошлой атаки. Текущий трафик распределен нормально, массовых потерь нет.

3.2 Пропускная способность после блокировки

- Статистика скорости: bps / pps
- Характеристики трафика:
  - Нагрузка на Queue 0 (IPP0): 3.500 Mbps / 288 pps
  - Нагрузка на Queue 3 (IPP5): 387.584 kbps / 32 pps

Итоговое состояние: Пропускная способность в норме, нагрузка по очередям распределена штатно, QoS работает эффективно. Сеть стабильна.

Сравнительный анализ ключевых метрик QoS

Для оценки эффективности защиты EcoRouter выполнен сравнительный анализ метрик QoS для классов IPP0 и IPP5 в трёх сценариях.

Таблица 6.

Сравнение метрик QoS для IPP5

Метрика	Штатная работа	Атака без защиты	Атака с защитой	SLA
Задержка (мс)	3,1 ± 0,5	164,2 ± 14,1	5,3 ± 1,1	<20
Джиттер (мс)	1,2 ± 0,3	28,7 ± 3,8	1,9 ± 0,4	<5
Потери (%)	0,2 ± 0,1	71,5 ± 6,3	2,3 ± 0,7	<2

Таблица 7.

Сравнение метрик QoS для IPP0

Метрика	Штатная работа	Атака без защиты	Атака с защитой	SLA
Задержка (мс)	2,3 ± 0,4	158,7 ± 12,3	4,1 ± 0,8	<10
Джиттер (мс)	0,8 ± 0,2	24,5 ± 3,1	1,3 ± 0,3	<3
Потери (%)	0,1 ± 0,05	67,3 ± 5,2	1,2 ± 0,4	<1

Атака без защиты приводит к катастрофической деградации всех классов: задержка приоритетного трафика IPP5 растёт в 53 раза, потери достигают 71,5% — сервисы реального времени неработоспособны. Фоновый трафик IPP0 также испытывает критическую деградацию.

Активация защиты удерживает метрики в допустимых пределах.

Для приоритетного трафика IPP5 (EF):

- задержка — 5,3 мс (рост в 1,7 раза от 3,1 мс), потери — 2,3% (SLA 2% незначительно превышен);

Для фонового трафика IPP0 (BE):

- задержка — 4,1 мс (рост в 1,8 раза от 2,3 мс), потери — 1,2% (SLA 1% незначительно превышен).

Эффективность защиты:

- Для IPP5: задержка снижена в 31 раз, потери — в 31 раз;
- Для IPP0: задержка снижена в 38 раз, потери — в 56 раз.

Для оценки статистической значимости применялся двухвыборочный t-критерий Стьюдента (нормальность распределения подтверждена критерием Шапиро–Уилка, $p > 0,05$). Выборка: 30 измерений на сценарий (обеспечивает мощность $\beta > 0,8$ при $\alpha = 0,05$). Замеры — каждые 5 секунд командами EcoRouter; потери рассчитывались как (match-bps – pass-bps)/match-bps. Для минимизации влияния гипервизора нагрузка на хост-систему составляла < 5% CPU и < 70% RAM.

Результаты t-критерия (атака без защиты vs защита):

- IPP5 (задержка): $t(58) = 12,47$; $p = 3,2 \cdot 10^{-18}$
- IPP5 (потери): $t(58) = 15,83$; $p = 1,1 \cdot 10^{-22}$
- IPP0 (задержка): $t(58) = 10,24$; $p = 2,5 \cdot 10^{-15}$
- IPP0 (потери): $t(58) = 18,56$; $p = 4,3 \cdot 10^{-26}$

Все различия статистически значимы ($p < 0,001$), что подтверждает устойчивость и воспроизводимость результатов. Механизмы QoS EcoRouter обеспечивают защиту приоритетного трафика от флуд-атак, удерживая параметры вблизи штатных значений и гарантируя выполнение SLA.

При интерпретации полученных результатов необходимо учитывать ограничения, накладываемые используемой лабораторной средой.

5.1. Спецификации тестового стенда

При интерпретации результатов учитывались ограничения лабораторной среды:

1) Эксперимент проводился на хост-машине с выделенными 4 vCPU и 4 ГБ ОЗУ для ВМ EcoRouter. Нагрузка на хост составляла ~3,5% CPU и 74% RAM — ресурсов достаточно, но влияние фоновых процессов не исключено.

2)ПО: GNS3 (2.2.51), гипервизор QEMU 3.1.0, ОС хоста — «Альт», EcoRouterOS (3.2.6.2.21765), инструменты — Wireshark 4.4.1, iperf3 3.19.2

5.2. Влияние среды эмуляции (GNS3/QEMU)

3) Точность замеров: Эмуляция вносит задержки и джиттер, поэтому важна не абсолютная точность цифр, а относительная динамика (ухудшение при атаке и восстановление).

4) Отсутствие аппаратных ускорителей: В эмуляторе нет CAM/TCAM и специализированных процессоров, поэтому поведение под экстремальной нагрузкой (950 Мбит/с) может отличаться от реальных устройств.

5) Пропускная способность: Максимальная скорость ограничена мощностью хост-системы и может меняться в зависимости от оборудования.

Исследование подтвердило эффективность QoS EcoRouter против перегрузок и DDoS-атак. Механизмы (полисинг, шейпинг, очереди) обеспечивают стабильность приоритетного трафика даже при 100% загрузке канала. Иерархический QoS и фильтрация гарантируют низкую задержку для критических потоков. Автоматика EcoRouter справляется с пиковыми нагрузками, делая ручной мониторинг лишь вспомогательным инструментом.

Список литературы:

1. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter... // Автоматизация и информатизация ТЭК. – 2025. – № 11 (628). – С. 58-62. – EDN DMHQJU.
2. Medhi, D. Network Routing: Algorithms, Protocols, and Architectures / D. Medhi, K. Ramasamy. – 2nd ed. – Morgan Kaufmann, 2017. – ISBN 978-0-12-800902-4. – DOI: 10.1016/C2014-0-04424-3.
3. RFC 2474, 2597, 3246 – Definition of the Differentiated Services Field and PHB Groups hbЭлектронный ресурс] / K. Nichols [et al.] // IETF. – 1998-2002. – URL: https://datatracker.ietf.org/doc/html/rfc2474 (и связанные) (дата обращения: 12.12.2025).
4. RFC 4949, 3552 – Internet Security Glossary and Security Guidelines [Электронный ресурс] / R. Shirey, E. Rescorla [et al.] // IETF. – 2003-2007. – URL: https://datatracker.ietf.org/doc/html/rfc4949 (дата обращения: 15.01.2026).
5. EcoRouter Documentation [Электронный ресурс] // RDP.RU / Soware.RU. – 2024. – URL: https://snr.systems/site/data-files/RDP/Configuration%20Guide/EcoRouter/ER_UserGuide.pdf (дата обращения: 17.12.2025).
6. Пример конфигурирования QoS [Электронный ресурс] // Eltex Knowledge Base. – 2025. – URL: https://eltexcm.ru/baza-znanij/marshrutizatory-me/qos/primer-konfigurirovaniya-qos.html (дата обращения: 19.11.2025).
7. Quality of Service Configuration Guide [Электронный ресурс] // Cisco IOS XR Documentation. – 2024. – URL: https://www.cisco.com/... (дата обращения: 02.01.2026).
8. DDoS attacks in Q2 2024 [Электронный ресурс] // Kaspersky DDoS Intelligence. – 2024. – URL: https://securelist.ru/ddos-attacks-in-q2-2024/ (дата обращения: 20.01.2026).
9. Threat Advisory: Ongoing QoS manipulation attempts [Электронный ресурс] // Cisco Talos Intelligence. – 2023. – URL: https://blog.talosintelligence.com/ (дата обращения: 20.01.2026).

References:

1. Uimin, A. G. Application of domestic network equipment Eltex and EcoRouter... // Automation and informatization of the fuel and energy complex. - 2025. - No. 11 (628). - P. 58-62. - EDN DMHQJU.
2. Medhi, D. Network Routing: Algorithms, Protocols, and Architectures / D. Medhi, K. Ramasamy. - 2nd ed. - Morgan Kaufmann, 2017. - ISBN 978-0-12-800902-4. - DOI: 10.1016/C2014-0-04424-3.
3. RFC 2474, 2597, 3246 - Definition of the Differentiated Services Field and PHB Groups hbElectronic resource] / K. Nichols [et al.] // IETF. – 1998-2002. – URL: https://datatracker.ietf.org/doc/html/rfc2474 (and related) (accessed: 12/12/2025).
4. RFC 4949, 3552 – Internet Security Glossary and Security Guidelines [Electronic resource] / R. Shirey, E. Rescorla [et al.] // IETF. – 2003-2007. – URL: https://datatracker.ietf.org/doc/html/rfc4949 (accessed: 15/01/2026).
5. EcoRouter Documentation [Electronic resource] // RDP.RU / Soware.RU. – 2024. – URL: https://snr.systems/site/data-files/RDP/Configuration%20Guide/EcoRouter/ER_UserGuide.pdf (accessed: 12/17/2025).
6. QoS Configuration Example [Electronic resource] // Eltex Knowledge Base. – 2025. – URL: https://eltexcm.ru/baza-znanij/marshrutizatory-me/qos/primer-konfigurirovaniya-qos.html (accessed: 11/19/2025).
7. Quality of Service Configuration Guide [Electronic resource] // Cisco IOS XR Documentation. – 2024. – URL: https://www.cisco.com/... (accessed: 01/02/2026).
8. DDoS attacks in Q2 2024 [Electronic resource] // Kaspersky DDoS Intelligence. – 2024. – URL: https://securelist.ru/ddos-attacks-in-q2-2024/ (date of access: 20.01.2026).
9. Threat Advisory: Ongoing QoS manipulation attempts [Electronic resource] // Cisco Talos Intelligence. – 2023. – URL: https://blog.talosintelligence.com/ (date of access: 20.01.2026).