

ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕХАНИЗМОВ ФОРМИРОВАНИЯ И ОГРАНИЧЕНИЯ ТРАФИКА

В статье рассмотрены некоторые практические аспекты применения формирования и ограничения трафика – технологии качества обслуживания в телекоммуникационных сетях.

The article discusses some practical aspects of the traffic shaping and policing - Quality of Service technology in telecommunication networks.

Направление и цель работы

Поводом для данной статьи послужило проведение тренингов по управлению трафиком в конвергентных сетях, где возникла необходимость проиллюстрировать действие тех или иных механизмов QoS (Quality of Service, качество обслуживания) статистическими характеристиками трафика. Суть качества обслуживания – в обеспечении требуемых характеристик сервиса (как правило, задержки, джиттера и потерь) для определенных классов трафика. Стратегии обеспечения QoS направлены на управление перегрузками (очередями) и предотвращение перегрузок (контроль за установлением соединений, профилирование трафика и управление скоростью передачи). Фундаментальные исследования на данную тему приведены, например, в [1,2].

В ранее опубликованной статье [3] были исследованы механизмы управления очередями. В этой статье исследуем механизмы управления интенсивностью трафика. В данном контексте под управлением интенсивностью трафика будем понимать принудительное воздействие на трафик с целью соответствия потока пакетов заданному скоростному профилю. Различают два механизма управления интенсивностью трафика: формирование трафика (traffic shaping, TS) и ограничение трафика (traffic policing, TP). Мотив использования этих механизмов – создание предсказуемого потока трафика или ограничение скорости передачи.

Цель данной работы состоит в исследовании влияния механизмов управления трафиком (формирования и ограничения) и параметров их настройки на характеристики обслуживания.

Формирование трафика

Формирование трафика ограничивает скорость передаваемых пакетов путем временного удержания некоторых пакетов в очереди. Т.е. пакеты, передача которых отложена, задерживаются в очереди. Как результат, скорость передачи пакетов не будет превосходить заданную величину.

Реализация механизмов управления интенсивностью трафика основана на алгоритме маркерного ведра (token bucket). Легенда гласит, что есть ведро заданной емкости, которое периодически пополняется определенным количеством маркеров, а при передаче пакета некоторого размера соответствующее количество маркеров удаляется из ведра. При этом ведро не может вместить больше заданного количества маркеров, т.е. избыточные маркеры попросту «сливаются».

Другими словами, если в ведре достаточно маркеров для передачи пакета — он передается, а соответствующее количество маркеров удаляется из ведра. В ином случае пакет задерживается в очереди до тех пор, пока в ведре не будет достаточно маркеров для его передачи (или же очередь достигнет предела и излишние пакеты будут сброшены).

При настройке формирования трафика, как правило, задаются три величины: согласованная скорость передачи (CIR, Committed Information Rate), согласованный выброс (Bc, Burst Committed) и избыточный выброс (Be, Burst Excess). Время, в течение которого может быть передано количество трафика, соответствующее Bc, равно Bc/CIR и обозначается как Tc. Tc это и есть временной интервал, через который ведро маркеров пополняется на Bc маркеров. Как правило, в оборудовании используются значения Tc от 10 до 125 мс.

Если задано значение избыточного выброса

(Be), то максимальное количество маркеров в ведре может достигать $Vc+Be$. Когда в конце предыдущего Tc интервала осталось некоторое количество маркеров, то к ним в начале следующего интервала добавляются Vc маркеров. В частности, после Tc интервала не активности за следующий интервал может быть передано $Vc+Be$ трафика. Следует добавить, что формирование трафика может быть применено только к исходящему трафику интерфейса или субинтерфейса.

Ограничение трафика

Ограничение трафика, в отличие от формирования, не откладывает передачу пакета. Реализация механизма ограничения трафика также основывается на алгоритме маркерного ведра. Механизм ограничения трафика отличается от формирования трафика поведением при исчерпании маркеров. В одном варианте настройки, если для передачи пакета достаточно маркеров — он передается. Если используются избыточные маркеры (Be), то к пакету применяется действие1. В ином случае (отсутствие маркеров) — применяется действие2. «Действием» может быть передача пакета, сброс пакета или изменение метки пакета. Заметим, что формирование трафика не предполагает перемаркировку пакетов.

Другой вариант настройки ограничения трафика предполагает использование двукратного алгоритма маркерного ведра. Первое «ведро», как и в предыдущих случаях, контролирует среднюю скорость (CIR), а второе — пиковую скорость (PIR, Peak Information Rate). Первое ведро, как и ранее, пополняется на Vc маркеров в начале каждого интервала Tc , а второе, соответственно, на Be . Если для передачи пакетов хватает маркеров из ведра CIR — они используются и пакет передается далее. Иначе, если достаточно маркеров в ведре PIR, маркеры используются и к пакету применяется действие1. В ином случае (отсутствует достаточное количество маркеров) — к пакету применяется действие2. «Действием», аналогично, может быть передача пакета, сброс пакета или изменение метки пакета.

Таким образом, механизм ограничения трафика позволяет ограничивать скорость пакетов и удалять избыточное количество пакетов или изменять их принадлежность к некоторому классу трафика (деклассируя их,

путем установления метки принадлежности к менее приоритетному классу).

Ограничение трафика может применяться как к исходящему, так и входящему трафику интерфейса или субинтерфейса. Обычно формирование или ограничение трафика применяется к классовым очередям, т.е. классам трафика. Формирование или ограничение трафика может также применяться ко всему трафику интерфейса.

В оборудовании многих производителей существуют опции настройки, позволяющие настраивать параметры формирования или ограничения трафика как в абсолютных величинах (обычно, скорость в битах за секунду), так и в процентах к скорости интерфейса. Второй случай более подходит для определения универсальных профилей QoS, применимым к интерфейсам с разной скоростью.

Эксперименты и результаты

Для демонстрации свойств механизмов формирования и ограничения трафика покажем результаты экспериментов. Возьмем следующую топологию:

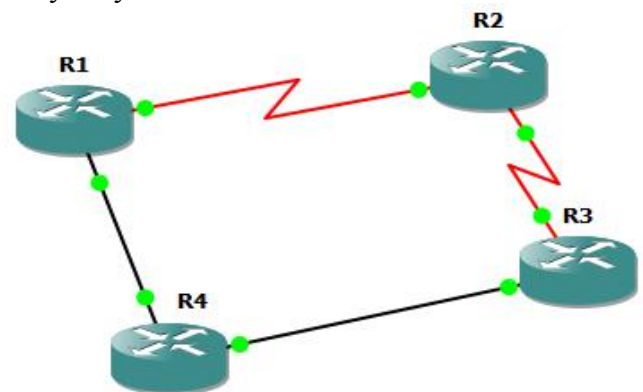


Рис. 1. Топология сети

Механизмы TS и TP будут применяться к выходному трафику маршрутизатора R1 (канал R1-R2). Скорости последовательных каналов (R1-R2 и R2-R3) искусственно ограничим 800 Кбит/с, а скорости остальных каналов (Ethernet) возьмем равными 10 Мбит/с. На R4 запустим генератор трафика TGN [4] и создадим 4 потока трафика с равной интенсивностью (средняя интенсивность каждого потока — 44 пакета/сек., длина пакетов равномерно распределена в интервале от 200 до 1000 байт.), которая подобрана таким образом, чтобы канал R1-R2 постоянно был в состоянии насыщения с минимально возможными потерями. Поток

трафика передается по маршруту R1-R2-R3-R4 и принимается на другом порту R4. На всех очередях установлена дисциплина обслуживания FIFO.

В 1-м эксперименте механизмы TS и TP не используются. Во 2-м эксперименте применим формирование трафика и каждому классу трафика выделим равную ПС (200000 бит/с). В 3-м установим ограничение скорости с аналогичными параметрами. А в 4-м эксперименте трафику 1 (условно, наиболее приори-

тетному) позволим использовать скорость до $PIR=250000$ бит/с. Трафику 2 (менее приоритетному) назначим $Be=2*Vc=25000$ бит. В настройках ограничения скорости трафика 3 (наименее приоритетного) установим только $Vc=25000$ бит. Весь трафик, превосходящий установленные ограничения скорости, будет сброшен. К трафику 4 механизмы формирования/ограничения скорости не применяются. Все параметры экспериментов приведены в Табл. 1.

Табл. 1. Параметры экспериментов.

Сценарий	2, 3		4			
	CIR (byte/s)	Vc (byte)	CIR (byte/s)	Vc (byte)	PIR (byte/s)	Be (byte)
1	200000	6250	200000	6250	250000	7812
2	200000	6250	200000	25000	-	50000
3	200000	6250	200000	25000	-	-

Результаты моделирования (табл. 2) подтверждают, что формирование трафика по сравнению с механизмом ограничения увеличивает время ожидания в очереди. В свою очередь, применение механизма ограничения скорости отличается большими потерями пакетов. Результаты 4-го эксперимента демонстрируют, что при установке параметра

Be (трафик 2) потери пакетов значительно меньше, чем для трафика 3. В то же время, увеличение максимальной скорости (трафик 1), естественно, ликвидировало сброс пакетов для данного трафика. А уменьшение среднего времени задержки объясняется увеличением количества сброшенных пакетов.

Табл. 2. Результаты моделирования.

Сценарий	1			2			3			4		
	Delay (ms)	Jitter (ms)	Loss	Delay (ms)	Jitter (ms)	Loss	Delay (ms)	Jitter (ms)	Loss	Delay (ms)	Jitter (ms)	Loss
1	42,7	20,9	4	163	61	182	27,4	10,2	26	14,9	6,9	0
2	42,9	20,7	6	167	58,7	192	26,7	10,2	24	15,4	6,7	30
3	42,1	20,8	9	160	59,2	171	27,1	10,1	29	14,7	6,9	86
4	42,5	20,8	2	161	55,2	164	27,5	10,1	25	15,3	6,9	0

Однако, экспериментально не удалось показать влияние параметра Tc на время задержки и потери пакетов. Это можно объяснить пачечностью трафика или особенностями реализации механизмов TS и TP.

Сравнивая механизмы формирования и ограничения трафика в целом, отметим, что ограничение скорости «срезает» выбросы интенсивности, а формирование трафика выравнивает скорость передачи на уровне установленной интенсивности (что естественным образом делает трафик более предска-

зуемым).

Можно заметить, что эффективность утилизации пропускной способности выше при использовании формирования трафика (передача пакета может быть отложена, в то время, как при механизме ограничения скорости пакет будет сброшен). Причем, формирование трафика достигает наибольшей эффективности, если размеры выбросов трафика меньше значения Vc .

Кроме того, из-за эффекта глобальной синхронизации, ограничение скорости ухудшает эффективность передачи TCP

трафика, в то время, как для UDP-трафика или в случае использования формирования трафика этого не наблюдается. Это объясняется тем, что при отбрасывании пакетов протокол TCP сужает окно потока, что может быть причиной падения интенсивности. Подобрав параметры всплеска трафика в соответствии с реализацией TCP теоретически возможно повысить эффективность передачи TCP. На трафики, не использующие адаптивное регулирование скорости передачи (IP, UDP, ICMP), параметр всплеска не оказывает заметного влияния.

Вариация параметров настройки ограничения трафика показала, что для потоков с большими колебаниями интенсивности эффективней большие значения B_c . В некоторых случаях утилизацию канала можно повысить, удвоив значение B_c (в рекомендациях производителя оборудования встречается рекомендованная цифра $B_c=1.5 \cdot CIR$).

Выводы

Знание особенностей управления интенсивностью трафика (формирования и ограничения)

позволяет более конструктивно применять данные механизмы с целью профилирования трафика на входе в сеть или на границе областей ответственности. Оперируя трафиками с предсказуемым профилем, возможно более точно организовать обработку таких потоков с целью обеспечить требуемые характеристики качества обслуживания.

Не смотря на то, что применяемые в настоящее время модели и механизмы управления трафиком сформировались примерно десяток лет тому назад, их эволюцию нельзя считать завершенной. За это время появились такие понятия, как конвергентные сети, triple play, wireless QoS, которые безусловно повлияли на представление об архитектуре качества обслуживания. Помимо этого, появляются новые реализации ранее известных механизмов качества обслуживания, а также категории трафика с не встречавшимися ранее статистическими паттернами, что требует некоторого переосмысления поведения известных механизмов качества обслуживания.

Список литературы

1. Вегешна Ш. Качество обслуживания в сетях IP. :Пер. с англ. - М.: Изд. дом «Вильямс», 2003. - 368 с.
2. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. - СПб.: Наука и Техника, 2004. - 336 с.: ил.
3. Демчинский В.В., Дорогой Я.Ю., Дорошенко К.С. Анализ и практика внедрения механизмов качества обслуживания. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. - К.: Век+, -2012. - №57. - 171 с.
4. TGN Traffic Generation Using Cisco Pagent IOS. - [Электронный ресурс]. - URL: <http://www.ciscoconsole.com/nms/traffic-generation-using-cisco-pagent-ios.html/>