Механизмы профилирования трафика

Лекция

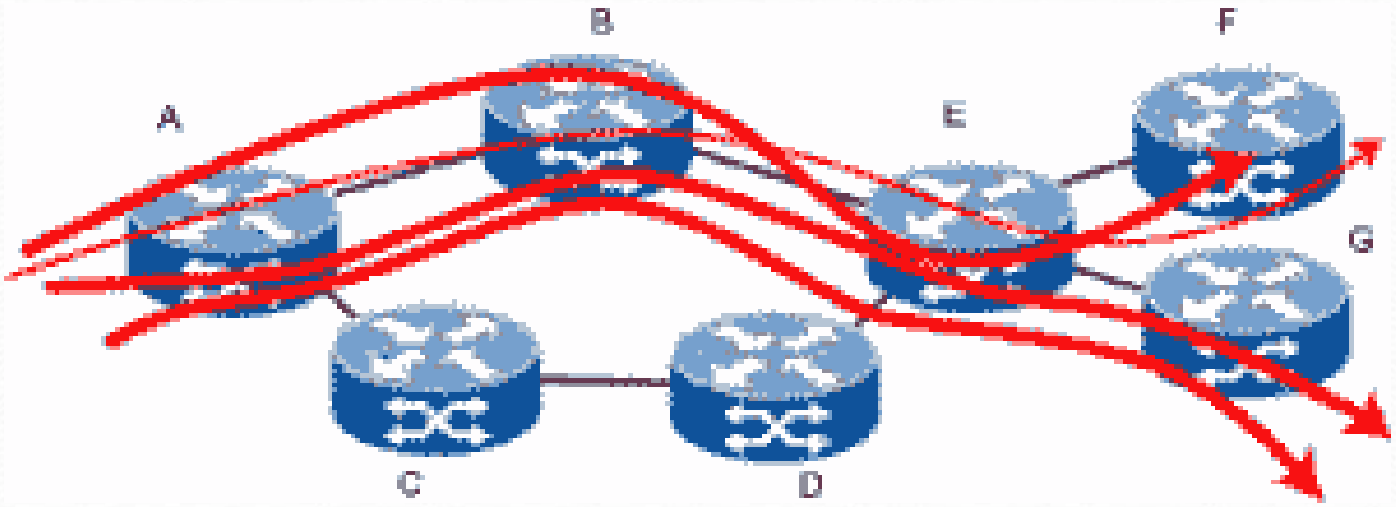
Основные задачи Traffic Engineering:

- ✓ Борьба с перегрузкой
- ✓ Профилирование трафика
- ✓ Резервирование ресурсов

TE – общее название методов, позволяющих обеспечивать QoS согласно заключенному SLA.

Traffic Engineering

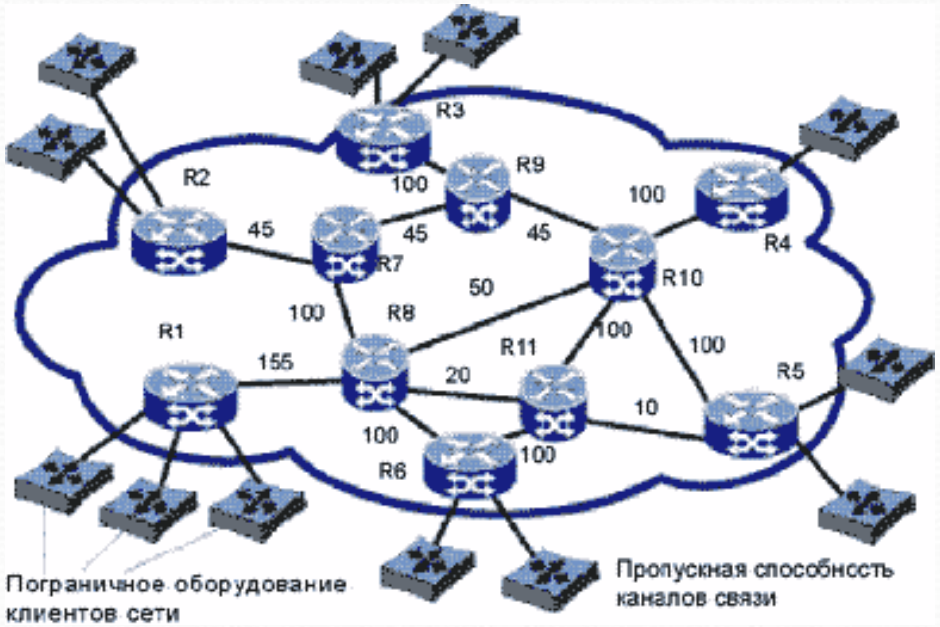
TE – методы и механизмы достижения сбалансированности загрузки всех ресурсов сети за счета рационального выбора путей прохождения трафика через сеть.



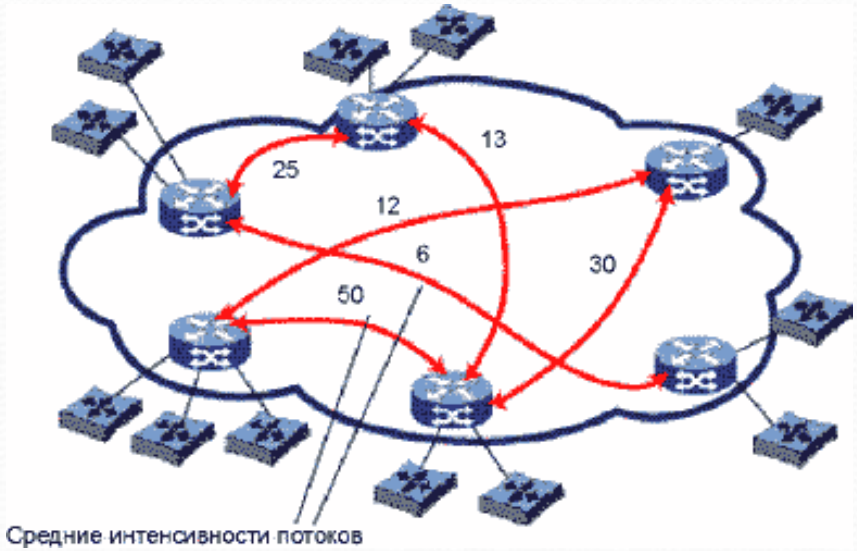
Неэффективность загрузки ресурсов сети путями, определяемыми протоколами маршрутизации.

Постановка задачи TE

Топология сети и производительность её ресурсов

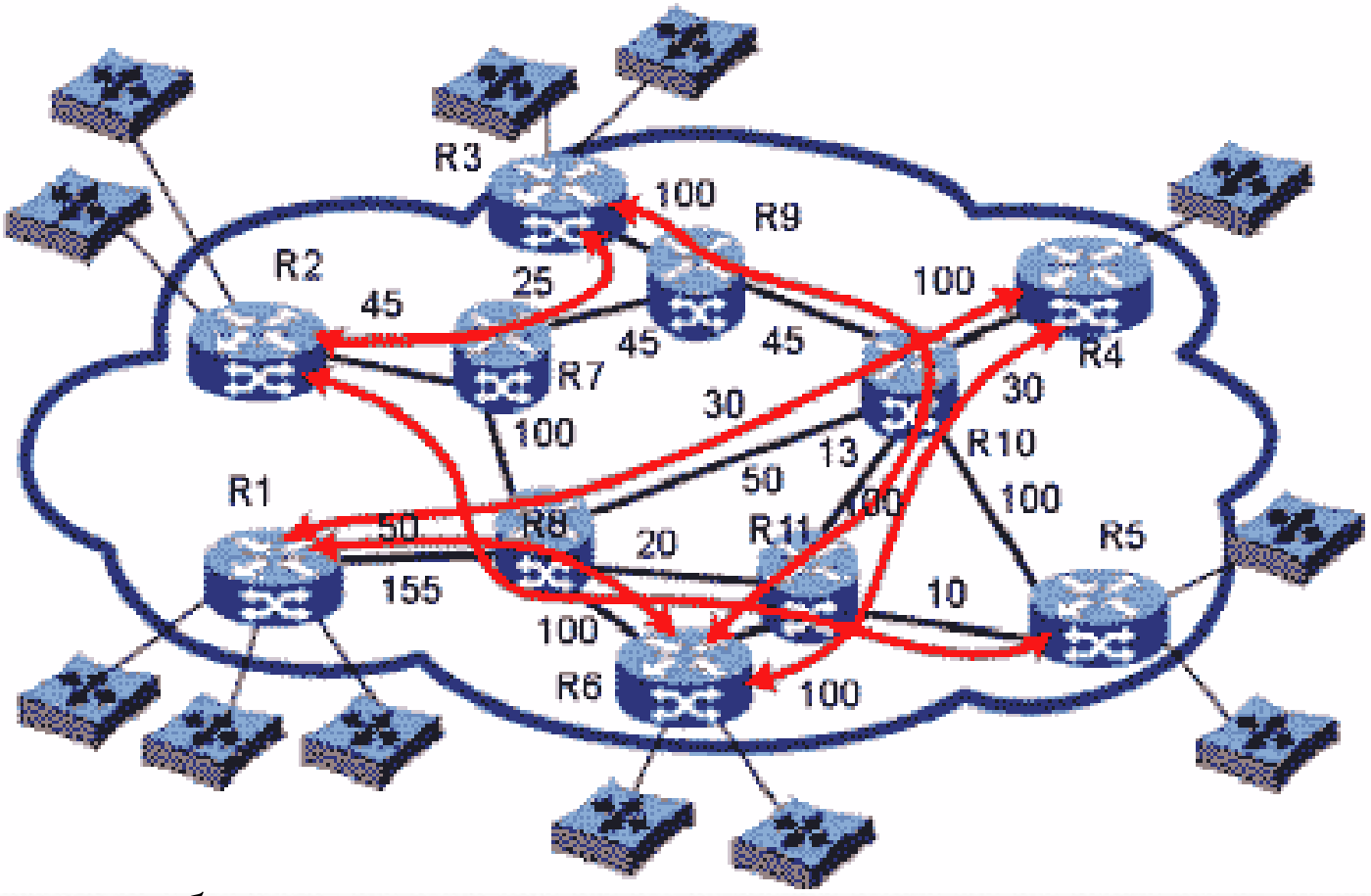


Предложенная нагрузка



Максимальный коэффициент использования ресурса по всем ресурсам сети должен быть минимален, чтобы трафику был нанесен как можно меньший ущерб.

Распределение нагрузки по сети — выбор пути следования трафика



Поиск такого набора маршрутов для заданного множества потоков трафика, для которого все значения коэффициентов использования ресурсов вдоль следования каждого потока не превышают заданного порога K_max.

Общая формулировка задачи управления сетью связи:

- Задача управления в IP-сетях сводится к выбору служб и программно-аппаратных средств, обеспечивающих администратора информацией о работе сети и дающих возможность автоматически или автоматизировано влиять на её работу.

Частные задачи управления

- контрольная плоскость:
  - маршрутизация (OSPF, BGP);
  - управление удаленными устройствами (администрирование - SNMP).
- плоскость данных:
  - управление трафиком: политики и профилирование (LB, RED, WFQ и т.д.);
- плоскость менеджмента:
  - уведомление об ошибках (ICMP);
  - мониторинг (ICMP, netstat).

Общие принципы борьбы с перегрузкой:

- ✓ Наблюдение за системой (мониторинг)
- ✓ Передача информации о возможной перегрузке
- ✓ Принятие необходимых мер для предотвращения перегрузки
- ✓ Принятие необходимых мер для устранения перегрузки при ее возникновении

Стратегии предотвращения перегрузки:

- ✓ Транспортный уровень:
  - Повторная передача
  - Кэширование пакетов (на приеме и передаче)
  - Подтверждения (квитирование)
  - Управление потоком
  - Определение тайм-аутов

- Сетевой уровень
  - Использование резервирования ресурсов путем организации виртуальных каналов
  - Политика обслуживания очередей
  - Политика отбрасывания пакетов
  - Управление временем жизни пакета
  - Маршрутизация
- Канальный уровень
  - Управление потоком
  - Кэширование
  - Повторная передача
  - Квитирование

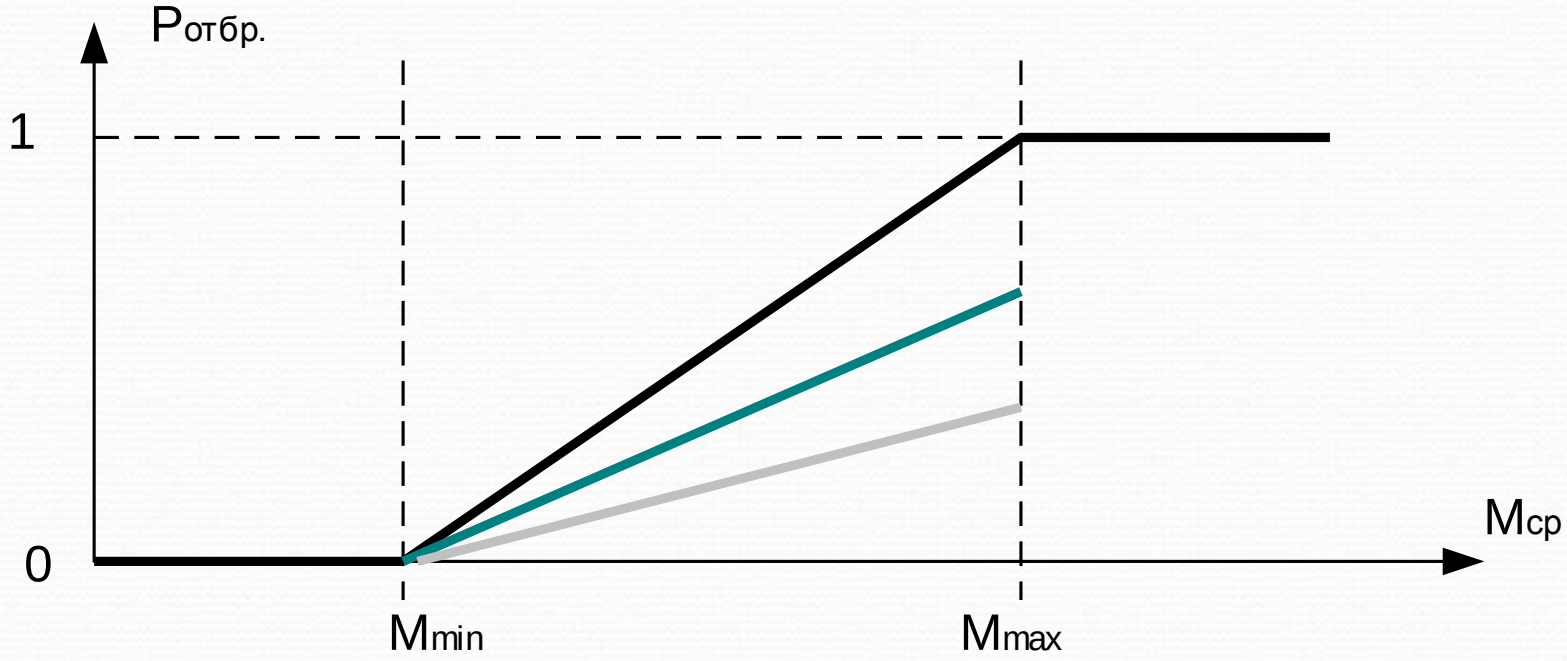
- Механизмы ***кондиционирования*** трафика обычно включает: ***классификацию, профилирование и формирование трафика***.
- **Классификация трафика** может выполняться на основе различных формальных признаков потока данных (адрес назначения, метка потока и др.).
- **Профилирование трафика** подразумевает проверку соответствия каждого входного потока (например, его средней скорости или времени пульсаций) ограничениям, заданным в контракте, с последующим приведением параметров потока-нарушителя к ранее оговоренным путем отбрасывания части его пакетов.
- Путем **формирования трафика** стремятся сгладить его пульсации, чтобы на выходе из узла поток был более равномерным, чем на его входе.

Механизмы профилирования трафика

- **Drop tail** – отбрасывание хвоста: отбрасываются все пакеты, заставшие буфер полным. Используется в «best effort».
- **RED** – случайное раннее обнаружение: при угрозе перегрузки пакеты из буфера отбрасываются с ненулевой вероятностью.
- **Дырявое ведро** – отбрасываются пакеты, не обслужившиеся за установленный период.
- **Корзина маркеров** (токенов) – дозирование трафика с целью уменьшения неравномерности продвижения пакетов

Алгоритм RED

- RED - Random Early Detection: случайное раннее обнаружение. Применяется в IP-ориентированных сетях. Предотвращает предвзятое обслуживание трафика, эффект глобальной синхронизации, выравнивает джиттер задержки.



RED базируется на двух основных алгоритмах:

-алгоритм вычисления среднего размера очереди

$$M_{ср} = M_{ср(t-1)} \cdot (1 - 0{,}5^n) + M_t \cdot 0{,}5^n ,$$

где $M_{ср(t-1)}$ – предыдущий средний размер очереди,

M_t – текущий размер очереди,

n – экспоненциальный весовой коэффициент

-алгоритм вычисления вероятности отбрасывания пакетов

$$P = \frac{(M_{cp} - M_{min})}{(M_{max} - M_{min})} \cdot \frac{1}{K}$$

где $M_{ср}$ – средний размер очереди,

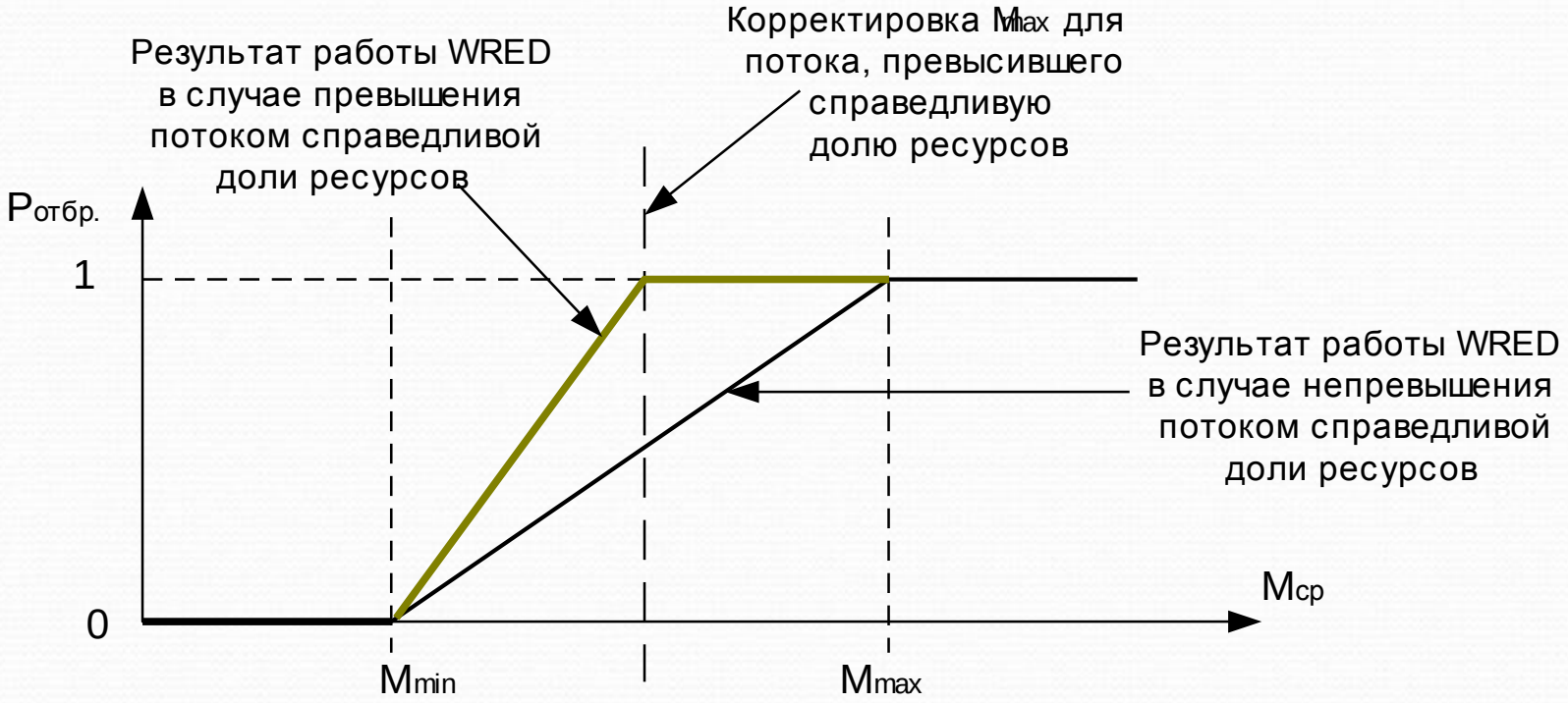
M_{min} – минимальное пороговое значение среднего размера очереди,

M_{max} – максимальное пороговое значение среднего размера очереди,

K – знаменатель граничной вероятности

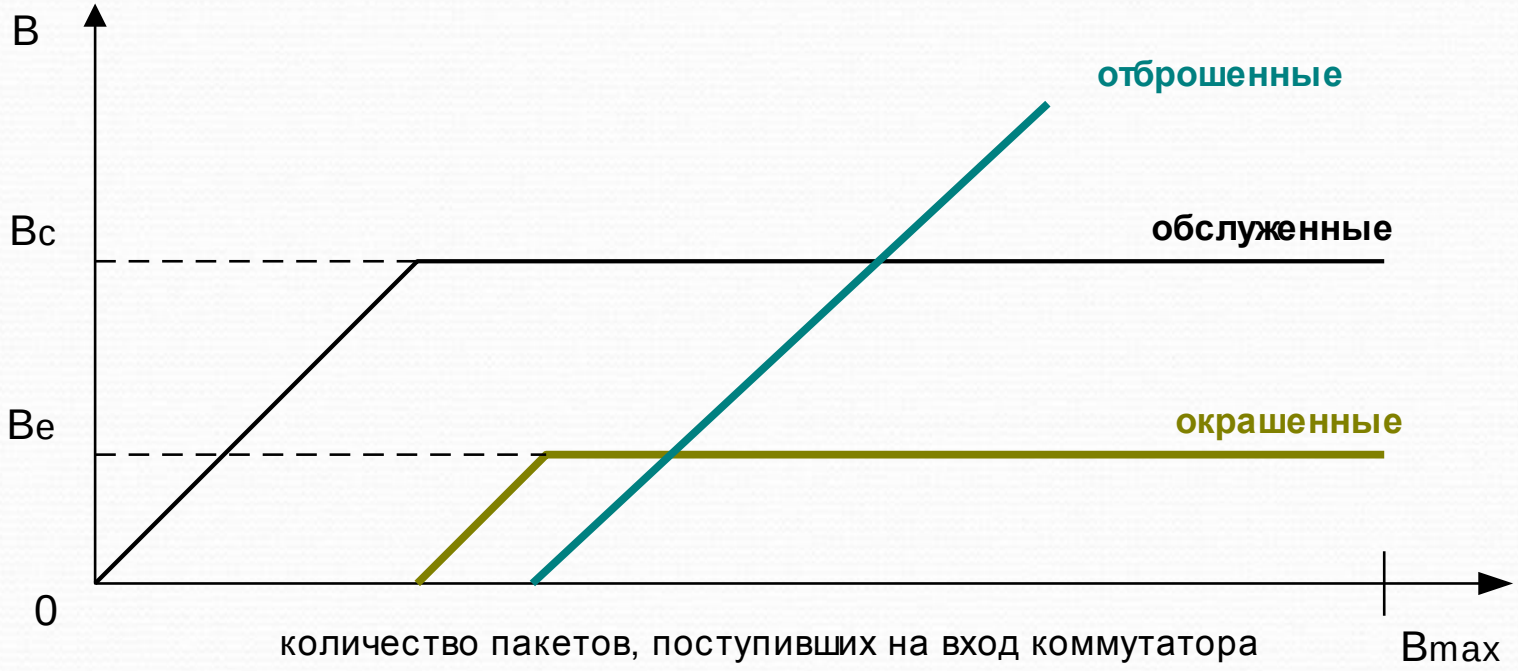
Flow WRED

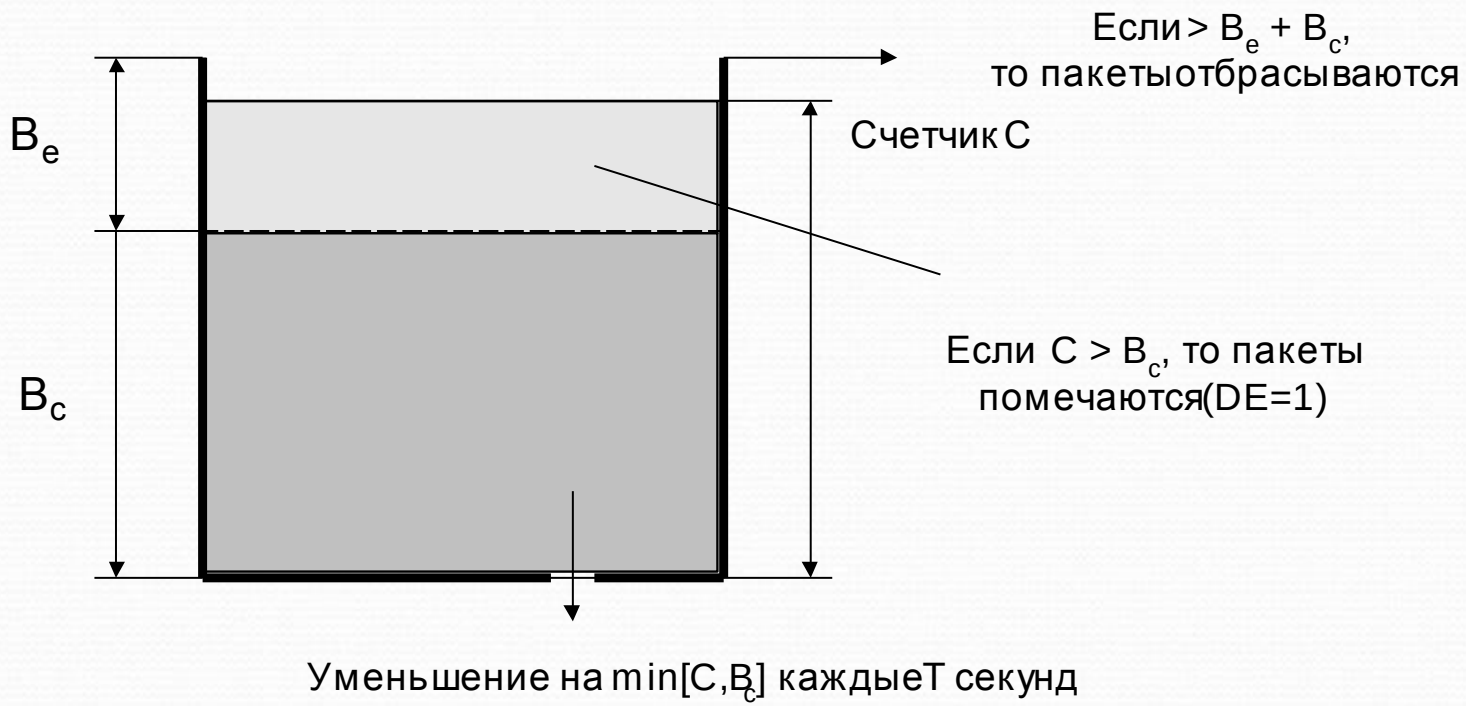
- Модификация алгоритма RED – взвешенное случайное раннее обнаружение перегрузки на основе потока. Классифицирует пакеты в зависимости от приоритета, производит мониторинг состояния активных потоков, корректирует политику отбрасывания пакетов путем введения коэффициента масштабирования.



Алгоритм «дырявого ведра»

- Семейство алгоритмов класса «дырявое ведро» (LB – Leaky Bucket) используется практически во всех современных коммутаторах Frame Relay и ATM-коммутаторах. Модификация алгоритма «дырявого ведра» Generic Cell Rare Algorithm (GCRA) применяется в сетях ATM для контроля нескольких параметров: пиковой скорости, средней скорости, вариации интервала прибытия ячеек и объема пульсации.





CIR – Committed Information Rate: средняя скорость трафика;

T — период усреднения скорости;

B_c — объем пульсации, соответствующий средней скорости CIR и периоду T: $B_c = CIR \times T$;

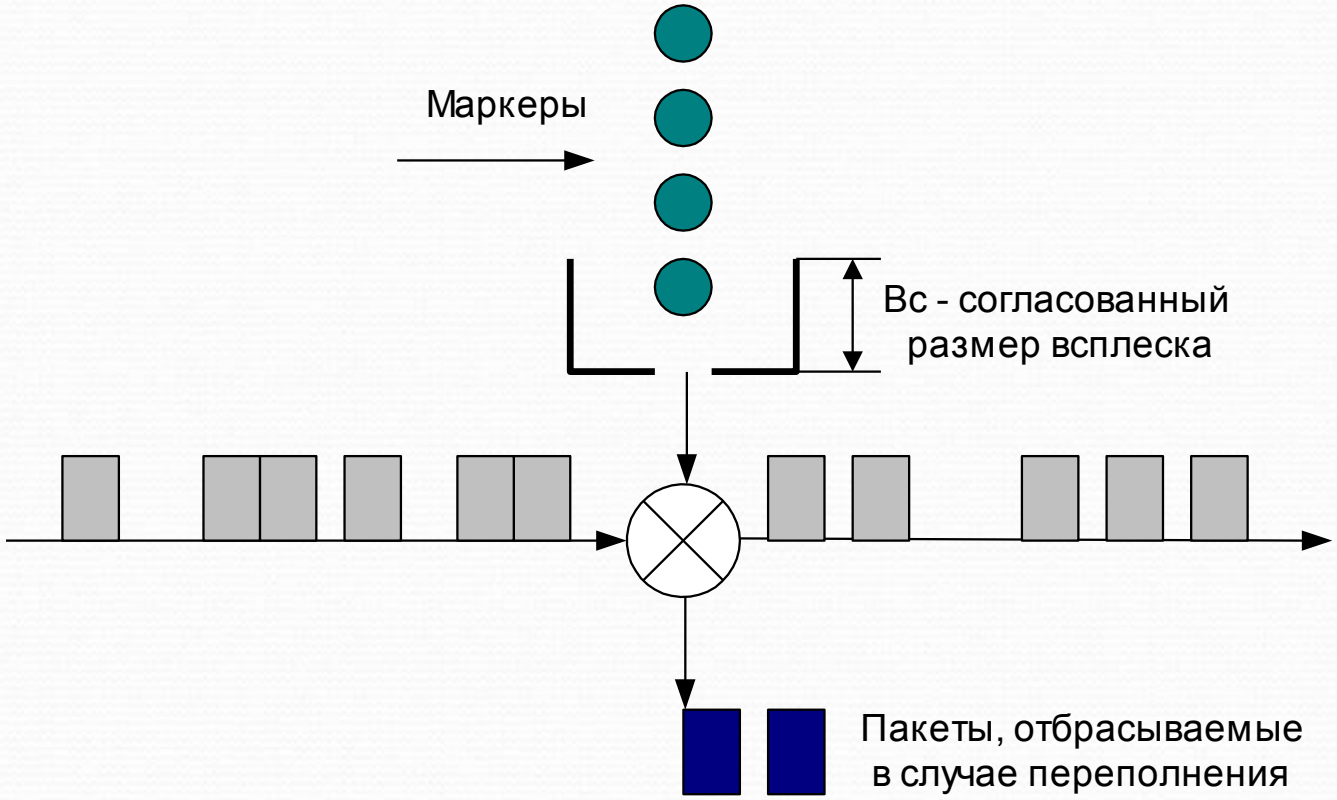
B_e — допустимое превышение объема пульсации.

DE=1 (Discard Eligibility) – признак «окрашивания» пакета.

Если пакет с признаком DE=1 не обслужен в течение периода, то он должен быть отброшен.

Корзина маркеров

- Дозирование и выравнивание трафика. Применяется во всех пакетных сетях. Имеет две модификации: стандартная: не поддерживает резкого увеличения всплеска, допускает потери пакетов (отбрасывание хвоста); с возможностью резкого увеличения всплеска: количество маркеров может изменяться при увеличении интенсивности трафика.



Испытания систем управления пропускной способностью

- Длительность испытаний: месяц
- 4 производителя:
  - Cisco 7206VXR фирмы Cisco Systems
  - NetEnforcer AC301 фирмы Allot Communication
  - NetScreen-5 фирмы NetScreen Technologies
  - GuardianPro 4.11 фирмы NetGuard
- Нагрузка: около двух сотен одновременных Web-сеансов связи
- Цель: оценка работоспособности оборудования ЛВС при взрывном характере трафика

Классификация трафика

- Продукт Cisco 7206VXR предоставляет самое большое число критериев классификации трафика, начиная с MAC-адресов на втором уровне и кончая указателями URL и маркерами cookies на седьмом уровне.
- Устройство фирмы Allot также умеет анализировать адреса URL.
- Производители не изъявили желания демонстрировать в тестах на производительность механизмы классификации трафика на прикладном уровне. Это связано с тем, что указатели URL спрятаны внутри пакетов слишком глубоко, и процесс их поиска и интерпретации привносит дополнительную задержку.
- Общими для всех четырех продуктов были возможности классифицировать трафик на основании IP-адресов и номеров протокольных портов TCP/UDP.
- Лишь устройства Allot и Cisco поддерживают два новых механизма QoS, использующих поля IP Precedence и DiffServ CodePoint (DSCP) заголовка IP-пакета. Продукты обоих этих производителей могут не только классифицировать трафик на основании ранее установленных значений этих полей, но и помечать пакеты, устанавливая новые значения битов IP Precedence и DSCP.

Базовые испытания

- Измерения пропускной способности и задержек.
- Правила профилирования (shaping) трафика в этих тестах не задействовались.
- Первый набор тестов предназначался для измерения скоростей передачи и числа потерянных кадров.
- На входы каждого устройства подавали потоки пакетов, имеющих длину 64 и 1518 байтов, и отмечали максимальную скорость передачи без потери пакетов.
- Использовались как однонаправленные, так и двунаправленные потоки данных.
- Результаты, полученные в ходе проведения данного теста, должны полностью удовлетворить пользователей, работающих по линиям со скоростями на уровне 1,5 Мбит/с: все устройства без труда обрабатывают потоки, поступающие на таких скоростях.

Результаты базовых испытаний. Пропускная способность

- Устройство фирмы NetScreen работает на максимальной скорости 10 Мбит/с, а устройство компании Cisco - на скорости 1,5 Мбит/с.
- Продукты NetEnforcer AC301 фирмы Allot и Guidepost фирмы NetGuard поддерживают скорости до 100 Мбит/с, правда, ни один из них не мог передавать на высоких скоростях **короткие пакеты**.
- Так, NetEnforcer AC301 начинал сбрасывать их при нагрузках, составляющих 15% и 5% от максимальной (для однонаправленных и двунаправленных потоков соответственно), а Guidepost - при нагрузках 29% и 12% от максимальной.
- Представители компании Allot считают, что трафик, состоящий лишь из пакетов **длиной 64 байта**, никогда не встречается в реальных сетях: тесты с пакетами такой длины предназначаются, главным образом, чтобы выявить границы работоспособности оборудования.

Результаты базовых испытаний. Задержки

- Самую низкую задержку обеспечивал продукт NetEnforcer AC301 фирмы Allot. Даже при обработке длинных пакетов и двунаправленных потоков он никогда не задерживал трафик более чем на 236 мкс.
- Наибольшую задержку - около 4,4 мс - показал продукт Cisco 7206VXR.
- Для остальных испытуемых устройств максимальная задержка пакетов, передаваемых на скорости 1,5 Мбит/с, не превышала 2 мс.

Условия испытаний

- Слежение за состоянием 200 соединений.
- Обработка взрывного трафика, представляющего собой короткие интенсивные пачки пакетов - именно такой характер чаще всего и носит трафик Web-узлов.
- Изучение информации, хранящейся на Web-сайтах, показывает, что средний размер их объектов составляет как раз где-то 10 Кбайт. Ясно, что для эффективного профилирования потоков менеджеры полосы пропускания должны быстро обрабатывать пульсирующий трафик.
- Для передачи Web-потоков использовался протокол HTTP версии 1.0, требующий установления нового TCP-соединения для каждого передаваемого объекта.

Способы профилирования трафика

- путем выделения трафику определенного типа строго заданной полосы пропускания,
- путем обеспечения ему заданной задержки,
- путем приоритезации разнородного трафика.

Таблица 1. Системы управления трафиком: результаты тестирования					
Критерий оценки	Значимость критерия, %	Cisco 7206VXR фирмы Cisco	NetScreen-5 фирмы NetScreen	NetEnforcer AC301 фирмы Allot	GuardianPro 4.11 фирмы NetGuard
Производительность	40	4	4	4	3
Конфигурирование/ управление	25	5	5	5	4
Функциональные возможности	20	5	5	5	4
Совместимость с други-ми устройствами QoS	10	5	3	4	3
Цена	5	2	5	2	4
Итоговая оценка		4,45	4,40	4,35	3,50
Примечание. Оценки выставлялись по пятибалльной системе					

Таблица 2.Характеристики протестированных систем управления трафиком Интернет

Характеристика	Cisco 7206VXR	NetScreen-5 фирмы NetScreen Technologies	NetEnforcer AC301 фирмы Allot Communications	GuardianPro 4.11 фирмы NetGuard
Исиользуемые режимы работы	Мост	Маршрутизатор	Мост/маршрутизатор	Маршрутизатор
Поддерживаемые интерфейсы	10/100 Base-T	10- и 100Base-T Ethernet; Gigabit Ethernet (оптический); Fast Ethernet ISL и Token Ring ISL; 4/16-Мбит/с Token Ring; T3 ATM и OC-3 ATM; шина и тег; для канализируемой линии T3; E1/E3; Escon; FDDI; HSSI; IMA; BRI и PRI ISDN; OC-3 POS; T1/T3	Определяется системой, на которую установлен данный пакет	10/100Base-T
Использование виртуальных интерфейсов	m	l	l	m
Возможность глобального изменения конфигурации	m	m (посредством менеджера QoS Policy Manager)	m	m
Время одной перезагрузки	48 с	1 мин 42 с	2 мин 3 с	30 с

- **NetEnforcer AC301**
  - Цена: 13 000 долл.
  - Фирма: Allot Communications
  - www.allot.com
- **Cisco 7206VXR (с NPE-300)**
  - Цена:22 000 долл.
  - Cisco QoS Policy Manager 1.1
  - Цена: 9995 долл.
  - Cisco QoS Device Manager 1.0
  - Цена: бесплатно (в США)
  - Фирма: Cisco Systems
  - Телефон в Москве: 961-1410
  - www.cisco.com
- **GuardianPro 4.11**
  - Цена: 2495 долл. (с лицензией на 25 пользователей)
  - Фирма: NetGuard
  - www.netguard.com
- **NetScreen-5**
  - Цена: 995 долл.
  - Фирма: NetScreen Technologies
  - www.netscreen.com