МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МОЭВМ

РЕФЕРАТ

Тема: Обзор предметной области

Студент гр. 4303 _____ Дронников И.М.

Преподаватель _____ Кринкин К.В.

Санкт-Петербург

2019

ВВЕДЕНИЕ

В настоящее время широкое распространение получили сервисы потокового вещания видео в реальном времени. Главная особенность таких сервисов заключается в том, что при потоковом вещании данные пересылаются непрерывным потоком в виде последовательности сжатых пакетов и используются по мере передачи на компьютер получателя.

Поскольку потоковое вещание подразумевает непрерывное получение пользователем данных от сервера, такие сервисы наиболее уязвимы к помехам в интернет-соединении, таким как: задержки и потери пакетов. Для имитации подобных помех и упрощения тестирования производительности протоколов доставки контента в различных условиях необходим инструмент, позволяющий изменять различные параметры производительности или качества обслуживания на действующей сети.

Цель данной работы состоит в реализации инструмента, позволяющего проводить шейпинг сетевого трафика для исследования производительности сетевых протоколов доставки данных.

Для достижения поставленной цели необходимо выполнить следующие **задачи**:

- Определить параметры сети, которые необходимо изменять.
- Произвести поиск инструментов, позволяющих создавать помехи или изменять параметры производительности сети.
- Выполнить сравнительный анализ отобранных кандидатов по указанным критериям.
- Сформировать перечень требований к разрабатываемому инструменту.
- Описать алгоритмы и механизмы работы разрабатываемого инструмента.
- Спроектировать архитектуру разрабатываемого инструмента.

- Разработать собственный инструмент, удовлетворяющий всем указанным критериям.
- Протестировать разработанный инструмент на одном из существующих протоколов.

Объектом исследования является шейпинг сетевого трафика для исследования производительности сетевых протоколов доставки данных.

Предметом исследования является инструмент, позволяющий проводить шейпинг трафика.

1. ОБЗОР ПРЕДМЕТНОЙ ОБЛАСТИ

1.1. Необходимые критерии

Для тестирования протокола доставки сетевого контента необходим инструмент, позволяющий организовывать в локальной сети те ограничения, которые может испытывать клиент при пользовании сервисом. К подобным ограничениям можно отнести:

- Пропускная способность канала.
- Задержка пакетов и время до получения первого байта (TTFB) — показатель скорости отклика сервера.
- Потери пакетов:
  - Имитация разрыва соединения – потеря определенного количества пакетов, идущих подряд;
  - Имитация дискретных помех в соединении – потеря отдельных пакетов в случайном порядке.
- Реордеринг – ситуация, когда пакеты идут в некорректном порядке относительно порядка отправки.
- Лимит пропускной способности маршрутизатора.

1.2. Обзор существующих средств

С целью детального изучения существующих реализованных подходов к шейпингу и анализу трафика, а также исследования возможных методов реализации подобного функционала был проведен обзор инструментов, решающих данную задачу. Поиск аналогов производился среди программных продуктов, поддерживающих операционную систему Linux. В качестве аналогов рассматривались все инструменты, которые реализуют какой-либо функционал, связанный с контролем и мониторингом трафика в сети. По результатам поиска было найдено 6 приложений. Их описание приведено ниже.

1.2.1. iproute2/tc [1]

tc используется для настройки системы контроля трафика (Traffic Control) ядра Linux. Система контроля трафика состоит из:

- Ограничение исходящего трафика;
- Планирование;
- Ограничение входящего трафика;
- Отбрасывание.

1.2.2. Trickle [2]

Trickle - это шейпер для сети, который позволяет ограничить скорость доступа прикладных программ к интернет-соединению без необходимости накладывания патчей на ядро, каких-либо настроек firewall, либо прав супер-пользователься в системе. Trickle может быть запущен как в режиме взаимодействия, так и в качестве отдельного сервиса. Trickle позволяет ограничивать использование канала как одному, так и группе указанных пользовательских приложений. Работает только с TCP.

1.2.3. Ipband [3]

Ipband – это монитор трафика, основанный на pcap. Позволяет отслеживать соединения в сети и статистику использования трафика, а также, если определенное приложение значительно превышает допустимый предел использования трафика, отправлять отчеты его работы, например, на электронную почту.

1.2.4. Wireshark [4]

Wireshark является анализатором сетевого протокола (или "пакетным сниффером"), который можно использовать для анализа сети, для поиска проблем, возникших в сети, при разработке программ, в процессе обучения и т. п. При помощи Wireshark возможно в реальном времени просматривать и вести учет трафика, собирать информацию обо всех пакетах, проходящих через сетевую карту.

Позволяет просматривать содержимое пакетов по полям, в зависимости от протокола передачи, а также фильтровать и сортировать результаты. Поддерживает экспорт данных в различные файловые форматы.

1.2.5. NeTAMS [5]

NeTAMS (Network Traffic Accounting and Monitoring Software) - многофункциональная программа по учету и управлению IP-трафиком для маршрутизаторов Cisco или компьютеров под управлением Unix (Linux/FreeBSD/Solaris). Имеет возможность проводить блокировку на базе квот, авторизации, исчерпании баланса, а также управлять полосой пропускания и контролировать подмену MAC-адреса.

Поддерживаются различные методы сбора статистики (tee/divert/ip_queue/ulog/libpcap/netflow v5 и v9/netgraph), хранения в базе данных (BerkleyDB/MySQL/PostgresSQL/Oracle/Radius), агрегирования, отображения и оповещения.

1.2.6. Netfiler/iptables [6]

Iptables — это утилита командной строки, которая является стандартным интерфейсом управления работой межсетевого экрана Netfilter для Linux, начиная с версии ядра 2.4. В системе netfilter, пакеты пропускаются через цепочки. Цепочка является упорядоченным списком правил, каждое правило может содержать критерии и действие или переход. Когда пакет проходит через цепочку, система netfilter по очереди проверяет, соответствует ли пакет всем критериям очередного правила, и если так, то выполняет действие (если критериев в правиле нет, то действие выполняется для всех пакетов, проходящих через правило). Стандартные действия доступные во всех цепочках — ACCEPT (пропустить), DROP (удалить), QUEUE (передать на анализ внешней программе), и RETURN (вернуть на анализ в предыдущую цепочку). Для использования утилиты Iptables требуются привилегии суперпользователя (root).

1.3. Анализ проблем существующих инструментов

В целях унификации оценки и сравнения представленных аналогов сформирован следующий набор критериев. Данные критерии основаны на вышеприведенном описании ожидаемого инструмента и позволяют выявить проблемы исследуемых аналогов в рамках задачи шейпинга и анализа трафика.

Критерии:

- Возможность ограничения пропускной способности канала;
- Возможность организации потери пакетов;
- Возможность организации задержки пакетов;
- Возможность отслеживания статистики объема проходящего трафика и/или количества пакетов.

Краткие результаты изучения аналогов приведены в Таблице 1.

Таблица 1 – Сравнение аналогов

	Ограничение пропускной способности	Потери пакетов		Задержки пакетов	Сбор статистики трафика	Реордеринг
		Блоками	Случайные			
tc	+	-	+	+	-	+
Trickle	+	-	-	-	+	-
Ipband	-	-	-	-	+	-
Wireshark	-	-	-	-	+	-
NeTAMS	+	-	-	-	+	-
iptables	+	+	+	-	-	-

1.4. Вывод

В результате изучения существующих инструментов можно сделать следующие выводы:

- Среди рассмотренных альтернатив только в четырех инструментах присутствует возможность ограничения пропускной способности соединения. Прочие инструменты предназначены исключительно для сбора статистики использования сети.

- Только в двух инструментах присутствует возможность конфигурации потерь пакетов.

Таким образом, несмотря на обширные возможности конфигурации отдельных инструментов, например, iptables или tc, существующие аналоги не позволяют в полной мере достигнуть поставленной цели. Исходя из данного факта, можно сделать вывод о необходимости создания инструмента, удовлетворяющего всем выдвинутым критериям.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] tc [Электронный ресурс]. URL: http://man7.org/linux/man-pages/man8/tc.8.html (дата обращения: 10.12.2019).

[2] Tricle [Электронный ресурс]. URL: http://manpages.ubuntu.com/manpages/bionic/man1/trickle.1.html (дата обращения: 10.12.2019).

[3] ipband [Электронный ресурс]. URL: http://manpages.ubuntu.com/manpages/cosmic/man8/ipband.8.html (дата обращения: 10.12.2019).

[4] Wireshark [Электронный ресурс]. URL: https://www.wireshark.org/ (дата обращения: 10.12.2019).

[5] Netams [Электронный ресурс]. URL: http://www.netams.com/ (дата обращения: 10.12.2019).

[6] Iptables [Электронный ресурс]. URL: https://www.netfilter.org/ (дата обращения: 10.12.2019).