

# **Технологии управления трафиком и перегрузками**

**Костюкович А.Е.  
Каф.АЭС, СибГУТИ**

# Цель управления трафиком и перегрузками

Любой оператор стремится **при заданном уровне качества – обеспечить максимальную утилизацию (использование)** сетевых ресурсов.

Работу пакетной сети можно считать эффективной, когда каждый ресурс загружен, но не перегружен.

Это значит, что утилизация ресурса должна приближаться к единице, но не настолько, чтобы очереди (неизбежное явление в пакетных сетях) были постоянно большими, приводя к задержкам и потерям из-за переполнения буферов в узлах.

Оптимизация сетевых ресурсов за счет управления трафиком позволяет выжать из сети максимум возможного. Эта цель достигается с помощью **технологий управления трафиком, очередями, перегрузками**.

# Управление трафиком

В ядре сети могут возникать перегрузки по отдельным направлениям, например, из-за неравномерности нагрузки во времени, отказов элементов сети и т.п.

Это может привести к значительному снижению качества пропуска трафика, вплоть до разрыва соединений и рестарта отдельных сетевых узлов и сети в целом (с потерей всего трафика на период рестарта).

В сетях ТфОП-TDM такой ситуации ни возникало, т.к. ТфОП не может принять больше трафика, чем может его обслужить.

Клиентам пытающимся получить доступ к ТфОП, когда все каналы заняты – идет отказ в обслуживании (очереди не в сети, а «на дому»), но если клиенту удалось дозвониться, то сеть ТфОП обслужит это соединение по высшему качеству!

# Управление трафиком

Сеть с КП принимает на обслуживание трафика больше, чем имеющаяся ПП в отдельных направлениях.

Это принципиально отличает сети с КП от сетей с КК и позволяет более эффективно использовать ПП!

Однако, это может приводить и к перегрузкам (локальным и глобальным)!

**Перегрузки приводят к снижению качества предоставляемых услуг.**

## Причины перегрузки:

- неравномерность пользовательского трафика во времени,
- недостатки проекта сети,
- отказы элементов сети (линий, СП, узлов),
- отсутствие механизмов управления трафиком,
- неквалифицированное вмешательство технического персонала... .

# Управление трафиком

Имеющиеся механизмы управления трафиком позволяют администратору сети грамотно распределять сетевые ресурсы и предупреждать перегрузки или мягко их устранять, не доводя до рестарта!

Управление трафиком является основным инструментом для управления качеством оказываемых услуг.

## К управляемым сетевым ресурсам относятся:

- пропускная способность сетевых интерфейсов
- очереди и приоритеты в узлах (буферная память)
- маршрутные таблицы
- тарифы

Максимальный коммерческий эффект от сети может быть получен только при оптимальном использовании всех сетевых ресурсов – в первую очередь пропускной способности.

# Управление трафиком

## К средствам управления трафиком относят:

1. Управление трафик-контрактами (SLA)
2. Управление пропускной способностью, осуществляемое путем:
  1. расширения полосы пропускания (ПП)
  2. динамического использования ПП
  3. резервирования ПП
3. Управление очередями, осуществляемое путем:
  1. сортировки входящего трафика по видам (например, по допустимым задержкам, по занимаемой ширине полосы пропускания)
  2. ограничения или сброса входящей нагрузки
  3. кэширования
  4. распределения приоритетов во входящем трафике
4. Управление маршрутизацией, осуществляемое путем:
  1. изменения маршрутных данных (планирование и модификация маршрутных таблиц)
  2. динамической маршрутизации с учетом таких показателей как стоимость маршрута, задержки, другие показатели QoS
5. Управление тарифами осуществляемое путем:
  1. изменения тарифов в отложенном времени
  2. изменения тарифов в реальном времени
  3. оплата не за время сеанса, а за реально переданный объем информации
6. Управление перегрузками

**SLA**

**Service Level Agreement**

# Принципы соглашения о трафике между пользователем и сетью (Service Level Agreement, SLA)

**Управление трафиком начинается с момента заключения договора с клиентом (трафик-контракта, SLA).**

**В SLA должны быть следующие параметры (профиль) трафика:**

- требуемая скорость в течение сеанса ( $V_{\text{пик}}$ ,  $V_{\text{ср}}$ ,  $K_{\text{пач}}$ )
- максимальная продолжительность пика нагрузки  $T_{\text{пик}}$
- допустимая задержка пакетов в потоке ( $t_3 \leq D$ )
- допустимая вероятность потери пакетов в потоке ( $P_{\text{пак}} \leq M$ )
- правила проверки соответствия действительных параметров трафика требуемым
- данные для маршрутизации трафика (адреса - пунктов назначения).

Оператор (провайдер) предлагает клиенту на выбор один из стандартизованных классов качества обслуживания в форме типовых SLA (профилей), соответствующих видам услуг (IP-телефония, IPTV, Интернет, E-mail,...).



# Технологии управления трафиком

Для технологии АТМ были предложены следующие механизмы управления трафиком:

- 1.CAC** (Connection Admission Control) – контроль за установлением соединения;
- 2.UPC/NPC** (Usage Parameter Control/Networks Parameter Control) – контроль за использованием пропускной способности сети;
- 3.Priority Control** – контроль приоритетов;
- 4.ABR Flow Control** – контроль потока ABR;
- 5.Selective Cell Discard** – выборочная отбраковка ячеек.

# Технологии управления трафиком

Контроль за установлением соединения (**CAC**) реализует процедуру доступа в сеть и определяет саму возможность установления запрошенного соединения.

Данный механизм использует параметры, указанные в [трафик-контракте \(SLA\)](#).

Если ресурсов достаточно и запрошенное качество услуг может быть предоставлено, а качество услуг других соединений не пострадает, то сеть разрешает установить соединение.

Если любое из перечисленных условий не выполняется, то запрос на соединение отклоняется.

Контроль за установлением соединения осуществляется на каждом коммутаторе в пути от отправителя к получателю.

Контроль за расходом пропускной способности сети (**UPC**) определяется как набор выполняемых сетью действий по мониторингу и контролю за трафиком.

Данный механизм проверяет корректность VPI/VCI, обеспечивает контроль за согласованным в SLA трафиком и, если это необходимо, осуществляет маркировку или отбраковку любых ячеек, передача которых может привести к нарушению достигнутых соглашений.

Т.е. UPC реализует проверку соответствия параметров поступившего трафика оговоренным в SLA параметрам.

Каждый раз, когда ячейка поступает в сеть, запускается тест на определение соответствия поступающего трафика заявленному.

Если ячейка не приводит к превышению заданных в SLA параметров, то она передается дальше; в противном случае ячейка либо отбрасывается до поступления в сеть, либо надлежащим образом помечается (с помощью бита CLP в заголовке).

Функционально механизм **UPC** реализуется первым коммутатором на входе в сеть с помощью алгоритма под названием "**дырявое ведро**" (Leaky Bucket - ITU-T\_I.371).

Такое название он получил потому, что принцип действия алгоритма демонстрируется на примере ведра с отверстием в днище фиксированного размера (ПП).

Ячейки попадают в это ведро, а затем "протекают" в сеть. При переполнении ведра избыточные ячейки маркируются как подлежащие удалению.

Серия тестов на соответствие может быть реализована с помощью одного или более "дырявых ведер", имеющих различные параметры.

Количество "дырявых ведер" зависит от типа трафика и "жесткости" заключенного **SLA**.

Например, при проверке трафика для соединений с постоянной скоростью передачи коммутатору достаточно одного "дырявого ведра", в то время как для соединений с переменной скоростью ему потребуется два.

Механизм **NPC** предназначен для проверки параметров контроля потока ячеек через интерфейс NNI между сетями.

При этом им используются те же методы, что и в **UPC**

# Технологии управления трафиком

В сетях на базе IP/MPLS под технологиями управления трафиком подразумевается поддержка следующих операций:

1. **Traffic policing** - планирование трафика
2. **Traffic Scheduling** - выбор алгоритмов обслуживания
3. **Traffic shaping** - формирование трафика

# Технологии управления трафиком

**Traffic Policing**. Для планирования трафика используются следующие механизмы:

- **Metering** – сравнение входящего трафика с профилем, заявленным в SLA и включение действий разметки или отбрасывания
- **Marking** – **Разметка («расцветка»)**. Назначение приоритета входящим пакетам, чтобы указать, соответствует ли каждый пакет профилю трафика по результатам сравнения
- **Dropping** – **Удаление пакета** в соответствии с результатом сравнения.

**Traffic Scheduling** – способность осуществлять приоритетную передачу пакетов, основанную на классификации или политике качества обслуживания, с помощью **нескольких очередей**.

## Технологии управления трафиком

**Traffic Shaping** – Формирование и профилирование трафика

**Traffic Shaping** предназначен для сглаживания пульсаций «взрывного» трафика, уменьшения неравномерности продвижения пакетов.

Во время формирования, поток трафика сглаживается и становится **более предсказуемым**. Это облегчает управление буферной памятью и очередями, и позволяет другим функциям управления трафиком более эффективно работать, **обеспечивая соблюдение SLA**.

Формирователь задерживает некоторые или все пакеты в потоке для того, чтобы поток соответствовал **профилю трафика в SLA**. Пакеты могут быть отброшены, если буферной памяти недостаточно.

Формирование трафика осуществляется в узле доступа в сеть.

# Технологии управления трафиком

В стандарте DiffServ механизм **Traffic Shaping** реализуется посредством алгоритмов:

- «**leaky bucket**» (дырявое ведро) – разработан еще для технологий FR и ATM и широко применяется для сглаживания пульсаций трафика, включая сброс пакетов при нарушениях SLA.

Размер «дыры» в ведре соответствует средней (согласованной) пропускной способности. Объем ведра соответствует емкости буферной памяти для сглаживания пиков трафика.

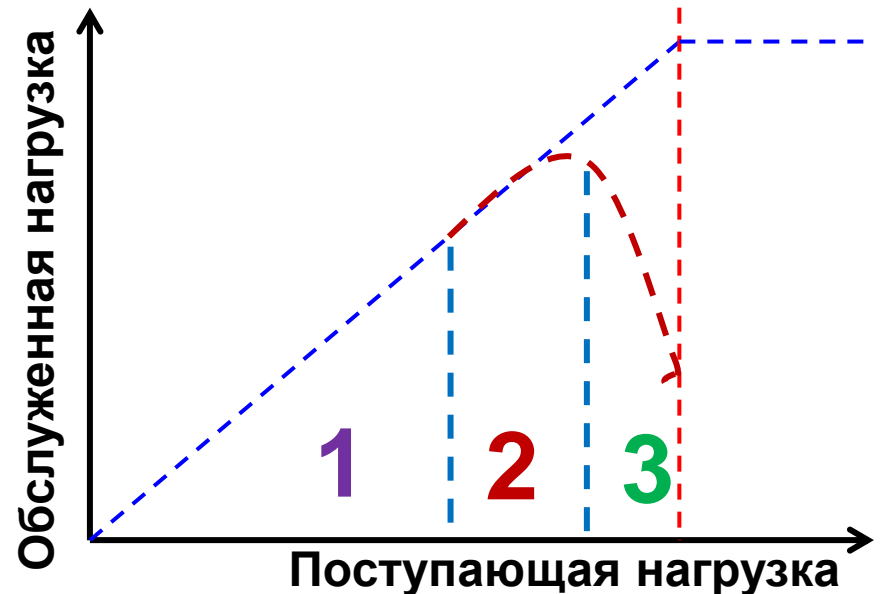
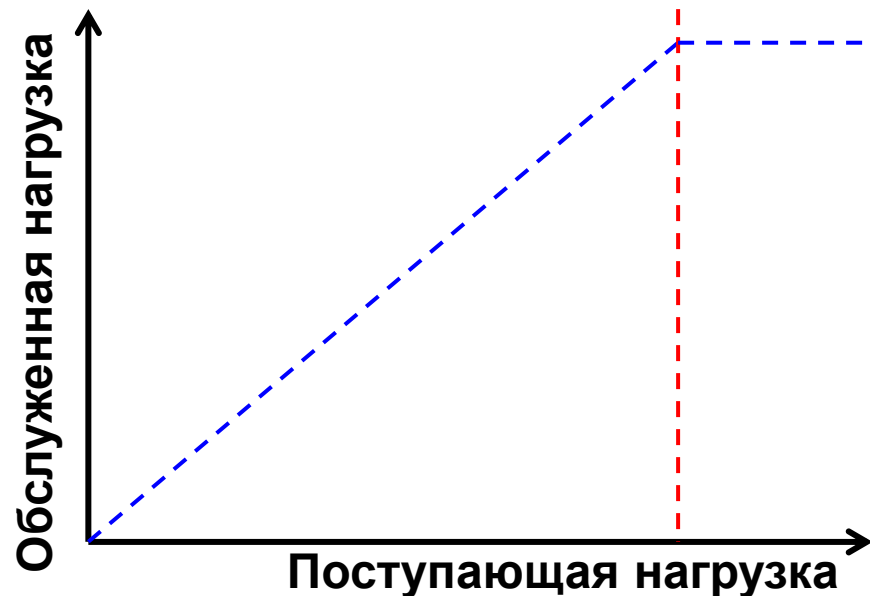
- «**token bucket**» (маркерное ведро) - применяется для мягкого формирования пульсирующего трафика (без сброса пакетов). Количество маркеров в секунду соответствует согласованному количеству пакетов в секунду. Пакеты, не получившие маркер – ожидают в буфере (ведре), размер которого выбирается в соответствии с допустимой задержкой.

# Управление перегрузками

Можно по-разному классифицировать методы борьбы с перегрузками.

Если в качестве признака классификации принять реакцию сети на перегрузку, то можно выделить **три категории** (уровня) управления перегрузками:

- 1. Предотвращение перегрузки (до 60%)**
- 2. Менеджмент перегрузок (60...80%)**
- 3. Восстановление работоспособности сети или ее элементов после перегрузки (>80%)**





# Предотвращение перегрузки (Congestion Avoidance)

Основными методами предотвращения перегрузок являются комбинации методов управления трафиком и очередями:

- явное прямое указание перегрузки (EFCI - Explicit Forward Congestion Indication) – широко использовалось в сетях FR, есть в IPv6;
- маркировка пакетов при контроле параметров пользователя – широко использовалось в сетях ATM, есть в DiffServ/MPLS (**маркерное ведро**);
- управление доступом в сеть на основе контроля ресурсов (метод CAC в ATM);
- контроль потока служб на основе окна, скорости и кредита – TCP, SCCP.
- блокировка вызовов – ТфОП, ATM, H.323;

# Предотвращение перегрузок

Контроль потока служб

Обычно используются три метода управления потоком:

1. на основе окна,
2. на основе скорости,
3. на основе кредита.

1. Контроль потока на основе окна ограничивает объем потока данных (называемый окном), передаваемых источником, и осуществляет регулировку размера окна на основе обратной связи. Контроль потока на основе окна был первым методом, внедренным в СПД. Этот метод широко используется в TCP.

2. При контроле потока на основе скорости вместо размера окна контролируется скорость передачи источника, выражаемая в количестве пакетов, передаваемых за период отклика.

Первоначально скорость передачи равна нулю.

С каждым периодом отклика коммутатор обеспечивает обратную связь с источником, увеличивая или уменьшая допустимую скорость источника.

При контроле потока на основе скорости обеспечивается более равномерная расстановка пакетов, а также более высокая пропускная способность, по сравнению с управлением на основе окна.

3. При управлении потоком на основе кредита источник может продолжать отправлять пакеты до тех пор, пока отсчет кредита превышает ноль. В каждый период отклика коммутатор посылает сообщения обратной связи, объявляя новое значение кредита каждому источнику.

Кредит рассчитывается сетевым узлом как число оставшихся пакетов в буфере для каждого виртуального соединения.

Метод кредита приводит к очень прерывистой, но регулярной передаче ячеек, позволяет изолировать все виртуальные соединения друг от друга.

Используется в **SCCP (ОКС-7)**.

# Менеджмент перегрузки (Congestion Management)

**Управление перегрузками** – способность управлять поведением сети, отбрасывая определенные пакеты на основе классификации, например с помощью технологии **WRED** (Weighted Random Early Detection) и множества очередей на интерфейсах.

Используя возможности протоколов FR, ATM, MPLS, TSP эти механизмы позволяют управлять скоростью передачи данных и снизить скорость передачи между конечными системами, до того как перегрузка затронет приоритетные приложения.

Для настройки механизма управления перегрузкой администратор устанавливает **пороги заполнения буферной памяти** для различных уровней приоритета.

# Менеджмент перегрузки (Congestion Management)

Менеджмент перегрузки начинается в области, где перегрузки еще нет, с целью, чтобы перегрузка не появлялась (от 60 до 80%).

Основными мерами защиты от перегрузок в этом случае являются:

- совершенствование архитектуры сети
- распределение сетевых ресурсов
- контроль доступа в сеть по пиковой скорости потока пакетов, гарантирующий отсутствие перегрузки ПП
- сброс пакетов при контроле параметров трафика пользователя

## Восстановление сети после начавшихся перегрузок

Восстановление после начавшихся перегрузок - это реакция на попадание сети в зону сильных перегрузок ( $>80\%$ ).

Основными методами восстановления являются:

- селективный сброс пакетов при контроле параметров потока пользователя (drop tail, дырявое ведро,...);
- динамическое управление параметрами потока пользователя;
- уменьшение передаваемой нагрузки под воздействием обратной связи;
- **разъединение (сброс) соединений;**
- **управляющие воздействия операторов (рестарт).**

# **Механизмы управления качеством**

# Механизмы управления качеством

Механизмы **управления качеством услуг**,  
включают:

- управление трафиком,
  - управление **приоритетами и очередями**
  - управление **перегрузками**,
- управление пропускной способностью,
- управление задержками,
- управление надежностью...

# Механизмы организации очередей

- 1. FIFO** – Элементарная очередь с последовательным прохождением пакетов, работающая по принципу первый пришел – первый ушел (First In First Out - FIFO). Включается по умолчанию на интерфейсах со скоростью больше 2 мбит/с
- 2. Priority Queuing (PQ)** – очередь с абсолютным приоритетом. PQ обеспечивает безусловный приоритет одних пакетов над другими. Можно организовать несколько очередей, например: high, medium, normal и low. Обработка ведется последовательно (от high до low), начинается с высокоприоритетной очереди и до ее полной очистки не переходит к менее приоритетным очередям. Таким образом, PQ допускает **монополизацию канала** высокоприоритетными очередями. Трафик, приоритет которого явно не указан, попадет в очередь по умолчанию (default).
- 3. Class Based Queueing (CBQ)** - классовая дисциплина, предназначенная для создания сложных систем управления трафиком. Поддерживает ограничения и приоритеты



# Механизмы организации очередей

Механизмы Активного Управления Очередью (Active Queue Management – AQM)

1. **Weighted Fair Queuing (WFQ)** – взвешенная справедливая очередь,
2. **Class-Based Weighted Fair Queuing (CBWFQ)** – тоже, но с классификацией,
3. **Low Latency Queuing (LLQ)** – очередь с малой задержкой,
4. **Tail drop** (Отбрасывание конца очереди или Обрубание хвоста) – простейший алгоритм AQM для управления переполнением очередей
5. **Random early detection (RED)** (Произвольное Раннее Обнаружение) - управление переполнением очередей (по превышению порога).
6. **Weighted Random Early Detection (WRED)** - Взвешенное Произвольное Раннее Обнаружение - управление переполнением очередей, с возможностями предотвращения перегрузок (несколько порогов!) (TCP, FR, ATM).

# Механизмы организации очередей

Простейшие технологии, не обладающие свойствами управления трафиком, реализуют дисциплину обслуживания очередей без приоритетов (пример - Ethernet):

FIFO – First-in-First-out

Для полноценного **управления трафиком**, включая защиту от перегрузок, разработаны следующие механизмы организации очередей и формирования трафика:

# Механизмы организации очередей

- 1.**PQ** (Priority Queuing) – очередь с абсолютными приоритетами
- 2.**CQ** (Custom Queuing) – настраиваемая очередь
- 3.**CBQ** (Class Based Queueing) - классовая дисциплина.  
Поддерживает ограничения и приоритеты
- 4.**WFQ** (Weighted Fair Queuing) – взвешенная справедливая очередь
- 5.**CBWFQ** (Class-Based Weighted Fair Queuing) –  
справедливая очередь, основанная на классах
- 6.**LLQ** (Low Latency Queuing) – очередь с малой задержкой
- 7.**WRED** (Weighted Random Early Detection) – взвешенное случайное обнаружение

# Механизмы организации очередей

Приоритезация трафика требуется в узких, загруженных местах, когда пропускной способности интерфейса не хватает для передачи всех поступающих пакетов и нужно каким-то образом дифференцировать их обработку.

Приоритезация необходима также и в случае предотвращения влияния всплесков сетевой активности на чувствительный к задержкам трафик.

# Механизмы организации очередей

## 1. PQ – Очереди с абсолютными приоритетами.

PQ обеспечивает безусловный приоритет одних пакетов над другими.

Может быть организовано N очередей от **high** до **low**.

Обработка ведется последовательно, начинается с высокоприоритетной очереди (**high**) и до ее полной очистки не переходит к менее приоритетным очередям.

Недостаток этой дисциплины – если в поступающих пакетах присутствует интенсивный трафик реального времени (например, видео), то возможна монополизация канала высокоприоритетными очередями.

# Механизмы организации очередей

## 2. CQ – Custom Queuing – Произвольные очереди.

CQ обеспечивает возможность настройки очередей.

Предусматривается управление **долей полосы пропускания** канала для каждой очереди. Поддерживается до 17 очередей от высшей (для управляющих высокоприоритетных пакетов - маршрутизация и т.п.) до низшей для пакетов, обслуживаемых по остаточному принципу.

Очереди обслуживаются последовательно, начиная с высшей. Каждая очередь содержит счетчик байт, который в начале обхода содержит заданное значение и уменьшается на размер пакета (число байт), пропущенного из этой очереди. Если счетчик не равен нулю, то пропускается следующий пакет целиком, а не его фрагмент.

# Механизмы организации очередей

**3. CBQ (Class Based Queueing)** - классовая дисциплина, предназначенная для создания сложных систем управления трафиком. Поддерживает ограничения и приоритеты. Когда трафик передается на обработку классовой дисциплине, он должен быть отнесен к одному из классов (классифицирован). Определение принадлежности пакета к тому или иному классу выполняется фильтрами.

Фильтры CBQ возвращают результат классификации (класс пакета), после чего пакет передается в очередь, соответствующую заданному классу. Каждый из классов в свою очередь может состоять из подклассов и иметь свой набор фильтров для выполнения более точной классификации своей доли трафика. В противном случае пакет обслуживается дисциплиной одной очередью класса.

Классовые дисциплины выполняют шейпинг (формирование) трафика, с целью переупорядочивания пакетов и управления скоростью их передачи. Это необходимо в случае перенаправления трафика с высокоскоростного интерфейса (например, Ethernet) на медленный (например, модем). Это позволяет различным приложениям совместно использовать одну и ту же сеть, причем каждое из них предъявляет свои специфические требования к ширине полосы или к задержке.

# Механизмы организации очередей

## 4. WFQ – Weighted Fair Queuing – Взвешенные справедливые очереди.

WFQ автоматически разбивает трафик на потоки (flows). По умолчанию их число равно 256, но может быть изменено.

Если потоков больше, чем очередей, то в одну очередь помещается несколько потоков. Принадлежность пакета к потоку (классификация) определяется на основе TOS, протокола, IP адреса источника, IP адреса назначения, порта источника или порта назначения.

Обработчик WFQ (scheduler) обеспечивает равномерное (fair - честное) разделение полосы между существующими потоками. Для этого доступная полоса делится на число потоков и каждый получает равную часть. Кроме того, каждый поток получает свой вес, пропорциональный IP приоритету (TOS), который также учитывается обработчиком.

В итоге WFQ автоматически справедливо распределяет доступную пропускную способность, дополнительно учитывая TOS.

Потоки с одинаковыми IP приоритетами TOS получают равные доли полосы пропускания; потоки с большим IP приоритетом – большую долю полосы.

В случае перегрузок ненагруженные высокоприоритетные потоки функционируют без изменений, а низкоприоритетные высоконагруженные – ограничиваются.

Вместе с WFQ работает RSVP.

По умолчанию WFQ включается на низкоскоростных интерфейсах.



# Механизмы организации очередей

## 5. CBWFQ – Class Based Weighted Fair Queuing

CBWFQ соответствует механизму обслуживания очередей на основе классов. Весь трафик разбивается на 64 класса на основании следующих параметров:

- входной интерфейс,
- аксесс лист (access list),
- протокол,
- значение DSCP,
- метка MPLS QoS и др.

Общая пропускная способность выходного интерфейса распределяется по классам.

Выделяемую каждому классу полосу пропускания можно определять как в абсолютном значении (bandwidth в kbit/s) или в процентах (bandwidth percent) относительно установленного значения на интерфейсе.

Пакеты, не попадающие в сконфигурированные классы, попадают в класс по умолчанию, который можно дополнительно настроить и который получает оставшуюся свободной полосу пропускания канала.

При переполнении очереди любого класса пакеты данного класса игнорируются.

Алгоритм отклонения пакетов внутри каждого класса можно выбирать.

Только для класса по умолчанию можно включить равномерное (честное) деление полосы.

CBWFQ поддерживает взаимодействие с RSVP.

# Механизмы организации очередей

## 6. LLQ – Low Latency Queuing

LLQ – очередность с низкой задержкой.

LLQ можно рассматривать как механизм CBWFQ с приоритетной очередью PQ (LLQ = PQ + CBWFQ).

PQ в LLQ позволяет обеспечить обслуживание чувствительного к задержке трафика.

LLQ рекомендуется в случае наличия голосового (VoIP) трафика. Кроме того, он хорошо работает с видеоконференциями.

## 7. WRED (Weighted Random Early Detection) – взвешенное случайное обнаружение.

Данный механизм широко используется протоколами Frame Relay и TCP, позволяя гибко управлять скоростью передачи путем обмена извещениями о перегрузках.

**СПАСИБО за ВНИМАНИЕ**

