Александр Александрович Олейников

Компьютерные и телекоммуникационные сети

Лекция 1.1.4. Требования предъявляемые к современным вычислительным сетям.

Астрахань, 2018

- Общее пожелание, которое можно высказать в отношении работы сети — это выполнение сетью того набора услуг, для оказания которых она предназначена: например, предоставление доступа к файловым архивам или страницам публичных Web-сайтов Internet, обмен электронной почтой в пределах предприятия или в глобальных масштабах, интерактивный обмен голосовыми сообщениями IP-телефонии и т.п.
- Все остальные требования — *производительность*, надежность, совместимость, управляемость, защищенность, *расширяемость* и *масштабируемость* — связаны с качеством выполнения этой основной задачи. И хотя все перечисленные выше требования весьма важны, часто понятие *"качество обслуживания"* (*Quality of Service*, *QoS*) компьютерной сети трактуется более узко: в него включаются только две самые важные характеристики сети — *производительность* и *надежность*.

Производительность

Потенциально высокая *производительность* — это одно из основных преимуществ распределенных систем, к которым относятся компьютерные сети. Это свойство обеспечивается принципиальной, но, к сожалению, не всегда практически реализуемой возможностью распределения работ между несколькими компьютерами сети.

Основные характеристики *производительности* сети:

- время реакции;
- скорость передачи трафика;
- пропускная способность;
- задержка передачи и вариация задержки передачи.

Время реакции сети является интегральной характеристикой *производительности*сети с точки зрения пользователя. Именно эту характеристику имеет в виду пользователь, когда говорит: "Сегодня сеть работает медленно".

- В общем случае ***время реакции*** определяется как интервал между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на него.
- Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети — загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т.п.
- Поэтому имеет смысл использовать также и средневзвешенную оценку *времени реакции* сети, усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

Время реакции сети обычно складывается из нескольких составляющих. В общем случае в него входит:

- время подготовки запросов на клиентском компьютере;
- время передачи запросов между клиентом и сервером через сегменты сети и промежуточное коммуникационное оборудование;
- время обработки запросов на сервере;
- время передачи ответов от сервера клиенту и время обработки получаемых от сервера ответов на клиентском компьютере.

Очевидно, что разложение *времени реакции* на составляющие пользователя не интересует — ему важен конечный результат. Однако для сетевого специалиста очень важно выделить из общего *времени реакции* составляющие, соответствующие этапам собственно сетевой обработки данных, — передачу данных от клиента к серверу через сегменты сети и коммуникационное оборудование.

Знание сетевых составляющих *времени реакции* позволяет оценить *производительность* отдельных элементов сети, выявить узкие места и при необходимости выполнить модернизацию сети для повышения ее общей *производительности*.

Производительность сети может характеризоваться также скоростью передачи трафика.

Скорость передачи трафика может быть *мгновенной*, *максимальной* и *средней*.

- ***средняя скорость*** вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени — час, день или неделя;
- ***мгновенная*** скорость отличается от *средней* тем, что для усреднения выбирается очень маленький промежуток времени — например, 10 мс или 1 с;
- ***максимальная*** скорость — это наибольшая скорость, зафиксированная в течение периода наблюдения.

- Чаще всего при проектировании, настройке и оптимизации сети используются такие показатели, как *средняя* и *максимальная* скорость. *Средняя* скорость, с которой обрабатывает трафик отдельный элемент или сеть в целом, позволяет оценить работу сети на протяжении длительного времени, в течение которого в силу закона больших чисел пики и спады интенсивности трафика компенсируют друг друга. *Максимальная* скорость позволяет оценить, как сеть будет справляться с пиковыми нагрузками, характерными для особых периодов работы, например в утренние часы, когда сотрудники предприятия почти одновременно регистрируются в сети и обращаются к разделяемым файлам и базам данных. Обычно при определении скоростных характеристик некоторого сегмента или устройства в передаваемых данных не выделяется трафик какого-то определенного пользователя, приложения или компьютера — подсчитывается общий объем передаваемой информации. Тем не менее, для более точной оценки качества обслуживания такая детализация желательна, и в последнее время системы управления сетями все чаще позволяют ее выполнять.

- ***Пропускная способность*** — максимально возможная скорость обработки трафика, определенная стандартом технологии, на которой построена сеть. *Пропускная способность* отражает максимально возможный объем данных, передаваемый сетью или ее частью в единицу времени.
- *Пропускная способность* уже не является, подобно *времени реакции* или скорости прохождения данных по сети, пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети — передачи пакетов данных между узлами сети через различные коммуникационные устройства. Зато она непосредственно характеризует качество выполнения основной функции сети — транспортировки сообщений — и поэтому чаще используется при анализе *производительности* сети, чем *время реакции* или скорость.
- *Пропускная способность* измеряется либо в битах в секунду, либо в пакетах в секунду.

- *Пропускная способность* сети зависит как от характеристик физической среды передачи (медный кабель, оптическое волокно, витая пара) так и от принятого способа передачи данных (технология Ethernet, FastEthernet, ATM). *Пропускная способность* часто используется в качестве характеристики не столько сети, сколько собственно технологии, на которой построена сеть. Важность этой характеристики для сетевой технологии показывает, в частности, и то, что ее значение иногда становится частью названия, например, 10 Мбит/с Ethernet, 100 Мбит/с Ethernet.
- В отличие от *времени реакции* или скорости передачи трафика *пропускная способность* не зависит от загруженности сети и имеет постоянное значение, определяемое используемыми в сети технологиями.

- На разных участках гетерогенной сети, где используется несколько разных технологий, *пропускная способность* может быть различной. Для анализа и настройки сети очень полезно знать данные о *пропускной способности* отдельных ее элементов. Важно отметить, что из-за последовательного характера передачи данных различными элементами сети *общая пропускная способность* любого составного пути в сети будет равна минимальной из *пропускных способностей* составляющих элементов маршрута. Для повышения *пропускной способности* составного пути необходимо в первую очередь обратить внимание на самые медленные элементы. Иногда полезно оперировать ***общей пропускной способностью*** сети, которая определяется как среднее количество информации, переданной между всеми узлами сети за единицу времени. Этот показатель характеризует качество сети в целом, не дифференцируя его по отдельным сегментам или устройствам.

- ***Задержка передачи*** определяется как задержка между моментом поступления данных на вход какого-либо сетевого устройства или части сети и моментом появления их на выходе этого устройства.
- Этот параметр *производительности* по смыслу близок ко *времени реакции* сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки конечными узлами сети.

- Обычно качество сети характеризуют величинами максимальной *задержки передачи* и *вариацией задержки*. Не все типы трафика чувствительны к *задержкам передачи*, во всяком случае, к тем величинам *задержек*, которые характерны для компьютерных сетей, — обычно *задержки* не превышают сотен миллисекунд, реже — нескольких секунд. Такого порядка задержки пакетов, порождаемых файловой службой, службой электронной почты или службой печати, мало влияют на качество этих служб с точки зрения пользователя сети. С другой стороны, такие же задержки пакетов, переносящих голосовые или видеоданные, могут приводить к значительному снижению качества предоставляемой пользователю информации — возникновению эффекта "эха", невозможности разобрать некоторые слова, вибрации изображения и т. п.

- Все указанные характеристики *производительности* сети достаточно независимы. В то время как *пропускная способность* сети является постоянной величиной, скорость передачи трафика может варьироваться в зависимости от загрузки сети, не превышая, конечно, предела, устанавливаемого *пропускной способностью*. Так в односегментной сети 10 Мбит/с Ethernet компьютеры могут обмениваться данными со скоростями 2 Мбит/с и 4 Мбит/с, но никогда — 12 Мбит/с.
- *Пропускная способность* и *задержки передачи* также являются независимыми параметрами, так что сеть может обладать, например, высокой *пропускной способностью*, но вносить значительные задержки при передаче каждого пакета. Пример такой ситуации дает канал связи, образованный геостационарным спутником. *Пропускная способность* этого канала может быть весьма высокой, например 2 Мбит/с, в то время как *задержка передачи* всегда составляет не менее 0,24 с, что определяется скоростью распространения электрического сигнала (около 300000 км/с) и длиной канала (72000 км).

Надежность и безопасность

Одна из первоначальных целей создания распределенных систем, к которым относятся и вычислительные сети, состояла в достижении большей надежности по сравнению с отдельными вычислительными машинами.

Важно различать несколько аспектов надежности.

Для сравнительно простых технических устройств используются такие *показатели надежности*, как:

- среднее время наработки на отказ;
- вероятность отказа;
- интенсивность отказов.

Однако эти *показатели* пригодны для оценки надежности простых элементов и устройств, которые могут находиться только в двух состояниях — работоспособном или неработоспособном. Сложные системы, состоящие из многих элементов, кроме состояний работоспособности и неработоспособности, могут иметь и другие промежуточные состояния, которые эти характеристики не учитывают.

Для оценки надежности сложных систем применяется другой набор характеристик:

- готовность или коэффициент готовности;
- сохранность данных;
- согласованность (непротиворечивость) данных;
- вероятность доставки данных;
- безопасность;
- отказоустойчивость.

Готовность или ***коэффициент готовности*** (availability) означает период времени, в течение которого система может использоваться. *Готовность* может быть повышена путем введения избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие.

- Чтобы компьютерную систему можно было считать высоконадежной, она должна как минимум обладать высокой *готовностью*, но этого недостаточно. Необходимо обеспечить *сохранность данных* и защиту их от искажений. Кроме того, должна поддерживаться *согласованность (непротиворечивость) данных*, например если для повышения надежности на нескольких файловых серверах хранится несколько копий данных, то нужно постоянно обеспечивать их идентичность.

- Так как сеть работает на основе механизма передачи пакетов между конечными узлами, одной из характеристик надежности является *вероятность доставки* пакета узлу назначения без искажений. Наряду с этой характеристикой могут использоваться и другие показатели: вероятность потери пакета (по любой из причин — из-за переполнения буфера маршрутизатора, несовпадения контрольной суммы, отсутствия работоспособного пути к узлу назначения и т. д.), вероятность искажения отдельного бита передаваемых данных, соотношение количества потерянных и доставленных пакетов.

- Другим аспектом общей надежности является ***безопасность*** (security), то есть способность системы защитить данные от несанкционированного доступа. В распределенной системе это сделать гораздо сложнее, чем в централизованной. В сетях сообщения передаются по линиям связи, часто проходящим через общедоступные помещения, в которых могут быть установлены средства прослушивания линий. Другим уязвимым местом могут стать оставленные без присмотра персональные компьютеры. Кроме того, всегда имеется потенциальная угроза взлома защиты сети от неавторизованных пользователей, если сеть имеет выходы в глобальные общедоступные сети.

- Еще одной характеристикой надежности является *отказоустойчивость* (fault tolerance). В сетях под ***отказоустойчивостью*** понимается способность системы скрыть от пользователя отказ отдельных ее элементов. Например, если копии таблицы базы данных хранятся одновременно на нескольких файловых серверах, пользователи могут просто не заметить отказа одного из них. В *отказоустойчивой* системе выход из строя одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову. Так, при отказе одного из файловых серверов в предыдущем примере увеличивается только время доступа к базе данных из-за уменьшения степени распараллеливания запросов, но в целом система будет продолжать выполнять свои функции.

Модели QoS

- Для поддержки передачи по одной сети трафика потоковых мультимедийных приложений (Voice over IP (VoIP), IPTV, видеоконференции, онлайн игры и др.) и трафика данных с различными требованиями к пропускной способности необходимы механизмы, обеспечивающие возможность дифференцирования и обработки различных типов сетевого трафика в зависимости от предъявляемых ими требований. Негарантированная доставка данных (*best effort service*), традиционно используемая в сетях, построенных на основе коммутаторов, не предполагала проведения какой-либо классификации трафика и не обеспечивала надежную доставку трафика приложений, гарантированную пропускную способность канала и определенный уровень потери пакетов. Для решения этой проблемы было введено такое понятие, как **качество обслуживания** (*Quality of Service, QoS*).

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритизации.

Можно выделить три модели реализации QoS в сети.

- **Негарантированная доставка данных (Best Effort Service)** — обеспечивает связь между узлами, но не гарантирует надежную доставку данных, время доставки, пропускную способность и определенный приоритет.
- **Интегрированные услуги (Integrated Services, IntServ)** — эта модель описана в RFC 1633 и предполагает предварительное резервирование сетевых ресурсов с целью обеспечения предсказуемого поведения сети для приложений, требующих для нормального функционирования гарантированной выделенной полосы пропускания на всем пути следования трафика. В качестве примера можно привести приложения IP-телефонии, которым для обеспечения приемлемого качества передачи голоса требуется канал с минимальной пропускной способностью 64 Кбит/с (для кодека G.711).

Модель IntServ использует сигнальный протокол RSVP (Resource Reservation Protocol, протокол резервирования ресурсов) для резервирования ресурсов для каждого потока данных, который должен поддерживаться каждым узлом на пути следования трафика. Эту модель также часто называют *жестким QoS (hard QoS)* в связи с предъявлением строгих требований к ресурсам сети.

- **Дифференцированное обслуживание (Differentiated Service, DiffServ)** – эта модель и предполагает разделение трафика на классы на основе требований к качеству обслуживания. В архитектуре DiffServ каждый передаваемый пакет снабжается информацией, на основании которой принимается решение о его продвижении на каждом промежуточном узле сети, в соответствии с политикой обслуживания трафика данного класса (Per-Hop Behavior, PHB). Модель дифференцированного обслуживания занимает промежуточное положение между негарантированной доставкой данных и моделью IntServ и сама по себе не предполагает обеспечение гарантий предоставляемых услуг, поэтому дифференцированное обслуживание часто называют *мягким QoS (soft QoS)*.

Приоритизация пакетов

- Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p. Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7 — наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	**Тег (Tag)**	Данные (Data)	Контрольная последовательность кадра (CRC)

Идентификатор протокола тега (TPID) 0x8100	**Приоритет (Priority)**	Индикатор канонического формата (CFI)	Идентификатор VLAN (VID)
16 бит	3 бита	1 бит	12 бит

Рис. 4.1. Формат кадра 802.1Q с битами приоритета 802.1p

Рис. 4.2. Байт ToS заголовка IPv4

- Для обеспечения QoS на сетевом уровне модели OSI в заголовке протокола IPv4 предусмотрено 8-битное поле ToS (Type of Service). Этот байт может быть заполнен либо значением приоритета IP Precedence, либо значением DSCP (Differentiated Services Code Point) в зависимости от решаемой задачи.
- Поле IP Precedence имеет размерность 3 бита и может принимать значения от 0 до 7. Оно используется для указания относительного приоритета обработки пакета на сетевом уровне.
- Поле DSCP было стандартизировано IETF с появлением модели DiffServ. Оно занимает 6 старших бит байта ToS и позволяют задать до 64 уровней приоритетов (от 0 до 63). По сути код DSCP является расширением 3-битового поля IP Precedence и обладает обратной совместимостью с IP-приоритетом.

Классификация пакетов

- Для обеспечения дифференцированного обслуживания трафика коммутаторы поддерживают в зависимости от модели от 4 до 8 аппаратных очередей приоритетов на каждом из своих портов. Для обеспечения требуемой очередности передачи пакетов данных в коммутаторе необходимо настроить алгоритм обслуживания очередей и карту привязки приоритетов 802.1p, ToS, DSCP к очередям.
- По умолчанию в коммутаторах D-Link используются следующие карты привязки пользовательских приоритетов 802.1p к аппаратным очередям:

• 4 очереди приоритетов

Приоритет	Номер очереди
0	Q0
1	Q0
2	Q1
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

• 8 очередей приоритетов

Приоритет	Номер очереди
0	Q0
1	Q1
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7

- **Внимание:** класс 7 в коммутаторах D-Link с поддержкой 8 очередей приоритетов зарезервирован для внутреннего использования и поэтому не настраивается.
- В коммутаторах с поддержкой 4-х очередей приоритетов очереди нумеруются от 0 до 3, где очередь 3 обладает наивысшим приоритетом, очередь 0 — низшим. В коммутаторах с поддержкой 8-ми очередей приоритетов очереди нумеруются от 0 (низший приоритет) до 7 (наивысший приоритет).
- Программное обеспечение коммутаторов позволяет настраивать карты привязки приоритетов 802.1p, ToS, DSCP к очередям в соответствии с требованиями пользователей.
- Для того чтобы поместить пакет в одну из очередей приоритетов в соответствии с заданной политикой QoS, коммутатор анализирует содержимое одного или нескольких полей его заголовка — приоритет 802.1p, IP-приоритет или поле DSCP в байте ToS. Этот процесс называется *классификацией пакетов (packet classification)*.

- Следует отметить, что при этом коммутатор не изменяет значения приоритетов внутри пакетов данных, а только определяет очередность и способ их обработки выходным портом, основываясь на реализованной в нем политике QoS.
- В том случае, если на входной порт коммутатора поступает немаркированный кадр (заголовок кадра не содержит битов приоритета), то его классификация осуществляется на основе значения приоритета 802.1p, по умолчанию назначенного данному порту.
- Также для классификации пакетов данных на основании различных параметров их заголовков, например MAC-адреса, IP-адреса, номера порта TCP/UDP, тега VLAN и т. д., могут использоваться списки управления доступом (Access Control List, ACL).

Маркировка пакетов

- После процесса классификации коммутатор может осуществить *маркировку пакетов (packet marking)*. Маркировка пакетов определяет способ записи/перезаписи значений битов приоритета (DSCP, 802.1p или IP Precedence) входящих пакетов данных. Обычно процесс маркировки выполняется на граничных устройствах и позволяет последующим коммутаторам/маршрутизаторам использовать новое значение приоритета пакета для отнесения его к одному из поддерживаемых в сети классов обслуживания. Изменить значения битов приоритета в заголовках входящих пакетов данных можно с помощью списков управления доступом.

Рис. 4.3. Маркировка пакетов

Управление перегрузками и механизмы обслуживания очередей

- Наиболее часто перегрузка сети возникает в местах соединения коммутаторами сетей с разной полосой пропускания. В случае возникновения перегрузки сети пакеты данных начинают буферизироваться и распределяться по очередям. Порядок передачи через выходной интерфейс поставленных в очередь пакетов на основе их приоритетов определяется *механизмом обслуживания очередей (Queueing mechanism)*, который позволяет управлять пропускной способностью сети при возникновении перегрузок.

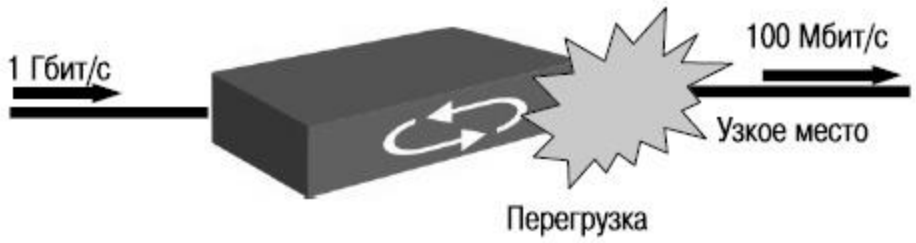

Рис. 4.4. Возникновение перегрузки в сети

Механизм управления перегрузками (*Congestion management*) включает следующие механизмы обслуживания очередей:

- механизм FIFO (First-In, First-Out);
- очереди приоритетов (Priority Queueing);
- взвешенный алгоритм кругового обслуживания (Weighted Round Robin, WRR);
- настраиваемые очереди (Custom Queueing).

В коммутаторах D-Link для обслуживания очередей используются взвешенный алгоритм кругового обслуживания, очереди приоритетов и комбинации этих методов.

Механизм обслуживания очередей FIFO ("первым пришел, первым ушел") передает пакеты, поставленные в очередь в том порядке, в котором они поступили в нее. Этот механизм не обеспечивает классификации пакетов и рассматривает их как принадлежащие одному классу.

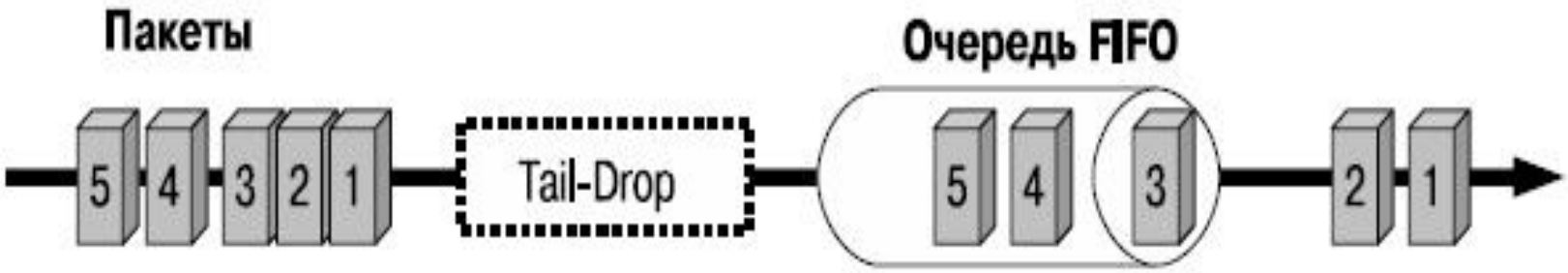

Рис. 4.5. Очередь FIFO

- *Очереди приоритетов со строгим режимом (Strict Priority Queue)* предполагают передачу трафика строго в соответствии с приоритетом выходных очередей. В этом механизме предусмотрено наличие 4-х очередей — с высоким, средним, обычным и низким приоритетами обслуживания. Пакеты, находящиеся в очереди с высоким приоритетом, обрабатываются первыми. Пакеты из следующей по приоритету обслуживания очереди начнут передаваться только после того, как опустеет высокоприоритетная очередь. Например, пакеты из средней по приоритету очереди не будут передаваться до тех пор, пока не будут обслужены пакеты из высокоприоритетной очереди. Пакеты из очереди с нормальным приоритетом не начнут передаваться до тех пор, пока не опустеет очередь со средним приоритетом и т.д.

- Следует отметить, что пакеты очереди с высоким приоритетом всегда получают предпочтение при обслуживании независимо от количества пакетов в других очередях и времени, прошедшего с момента передачи последнего пакета из очереди с низким приоритетом. В некоторых случаях это может привести к "зависанию" обслуживания низкоприоритетного трафика, т.е. пакеты из очередей с низким приоритетом долго не будут обрабатываться.
- По умолчанию на коммутаторах D-Link настроены очереди приоритетов со строгим режимом.

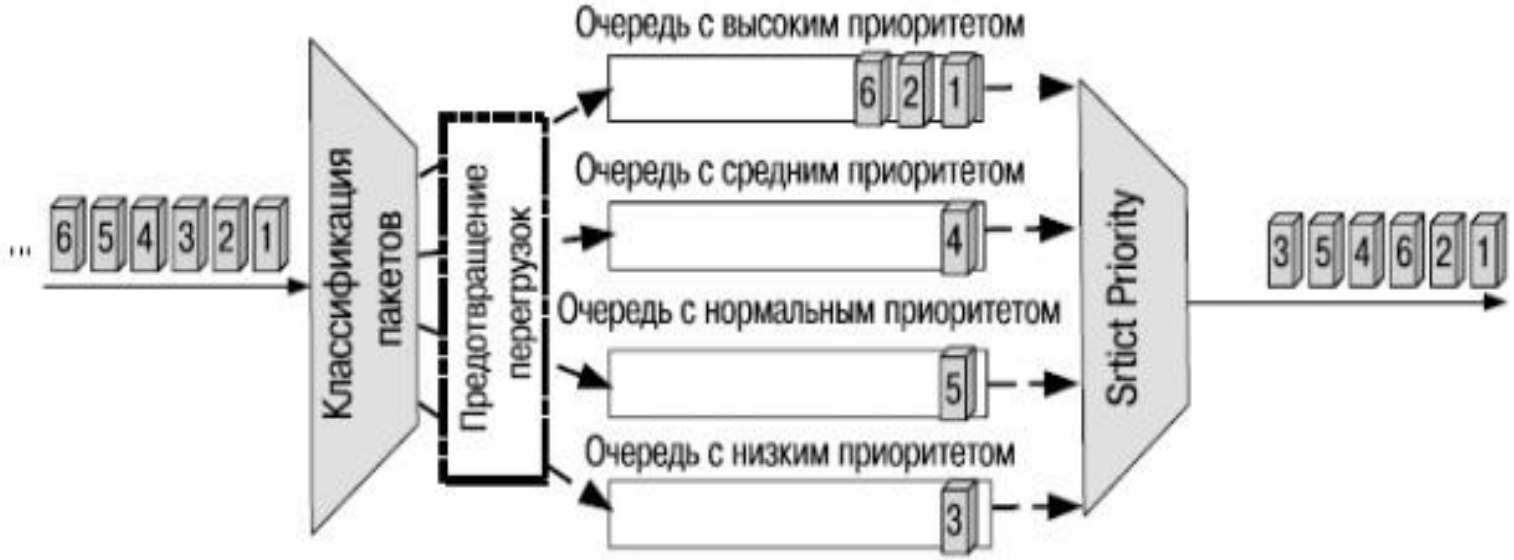

Рис. 4.6. Очереди приоритетов со строгим режимом

- Еще одним механизмом обслуживания очередей является *взвешенный алгоритм кругового обслуживания* (Weighted Round Robin, WRR). Этот механизм исключает главный недостаток очередей приоритетов, обеспечивая обработку очередей в соответствии с назначенным им весом и предоставляя полосу пропускания для пакетов из низкоприоритетных очередей.

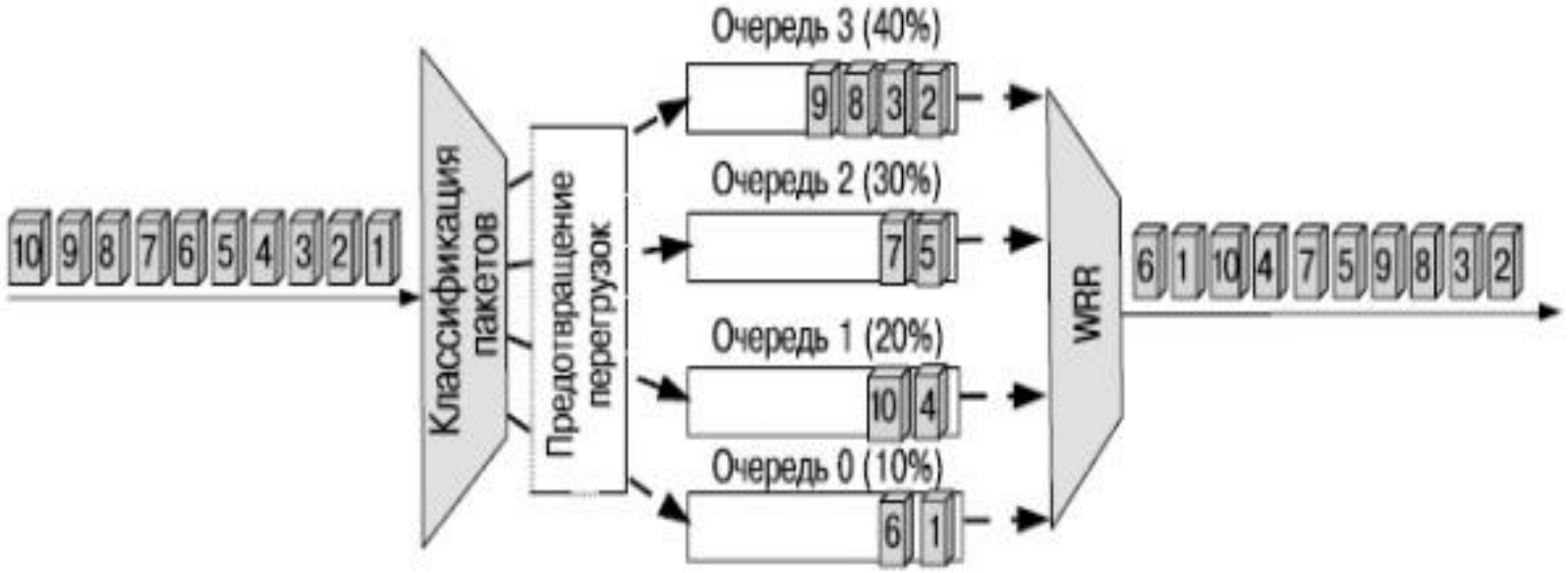

Рис. 4.7. Обслуживание очередей с использованием алгоритма WRR

- Процесс обработки очередей осуществляется по круговому принципу, начиная с самой приоритетной очереди. Из каждой непустой очереди передается некоторый объем трафика, пропорциональный назначенному ей весу, после чего выполняется переход к следующей по убыванию приоритета очереди и т.д. по кругу.

Механизм предотвращения перегрузок

- *Механизм предотвращения перегрузок (Congestion avoidance)* — это процесс выборочного отбрасывания пакетов во избежание перегрузок в сети в случае достижения выходными очередями своей максимальной длины (в пакетах).
- Традиционной политикой обработки пакетов коммутаторами в случае переполнения всех выходных очередей является их отбрасывание, которое продолжается до тех пор, пока длина очередей не уменьшится за счет передачи находящихся в них пакетов. Такой алгоритм управления длиной выходных очередей получил название *"отбрасывание хвоста" (Tail-Drop)*. Отбрасывание пакета будет служить сигналом о перегрузке сети источнику TCP-соединения, т.к. он не получит подтверждения о доставке пакета от приемника TCP-соединения. В этом случае он уменьшит скорость передачи путем уменьшения размера окна перегрузки до одного сегмента и перезапустит алгоритм *медленного старта (slow start)*.

- Поскольку коммутатор обрабатывает множество TCP-потоков в один момент времени, отбрасывание пакетов послужит сигналом о перегрузке тысячам источникам TCP-соединений, которые снизят скорость передачи. При этом почти все источники TCP-соединений будут использовать одинаковое время таймеров задержки перед началом увеличения скорости передачи. Значения этих таймеров достигнут своего лимита практически одновременно, что вызовет увеличение интенсивности трафика и переполнение очередей, которое приведет к отбрасыванию пакетов, и весь процесс повторится вновь.
- Процесс, когда каждый источник TCP-соединения уменьшает и увеличивает скорость передачи одновременно с другими источниками TCP-соединений, получил название *эффекта глобальной синхронизации (global synchronization)*. Эффект глобальной синхронизации приводит к неэффективному использованию полосы пропускания, а также к возрастанию задержки передачи пакетов.

- Для решения проблемы поведения источников TCP-соединения в момент отбрасывания пакетов был разработан *алгоритм произвольного раннего обнаружения (Random Early Detection, RED)*.
- В отличие от алгоритма "отбрасывания хвоста", алгоритм RED отбрасывает поступающие пакеты вероятностно, на основе оценки среднего размера очередей. Он не дожидается полного заполнения очередей, а начинает отбрасывать пакеты с некоторой вероятностью, когда средний размер очереди превысит определенное минимальное пороговое значение. Это позволяет избежать эффекта глобальной синхронизации, т.к. будут отбрасываться не все пакеты, а только пакеты произвольным образом выбранных потоков.

- В коммутаторах D-Link поддерживается *простой алгоритм произвольного раннего обнаружения (Simple Random Early Detection, SRED)*, который является расширенной версией алгоритма RED, реализованной на основе ASIC, и выполняет вероятностное отбрасывание входящих "окрашенных" пакетов. "Окрашивание" пакетов позволяет реализовать разные политики обслуживания пакетов (различную вероятность отбрасывания) на основе их приоритетов. Так пакеты, "окрашенные" в зеленый цвет обладают наивысшим приоритетом. Пакеты "окрашенные" в желтый цвет — средним, в красный цвет — низшим приоритетом.

- Алгоритм SRED позволяет задавать два пороговых значения размера для каждой очереди — минимальное и максимальное. Если длина очереди меньше минимального порогового значения, то пакеты будут помещаться в очередь. Если размер очереди будет находиться в интервале между минимальным и максимальным пороговыми значениями, т.е. будет наблюдаться умеренная перегрузка, то пакеты, "окрашенные" в красные и желтые цвета, будут отбрасываться с заданной вероятностью. Если длина очереди превысит максимальное пороговое значение, то пакеты любых цветов будут отбрасываться с заданной вероятностью. Т.е. алгоритм SRED обеспечивает возможность настройки более интенсивного отбрасывания пакетов низкоприоритетного трафика и менее интенсивного отбрасывания пакетов высокоприоритетного трафика.

- В коммутаторах D-Link при настройке SRED существует возможность выбора из восьми значений скоростей (вероятностей) отбрасывания пакетов:

	Скорость отбрасывания
1	100%
2	6.25%
3	3.125%
4	1.5625%
5	0.78125%
6	0.390625%
7	0.1953125%
8	0.09765625%

Контроль полосы пропускания

- Современные коммутаторы позволяют регулировать интенсивность трафика на своих портах с целью обеспечения функций качества обслуживания. Для этого они используют механизмы, называемые *Traffic Policing* (ограничение трафика) и Traffic Shaping (выравнивание трафика).

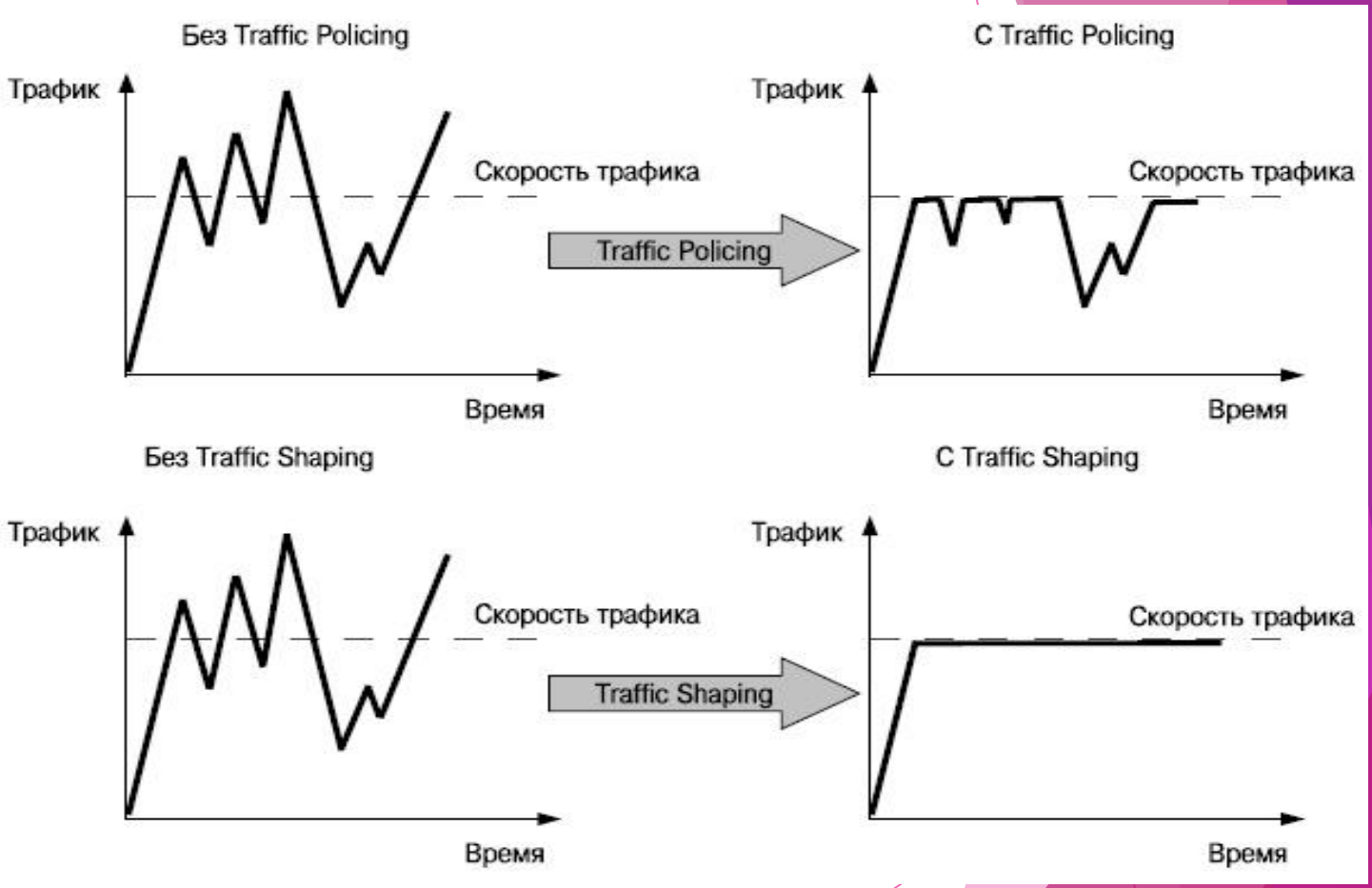

Рис. 4.8. Механизмы Traffic Policing и Traffic Shaping

- Механизм Traffic Policing служит для ограничения скорости трафика, получаемого или отправляемого с интерфейса коммутатора. Когда эта функция активна, администратор может устанавливать различные пороговые значения скорости передачи на каждом из выходных портов коммутатора. Трафик, скорость которого меньше или равна пороговому значению, будет передаваться; трафик, скорость которого превышает пороговое значение, будет обрабатываться в соответствии с настроенной политикой, например, отбрасываться или маркироваться новым значением приоритета.

Основным средством, используемым для ограничения трафика, является хорошо известный алгоритм *"корзина маркеров" (token bucket)*. Этот алгоритм предполагает наличие следующих параметров:

- **согласованная скорость передачи (Committed Information Rate, CIR)** -средняя скорость передачи трафика через интерфейс коммутатора/маршрутизатора. Этот параметр также определяет скорость помещения маркеров в корзину;
- **согласованный размер всплеска (Committed Burst Size, CBS)** — это объем трафика (в битах), на который может быть превышен размер корзины маркеров в отдельно взятый момент всплеска;
- **расширенный размер всплеска (Extended Burst Size, EBS)** — это объем трафика (в битах), на который может быть превышен размер корзины маркеров в экстренном случае.

- На рис. 4.9 показана схема реализации алгоритма "корзина маркеров" в рамках механизма Traffic Policing.
- Размер стандартной корзины маркеров (максимальное число маркеров, которое она может вместить) равен согласованному размеру всплеска (CBS). Маркеры генерируются и помещаются в корзину с определенной скоростью (CIR). Если корзина полна, то поступающие избыточные маркеры отбрасываются. Для того чтобы передать пакет из корзины вынимается число маркеров, равное размеру пакета в битах. Если маркеров в корзине достаточно, то пакет передается. Если размер пакета оказался больше, чем маркеров в корзине, то маркеры из корзины не извлекаются, а пакет рассматривается как не удовлетворяющий (non-conform) заданному профилю или избыточный. Для избыточных пакетов могут применяться различные способы обработки: они могут отбрасываться или перемаркировываться.

- Стандартная корзина маркеров не поддерживает экстренное увеличение размера всплеска, поэтому в такой реализации расширенный размер всплеска (EBS) равен согласованному размеру всплеска (CBS).
- В корзине маркеров с возможностью экстренного увеличения размера всплеска расширенный размер всплеска (EBS) больше согласованного размера всплеска (CBS). Объем трафика (в битах), на который может быть превышен размер корзины, рассчитывается по формуле:

$$CBS = 1{,}5 \times CIR/8$$
$$EBS = 2 \times CBS$$

Рис. 4.9. Алгоритм "корзина маркеров" в рамках механизма Traffic Policing

- При такой реализации корзины маркеров, в случае нехватки маркеров, необходимых для передачи пакета, учитывается расширенный размер всплеска.
- Механизм Traffic Shaping служит для сглаживания исходящего с интерфейсов коммутатора трафика. В отличие от механизма Traffic Policing, который в случае превышения скорости трафика заданного порогового значения может отбрасывать пакеты, механизм Traffic Shaping помещает избыточные пакеты в буфер.

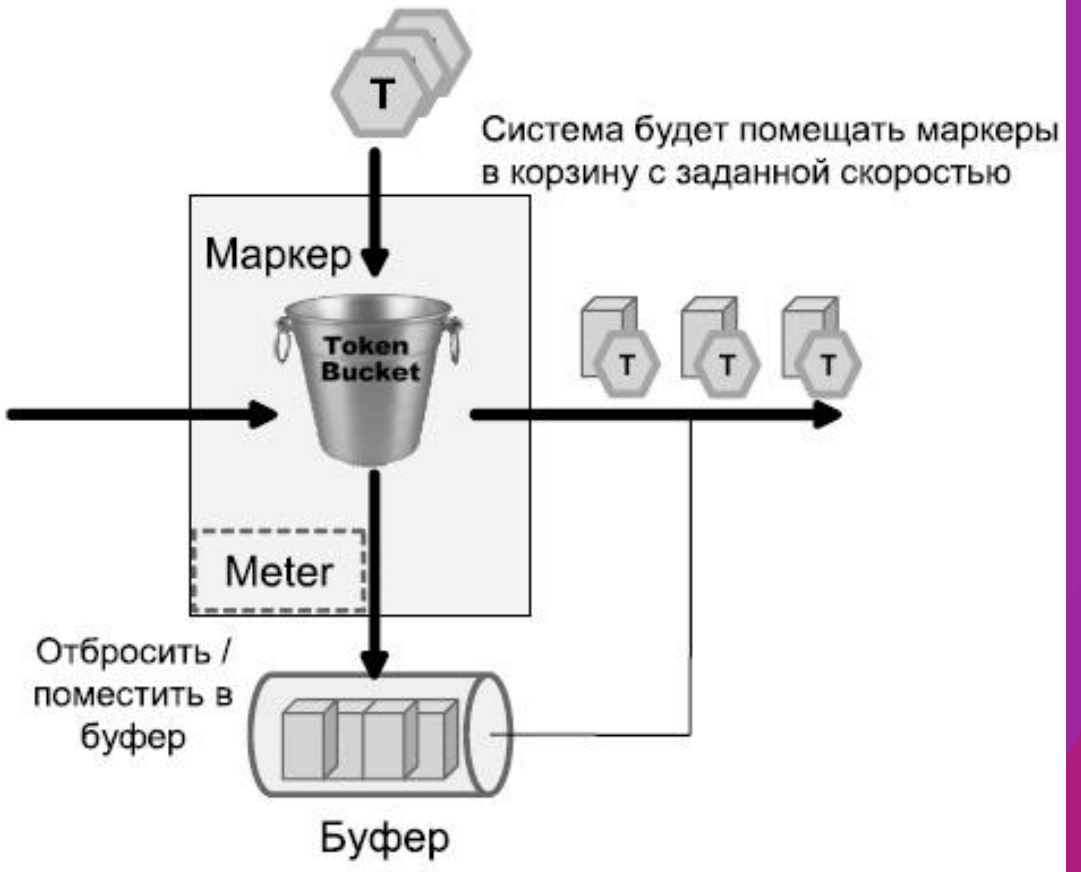

Рис. 4.10. Алгоритм "корзина маркеров"
в рамках механизма Traffic Shaping

- В качестве средства выравнивания трафика механизм Traffic Shaping также использует алгоритм "корзина маркеров". В соответствии с механизмом Traffic Shaping из корзины вынимается число маркеров, равное размеру пакета в битах. Если в корзине имелось достаточное количество маркеров, то пакет передается. В противном случае пакет маркируется как неудовлетворяющий заданному профилю и ставится в очередь (буферизируется) для последующей передачи. Как только в корзине накопится количество маркеров, достаточное для передачи пакета, он будет передан.
- Следует отметить, что механизм Traffic Shaping вносит задержку в передачу трафика, что критично для приложений, чувствительных к задержкам, таким как IP-телефония, потоковое видео и т.д. Однако этот механизм более дружествен к TCP-потокам, т.к. благодаря буферизации уменьшается количество отбрасываемых пакетов и число их повторных передач.

- Для управления полосой пропускания входящего и исходящего трафика на портах Ethernet коммутаторы D-Link поддерживают функцию Bandwidth control, которая использует для ограничения скорости механизм Traffic Policing. Администратор может вручную устанавливать требуемую скорость соединения на порте в диапазоне от 64 Кбит/с до максимально поддерживаемой скорости интерфейса с шагом 64 Кбит/с.
- В качестве примера приведем настройку ограничения скорости до 128 Кбит/с для трафика, передаваемого с интерфейса 5 коммутатора.

config bandwidth_control 5 tx_rate 128

- Более гибким решением ограничения полосы пропускания является функция per-flow Bandwidth control, реализованная на старших моделях управляемых коммутаторов D-Link. Эта функция позволяет ограничивать полосу пропускания не всему трафику, получаемому или передаваемому с интерфейса коммутатора, а конкретным потокам данных, определенным администратором сети.
- Функция per-flow Bandwidth control использует механизм списков управления доступом для просмотра определенного типа трафика и ограничения для него полосы пропускания. Весь этот процесс происходит на микросхемах портов ASIC. Таким образом, это не влияет на загрузку ЦПУ, соответственно, не снижает производительности коммутатора.

Пример настройки QoS Dlink

- На рис. 4.11 приведена схема локальной сети, в которой пользователи 1 и 3 используют приложения IP-телефонии. Голосовому трафику пользователей 1 и 3 требуется обеспечить наивысшее качество обслуживания по сравнению с трафиком других приложений, выполняемых на компьютерах остальных пользователей сети.

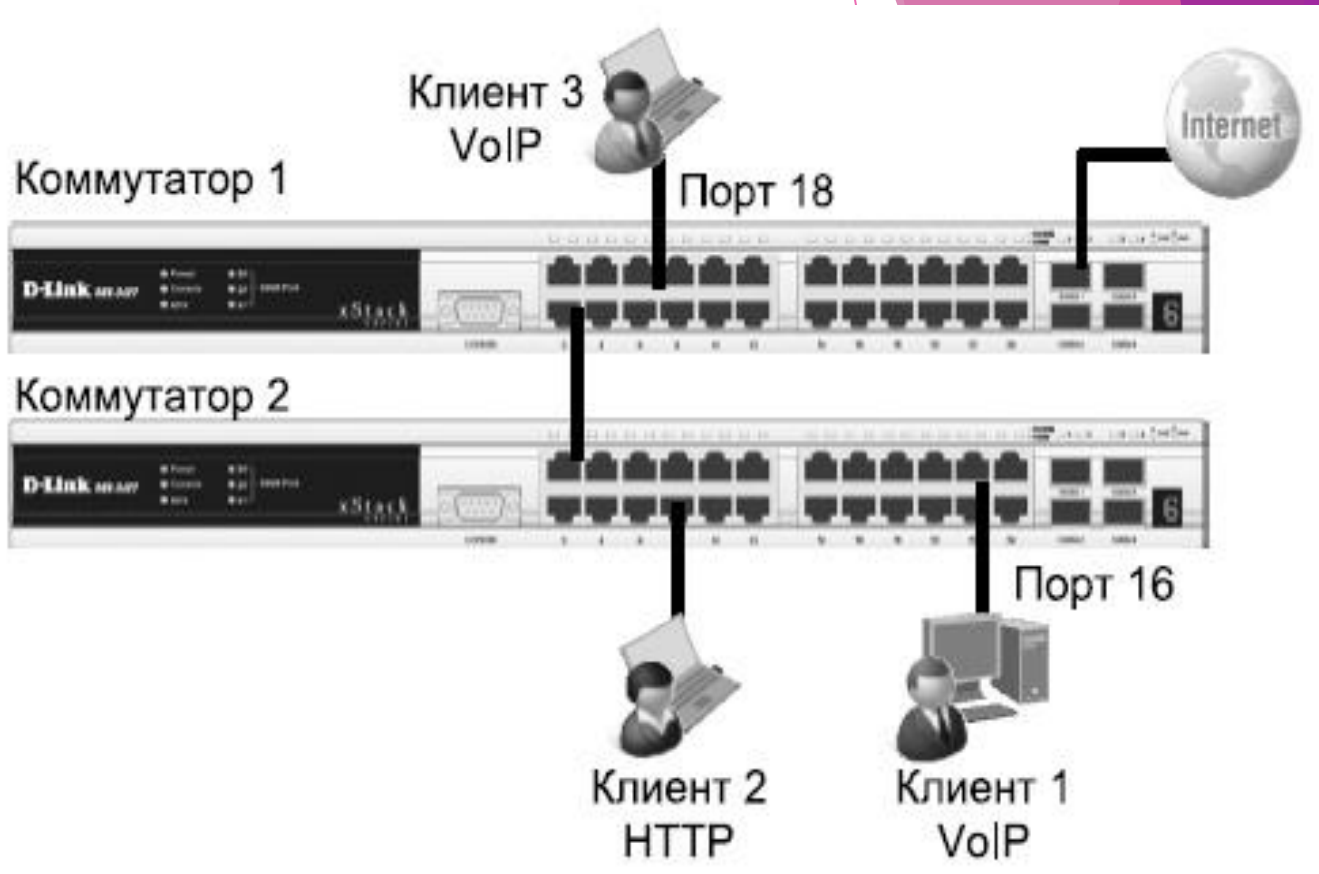

Рис. 4.11. Пример настройки QoS

Настройка коммутатора 1

- Для того чтобы внутри коммутатора могла обрабатываться информация о приоритетах 802.1p, состояние портов коммутатора, к которым подключены пользователи, необходимо перевести из "немаркированные" в "маркированные".
- config vlan default add tagged 1-6
- Изменить приоритет порта 18, к которому подключен пользователь 3, использующий приложения IP-телефонии, с 0 (установлено по умолчанию) на 7. Пакеты с приоритетом 7 будут помещаться в очередь Q6, которая имеет наивысший приоритет обработки.
- config 802.1p default_priority 18 7

Настройка коммутатора 2

- Изменить состояния портов с "немаркированные" на "маркированные"
- config vlan default add tagged 1-6
- Изменить приоритет порта 16, к которому подключен пользователь 1, использующий приложения IP-телефонии, с 0 (установлено по умолчанию) на 7. Пакеты с приоритетом 7 будут помещаться в очередь Q6, которая имеет наивысший приоритет обработки.
- config 802.1p default_priority 16 7
- Карта привязки приоритетов 802.1p к очередям и механизм обслуживания очередей не изменяются и используют параметры, настроенные по умолчанию.