

Качество обслуживания в сетях IP

В этой части...

Глава 1. Введение в качество обслуживания в сетях IP	19
Глава 2. Архитектура дифференцированных услуг	37
Глава 3. Формирование трафика на границе сети: классификация пакетов, маркировка пакетов и управление интенсивностью трафика	51
Глава 4. РНВ-политика: распределение ресурсов (часть1)	89
Глава 5. РНВ-политика: распределение ресурсов (часть2)	131
Глава 6. РНВ-политика: предотвращение перегрузки и политика отбрасывания пакетов	153
Глава 7. Интегрированные услуги: RSVP	177



В этой главе...

Уровни качества обслуживания	20
Краткий экскурс в историю возникновения и развития качества обслуживания в сетях IP	23
Характеристики производительности сетевого соединения	25
Функции качества обслуживания	28
Технологии качества обслуживания канального уровня	30
Многопротокольная коммутация меток	30
Сквозное качество обслуживания	31
Цели	32
Аудитория	32
Широта охвата и ограничения изложенного в книге материала	33
Организация книги	33

Введение в качество обслуживания в сетях IP

Вплоть до настоящего времени поставщикам услуг Internet и крупным компаниям приходилось создавать и поддерживать отдельные сети для передачи голосовой информации, видеоизображения, трафика, необходимого для решения критически важных задач, и всего остального сетевого трафика. Тем не менее нельзя не отметить сложившуюся в последнее время ярко выраженную тенденцию к объединению всех этих сетей в одну сеть с пакетной передачей данных на основе протокола Internet Protocol (IP).

Наиболее крупная IP-сеть — это, естественно, глобальная сеть Internet. За последние несколько лет рост Internet, передаваемого по Сети трафика и количества существующих Internet-приложений приблизился к экспоненциальному. В то время как Internet и корпоративные интрасети продолжают свой рост, многие аналитики предсказывают появление приложений, ориентированных на передачу нетрадиционных типов информации, — например, передачу голоса по сетям IP (Voice over IP — VoIP) или передачу трафика видеоконференций. Поскольку количество пользователей Internet и различных сетевых приложений увеличивается с каждым днем, Сеть нуждается в средствах, которые бы обеспечили поддержку как существующих, так и появляющихся приложений и служб. Тем не менее на сегодняшний день Internet может обеспечить всего лишь *негарантированную доставку данных (best effort service)*. Негарантированная доставка данных не предполагает предоставление каких-либо гарантий, касающихся времени и самого факта прибытия пакета в пункт назначения. При этом нельзя не отметить, что отбрасывание пакетов может произойти только в момент перегрузки сети. (Более подробно негарантированная доставка пакетов рассматривается в разделе “Уровни качества обслуживания” далее в этой главе.)

Как правило, передаваемые по сети пакеты различаются на основе пяти полей заголовка IP, которые однозначно определяют поток данных, — адрес источника IP-пакета, адрес назначения IP-пакета, поле протокола IP, порт источника и порт назначения. Поток информации состоит из пакетов, сгенерированных приложением, выполняющемся на компьютере-источнике, и предназначенных для передачи приложению, выполняющемся на компьютере-приемнике. Пакеты, принадлежащие одному потоку, имеют одинаковые значения всех пяти полей в заголовке IP-пакета.

С целью поддержки передачи голоса, видео и трафика данных приложений с различными требованиями к пропускной способности, системы ядра IP-сети должны обладать возможностью дифференцирования и обслуживания различных типов сетевого трафика в зависимости от предъявляемых ими требований. Негарантированная доставка данных не предполагает проведения какого-либо различия между тысячами потоков информации в ядре IP-сети. Следовательно, IP-сеть не может обеспечить никакой гарантии надежной доставки трафика приложений. Другими словами, негарантированная доставка данных препятствует передаче трафика, требующего выделения заданного минимума сетевых ресурсов и гарантии предоставления определенных услуг. Для разрешения описанной выше проблемы и было введено такое понятие, как качество обслуживания (*quality of service* — QoS) в сетях IP.

Функции *качества обслуживания в сетях IP (IP QoS)* заключаются в обеспечении гарантированного и дифференцированного обслуживания сетевого трафика путем передачи контроля за использованием ресурсов и загруженностью сети ее оператору. QoS представляет собой набор требований, предъявляемых к ресурсам сети при транспортировке потока данных. QoS обеспечивает сквозную гарантию передачи данных и основанный на системе правил контроль за средствами повышения производительности IP-сети, такими, как механизм распределения ресурсов, коммутация, маршрутизация, механизмы обслуживания очередей и механизмы отбрасывания пакетов.

Ниже перечислены некоторые из основных преимуществ качества обслуживания в сетях IP.

- Обеспечение поддержки существующих и появляющихся мультимедийных служб и приложений. Некоторые новые приложения, такие, как передача голоса по сетям IP (VoIP), предъявляют определенные требования к качеству обслуживания.
- Передача контроля за ресурсами сети и их использованием сетевому оператору.
- Обеспечение гарантии обслуживания и дифференцирование сетевого трафика. Это условие является необходимым для объединения аудио-, видеотрафика и трафика приложений в пределах одной IP-сети.
- Позволяет поставщикам услуг Internet предлагать клиентам дополнительные услуги наряду со стандартной услугой негарантированной доставки данных (другими словами, предоставлять услуги в соответствии с так называемым классом обслуживания — *Class of Service (CoS)*). Поставщик услуг Internet может определить несколько классов дополнительных услуг (например, “платиновый”, “золотой” и “серебряный” классы) и настроить сетевые правила, позволяющие обрабатывать трафик каждого класса в соответствии с заданными параметрами.
- Дает возможность организовать обслуживание сетевого трафика в зависимости от сгенерировавшего этот трафик приложения, информация о котором содержится в заголовке IP-пакета.
- Играет значительную роль в развитии новых сетевых технологий, таких, как виртуальные частные сети (*Virtual Private Networks* — VPNs).

Уровни качества обслуживания

Сетевой трафик состоит из множества потоков, сгенерированных приложениями конечных станций. Эти приложения отличаются друг от друга различными требованиями к

обслуживанию и к рабочим характеристикам сети. По сути, требование к обслуживанию каждого потока целиком и полностью определяется требованиями сгенерировавшего этот поток приложения. Следовательно, для того чтобы выяснить структуру существующих в сети запросов на качество обслуживания, необходимо определить типы сетевых приложений.

Способность сети обеспечивать различные уровни обслуживания, запрашиваемые теми или иными сетевыми приложениями, наряду с проведением контроля за характеристиками производительности — полосой пропускания, задержкой/дрожанием и потерей пакетов — может быть классифицирована по трем перечисленным ниже категориям.

- **Негарантированная доставка данных (best-effort service).** Обеспечение связности узлов сети без гарантии времени и самого факта доставки пакета в точку назначения. Следует отметить, что отбрасывание пакета может произойти только в случае переполнения буфера входной или выходной очереди маршрутизатора.

На самом деле негарантированная доставка пакетов не является частью QoS вследствие отсутствия гарантии качества обслуживания и гарантии обеспечения доставки пакетов. Следует отметить, что негарантированная доставка пакетов является на сегодняшний день единственной услугой, поддерживаемой в Internet.

Несмотря на некоторое снижение производительности, для большинства приложений, ориентированных на передачу информации (например, приложений, обеспечивающих взаимодействие по протоколу передачи файлов (File Transfer Protocol — FTP)), эта услуга является вполне достаточной. В целом же оптимальные условия функционирования всех приложений включают в себя требования к выделению определенных сетевых ресурсов в терминах полосы пропускания, задержки и уровня потери пакетов.

- **Дифференцированное обслуживание (differentiated service).** Дифференцированное обслуживание предполагает разделение трафика на классы на основе требований к качеству обслуживания. Каждый класс трафика дифференцируется и обрабатывается сетью в соответствии с заданными для этого класса механизмами QoS. Подобная схема обеспечения качества обслуживания (QoS) довольно часто называется схемой CoS.

Следует отметить, что дифференцированное обслуживание само по себе не предполагает обеспечения гарантий предоставляемых услуг. В соответствии с данной схемой трафик распределяется по классам, каждый из которых имеет свой собственный приоритет. По этой причине дифференцированное обслуживание довольно часто называют *мягким QoS (soft QoS)*.

Дифференцированное обслуживание удобно применять в сетях с интенсивным трафиком приложений. В этом случае важно обеспечить отделение административного трафика сети от всего остального трафика и назначить ему приоритет, позволяющий в любой момент времени быть уверенным в связности узлов сети.

- **Гарантированное обслуживание (guaranteed service).** Гарантированное обслуживание предполагает резервирование сетевых ресурсов с целью удовлетворения специфических требований к обслуживанию со стороны потоков трафика.

В соответствии с гарантированным обслуживанием выполняется предварительное резервирование сетевых ресурсов по всей траектории движения трафика. Гаран-

тированное обслуживание довольно часто называют еще *жестким QoS (hard QoS)* в связи с предъявлением строгих требований к ресурсам сети.

К сожалению, резервирование ресурсов на всем пути следования отдельных потоков трафика невозможно реализовать в масштабах магистральной сети Internet, обслуживающей в отдельный момент времени тысячи потоков данных. Исправить положение призвано агрегированное резервирование ресурсов, требующее хранения в базовых маршрутизаторах Internet всего лишь небольшого количества информации.

Приложения, требующие гарантированного обслуживания, включают в себя мультимедийные приложения, проводящие передачу голосовой информации и видеоизображений. Интерактивные приложения, ориентированные на передачу речи по Internet, могут функционировать нормально (т.е. не вызывая неудобств у пользователей) лишь в том случае, если значение латентности равно или меньше 100 мс. Следует отметить, что аналогичный уровень латентности является приемлемым для большинства мультимедийных приложений. А вот приложениям Internet-телефонии уже понадобится канал передачи информации с пропускной способностью как минимум 8 Кбит/с и со значением задержки подтверждения приема, равном 100 мс. Для того чтобы удовлетворить подобные требования к гарантированному обслуживанию, сеть должна обладать определенным запасом ресурсов.

Качество обслуживания уровня 2 эталонной модели OSI (Layer 2 QoS) включает в себя все механизмы QoS, предусмотренные различными технологиями канального уровня или технологиями, объектом которых этот уровень является. Более подробно качество обслуживания уровня 2 эталонной модели OSI рассматривается в главе 8, "Качество обслуживания на уровне 2: межсетевой обмен с IP QoS", далее в этой книге. Качество обслуживания уровня 3 эталонной модели OSI (Layer 3 QoS) включает в себя все механизмы QoS, предусмотренные на сетевом уровне (уровне протокола IP). В табл. 1.1 перечислены три уровня обслуживания и соответствующие им разрешающие функции QoS канального и сетевого уровней эталонной модели OSI. Более подробно эти функции рассматриваются в оставшейся части книги.

Таблица 1.1. Уровни обслуживания и соответствующие им разрешающие функции QoS

Уровень обслуживания	Разрешающая функция QoS сетевого уровня	Разрешающая функция QoS канального уровня
Негарантированная доставка пакетов	Связность узлов сети	Технология асинхронной передачи данных (Asynchronous Transfer Mode — ATM), обслуживание с неопределенной битовой скоростью (Unspecified Bit Rate — UBR), механизм согласования скорости передачи информации (Committed Information Rate — CIR) в сетях Frame Relay

Уровень обслуживания	Разрешающая функция QoS сетевого уровня	Разрешающая функция QoS канального уровня
Дифференцированное обслуживание	Механизм согласования скорости доступа (Committed Access Rate — CAR) CoS, взвешенный алгоритм равномерного обслуживания очередей (Weighted Fair Queuing — WFQ), взвешенный алгоритм произвольного раннего обнаружения (Weighted Random Early Detection — WRED)	IEEE 802.1p
Гарантированное обслуживание	Протокол резервирования ресурсов (Resource Reservation Protocol — RSVP)	Диспетчер пропускной способности подсети (Subnet Bandwidth Manager — SBM), механизм обслуживания с постоянной битовой скоростью (Constant Bit Rate — CBR) в сетях ATM, механизм согласования скорости передачи информации (CIR) в сетях Frame Relay

Краткий экскурс в историю возникновения и развития качества обслуживания в сетях IP

Качество обслуживания в сетях IP не является чьей-то блестящей идеей, возникшей на протяжении нескольких последних лет. Отцы-основатели Internet предвидели эту потребность и предусмотрели байт типа обслуживания (Type of Service — ToS) в заголовке IP-пакета. Следовательно, возможность реализации качества обслуживания была заложена еще в начальной спецификации протокола IP. Ниже приведена выдержка из спецификации протокола IP, в которой описывается предназначение байта ToS.

“Байт типа обслуживания (Type of Service — ToS) используется для указания абстрактных параметров требуемого качества обслуживания. На основании этих параметров производится выбор реальных характеристик механизмов обслуживания при передаче датаграммы через заданную сеть.”¹

Вплоть до конца 80-х годов Internet пребывала в “зародышевом” состоянии, что характеризовалось низким объемом трафика и малым числом используемых сетевых приложений. Следовательно, поддержкой байта ToS можно было пренебречь, что и сделано практически во всех реализациях протокола IP. IP-приложения не производили установку значения байта ToS, а маршрутизаторы игнорировали его при принятии решения о продвижении IP-пакета.

Важность внедрения механизма QoS в масштабах Internet возросла благодаря увеличению популярности Сети и приобретению ею коммерческих черт. Функционирование Internet базируется на сквозном режиме обслуживания пакетов данных без ориентации на установку соединения, который подразумевает негарантированную доставку информации

¹ RFC 791: Internet Protocol Specification/Postel J., 1981.

с использованием для этого связки из двух протоколов — протокола управления передачей (Transmission Control Protocol — TCP) и протокола Internet (Internet Protocol — IP), более известную как TCP/IP. Несмотря на то что отсутствие ориентации на установку соединения делает Internet более гибкой и устойчивой к сбоям, динамика передаваемых потоков данных делает ее склонной к перегрузкам, которые чаще всего возникают в местах стыка двух сетей со значительно различающимися пропускными способностями. Проблема снижения работоспособности TCP/IP сетей в моменты перегрузки была рассмотрена Джоном Наглем (John Nagle) в середине 80-х годов прошлого столетия².

Первоначально функции качества обслуживания были возложены на узлы Internet. Одна из наиболее серьезных проблем, касающаяся дорогостоящих каналов передачи информации глобальных сетей (Wide-Area Network — WAN), заключалась в их чрезмерной перегрузке пакетами протокола TCP, имеющими небольшой объем и сгенерированными такими приложениями, как *telnet* и *rlogin*. Алгоритм Нагля, призванный решить эту проблему, реализован сегодня во всем программном обеспечении, установленном в узлах Internet и поддерживающем протокол IP³. Можно сказать, что алгоритм Нагля “возвестил” о начале эпохи качества обслуживания в сетях IP.

В 1986 году Ван Якобсон (Van Jacobson) разработал следующий набор функций Internet QoS для конечных систем — механизмы предотвращения перегрузки, являющиеся стандартом де-факто для всех современных реализаций TCP. Следует отметить, что эти механизмы (механизм медленного старта и механизм предотвращения перегрузки) играют огромную роль в предупреждении критического снижения работоспособности сети в сегодняшней Internet. Ответственными за реагирование на сигналы о перегрузке сети (которыми служат отброшенные пакеты) являются потоки трафика TCP. В 1990 году для обеспечения оптимальной производительности сети в моменты потери пакетов были разработаны два дополнительных механизма — механизм быстрой повторной передачи и механизм быстрого восстановления⁴.

Несмотря на то что реализация механизмов QoS в конечных системах является необходимым условием, она не позволяет говорить о сквозном качестве обслуживания до тех пор, пока соответствующие механизмы не будут реализованы в маршрутизаторах — устройствах, ответственных за передачу трафика между конечными системами. Следовательно, с 1990-х годов акцент в разработке механизмов QoS вполне логично переместился на исследование возможности реализации функций качества обслуживания в маршрутизаторах. Маршрутизаторы, поддерживающие только один механизм обслуживания очередей — “первым пришел, первым обслужен” (first-in, first-out — FIFO), — не способны обеспечить дифференцирование потоков трафика на основе их приоритета на уровне алгоритма планирования очередей. Более того, обслуживание очередей по методу FIFO приводит к отбрасыванию пакетов и не способно защитить потоки с предсказуемым поведением от “шалунов”. Решить данную проблему на уровне магистрали Internet были призваны алгоритм обслуживания очередей WFQ (Weighted Fair Queuing — взвешенный алгоритм равномерного обслуживания очередей)⁵ и алгоритм управления очередями

² RFC 896: *Congestion Control in IP/TCP Internetworks/Nagle J., 1984*

³ RFC 1122: *Requirements for Internet Hosts— Communication Layers/Braden R., 1989.*

⁴ RFC 2001: *TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms/Stevens W., 1997.*

⁵ Demers A., Keshav S., Shenkar S. *Design and Analysis of a Fair Queuing Algorithm.* — In: *Proceedings of ACM SIGCOMM'89, Austin, TX, September 1989.*

WRED (Weighted Random Early Detection — взвешенный алгоритм произвольного раннего обнаружения)⁶.

Разработка механизмов QoS продолжилась попытками стандартизации функций сквозного качества обслуживания в масштабах Internet. Целью рабочей группы IETF по созданию интегрированных услуг (Integrated Services (intserv) Internet Engineering Task Force (IETF) Working Group)⁷ является обеспечение приложений средствами формулирования требований к ресурсам при сквозном обслуживании, а также разработка соответствующих механизмов на уровне маршрутизаторов и технологий подсетей. Используемым в этих целях сигнальным протоколом является протокол RSVP (Resource Reservation Protocol — протокол резервирования ресурсов). В соответствии с моделью intserv обслуживание каждого потока трафика производится на всей траектории соединения, что серьезно затрудняет использование этой модели в масштабах магистральной Internet, обрабатываемой в каждый момент времени тысячи потоков информации. Более подробно протокол RSVP и типы обслуживания intserv рассматриваются в главе 7, “Интегрированные услуги: RSVP”, далее в этой книге.

Несмотря на то что байт заголовка IP-пакета ToS до недавнего времени практически не использовался, сейчас это один из самых распространенных методов определения требований к качеству обслуживания. Байт ToS представляет собой главный механизм обеспечения услуг diffserv в масштабах Internet, что подвигло рабочую группу IETF по созданию дифференцированных услуг (IETF differentiated services (diffserv) Working Group)⁸ предложить стандартизировать этот байт в качестве байта diffserv. Более подробно архитектура diffserv рассматривается в главе 2, “Архитектура дифференцированных услуг”, далее в этой книге.

Характеристики производительности сетевого соединения

Внедрение механизмов QoS предполагает обеспечение со стороны сети соединения с определенными ограничениями по производительности. Основными характеристиками производительности сетевого соединения являются полоса пропускания, задержка, дрожание и уровень потери пакетов. Более подробно все упомянутые характеристики производительности рассматриваются в следующих разделах этой главы.

Полоса пропускания

Термин *полоса пропускания* (*bandwidth*) используется для описания номинальной пропускной способности среды передачи информации, протокола или соединения. Этот термин достаточно эффективно определяет “ширину канала”, требующуюся приложению для взаимодействия по сети.

Как правило, каждое соединение, нуждающееся в гарантированном качестве обслуживания, требует от сети резервирования минимальной полосы пропускания. К примеру, приложения, ориентированные на передачу оцифрованной речи, создают по-

⁶ Floyd S., Jacobson V. *Random Early Detection Gateways for Congestion Avoidance*. — IEEE/ACM Transactions on Networking August 1993.

⁷ IETF Intserv Working Group, www.ietf.org/html.charters/intserv-charter.html

ток информации интенсивностью 64 Кбит/с. Эффективное использование таких приложений становится практически невозможным вследствие снижения полосы пропускания ниже 64 Кбит/с на каком-либо из участков соединения.

Задержка и дрожание при передаче пакетов

Задержка при передаче пакета (packet delay), или *латентность (latency)*, на каждом переходе состоит из задержки сериализации, задержки распространения и задержки коммутации. Ниже приведены определения каждого из названных выше типов задержки.

- **Задержка сериализации (serialization delay).** Время, которое требуется устройству на передачу пакета при заданной ширине полосы пропускания. Задержка сериализации зависит как от ширины полосы пропускания канала передачи информации, так и от размера передаваемого пакета. Например, передача пакета размером 64 байт при заданной полосе пропускания 3 Мбит/с занимает всего лишь 171 нс. Обратите внимание, что задержка сериализации очень сильно зависит от полосы пропускания: передача того же самого пакета размером 64 байт при заданной полосе пропускания 19.2 Кбит/с занимает уже 26 мс. Довольно часто задержку сериализации называют еще *задержкой передачи (transmission delay)*.
- **Задержка распространения (propagation delay).** Время, которое требуется переданному биту информации для достижения принимающего устройства на другом конце канала. Эта величина довольно существенна, поскольку в наилучшем случае скорость передачи информации соизмерима со скоростью света. Обратите внимание, что задержка распространения зависит от расстояния и используемой среды передачи информации, а не от полосы пропускания. Для линий связи глобальных сетей задержка распространения измеряется в миллисекундах. Для трансконтинентальных сетей Соединенных Штатов характерна задержка распространения порядка 30 мс.
- **Задержка коммутации (switching delay).** Время, которое требуется устройству, получившему пакет, для начала его передачи следующему устройству. Как правило, это значение меньше 10 нс.

Обычно каждый из пакетов, принадлежащий одному и тому же потоку трафика, передается с различным значением задержки. Задержка при передаче пакетов меняется в зависимости от состояния промежуточных сетей.

В том случае, если сеть не испытывает перегрузки, пакеты не ставятся в очередь в маршрутизаторах, а общее время задержки при передаче пакета состоит из суммы задержки сериализации и задержки распространения на каждом промежуточном переходе. В этом случае можно говорить о минимально возможной задержке при передаче пакетов через заданную сеть. Следует отметить, что задержка сериализации становится незначительной по сравнению с задержкой распространения при передаче пакета по каналу с большой пропускной способностью.

Если же сеть перегружена, задержки при организации очередей в маршрутизаторах начинают влиять на общую задержку при передаче пакетов и приводят к возникновению разницы в задержке при передаче различных пакетов одного и того же потока. Колебание

⁸ IETF DiffServ Working Group, www.ietf.org/html.charters/diffserv-charter.html

задержки при передаче пакетов получило название *дрожания при передаче пакетов (packet jitter)*.

Дрожание пакетов имеет большую важность, поскольку именно оно определяет максимальную задержку при приеме пакетов в конечном пункте назначения. Принимающая сторона, в зависимости от типа используемого приложения, может попытаться компенсировать дрожание пакетов за счет организации приемного буфера для хранения принятых пакетов на время, меньшее или равное верхней границе дрожания. К этой категории относятся приложения, ориентированные на передачу/прием непрерывных потоков данных, например Internet-телефония или приложения, обеспечивающие проведение видеоконференций.

На рис. 1.1 проиллюстрировано влияние задержки сериализации, задержки распространения и задержки коммутации на общую задержку при передаче пакетов в зависимости от возрастания полосы пропускания канала.

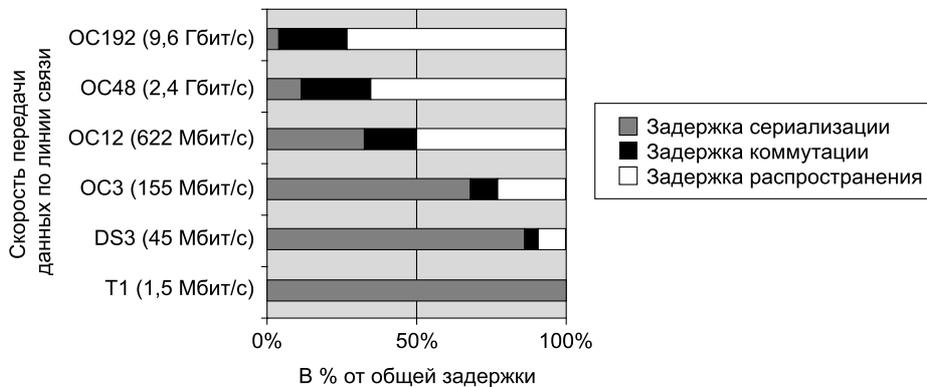


Рис. 1.1. Структура общей задержки при передаче пакета размером 1500 байт по трансконтинентальному каналу Соединенных Штатов в зависимости от возрастания полосы пропускания

Обратите внимание, что задержка сериализации становится незначительной по сравнению с задержкой распространения по мере увеличения полосы пропускания канала. Задержка коммутации пренебрежимо мала в случае отсутствия пакетов в очередях маршрутизаторов, однако склонна к существенному увеличению при росте размеров очередей.

Потеря пакетов

Уровень *потери пакетов (packet loss)* определяет количество пакетов, отбрасываемых сетью во время передачи. Основными причинами потери пакетов являются перегрузка сети и повреждение пакетов во время передачи по линии связи. Чаще всего отбрасывание пакетов происходит в местах перегрузки, где число поступающих пакетов намного превышает верхнюю границу размера выходной очереди. Кроме того, отбрасывание пакетов может быть вызвано недостаточным размером входного буфера. Как правило, уровень потери пакетов выражается как доля отброшенных пакетов за определенный интервал времени.

Некоторые приложения не способны нормально функционировать или же функционируют крайне неэффективно в случае потери пакетов. Подобные приложения требуют от сети гарантии надежной доставки всех пакетов.

Как правило, хорошо спроектированные сети характеризуются очень низким значением потери пакетов. Потеря пакетов также несвойственна приложениям, для которых были заранее зарезервированы требуемые этими приложениями ресурсы. Что касается волоконно-оптических линий связи со значением частоты появления ошибочных битов (Bit Error Rate — BER) $10E-9$, то здесь потеря пакетов возможна только в случае их отбрасывания в местах перегрузки сети. Отбрасывание пакетов, к сожалению, является неизбежным явлением при негарантированной доставке трафика, хотя и в этом случае оно обуславливается крайней необходимостью. Следует отметить, что отброшенные пакеты указывают на неэффективное использование ресурсов сети, часть которых была потрачена на доставку пакетов в точку, где они были потеряны.

Функции качества обслуживания

В данном разделе приводится краткое описание различных функций качества обслуживания, связанных с ними возможностей и преимуществ. Более подробно каждая из упомянутых здесь функций QoS рассматривается в оставшейся части этой книги.

Классификация и маркировка пакетов

Маршрутизаторы, расположенные на границе сети, используют функцию классификации для распознавания пакетов, принадлежащих различным классам трафика, в зависимости от значения одного или нескольких полей в заголовке TCP/IP. Функция маркировки пакетов используется для разметки классифицированного трафика путем установки значения поля IP-приоритета или поля кода дифференцированного обслуживания (Differentiated Services Code Point — DSCP).

Более подробно функции классификации и маркировки пакетов рассматриваются в главе 3, “Формирование трафика на границе сети: классификация пакетов, маркировка пакетов и управление интенсивностью трафика”, далее в этой книге.

Управление интенсивностью трафика

Поставщики услуг используют ограничивающую функцию для приведения параметров поступающего в сеть клиентского трафика в соответствие с его профилем. В то же время, корпорации используют выравнивающую функцию для дозирования поступающего в сеть поставщика услуг трафика и выравнивания его интенсивности в соответствии с заданным профилем. Наиболее распространенной схемой дозирования трафика является так называемая схема *корзины маркеров* (*token bucket*).

Более подробно эта функция качества обслуживания рассматривается в главе 3, “Формирование трафика на границе сети: классификация пакетов, маркировка пакетов и управление интенсивностью трафика”, далее в этой книге.

Распределение ресурсов

Наиболее распространенным механизмом обслуживания очередей в маршрутизаторах и коммутаторах современной Internet является ставший уже традиционным механизм

“первым пришел, первым обслужен” (first-in, first-out — FIFO). Несмотря на простоту реализации, для механизма FIFO характерно несколько фундаментальных проблем, затрудняющих выполнение функций качества обслуживания. Так, механизм FIFO не предусматривает приоритетной обработки чувствительного к задержке трафика путем его перемещения во главу очереди. Весь трафик обрабатывается одинаково, без учета принадлежности потоков к различным классам с разными требованиями к обслуживанию.

Минимальное требование, предъявляемое к поддерживающему функции QoS алгоритму обслуживания очередей, — способность дифференцировать и определять требования к обработке различных пакетов. В соответствии с этими параметрами алгоритм обслуживания должен планировать порядок передачи поставленных в очередь пакетов. Частота обслуживания пакетов одного и того же потока трафика определяет выделенную этому потоку полосу пропускания.

Более подробно функция распределения ресурсов рассматриваются в главе 4, “РНВ-политика: распределение ресурсов (часть 1)”, далее в этой книге.

Предотвращение перегрузки и политика отбрасывания пакетов

Традиционный механизм обслуживания очередей FIFO предусматривает отбрасывание всех входящих пакетов после достижения максимального значения длины очереди. Подобный способ управления очередью получил название “отбрасывание хвоста” (*tail drop*) и характеризуется тем, что сигнал о перегрузке поступает лишь в момент фактического переполнения очереди. К сожалению, механизм FIFO не предусматривает проведения каких-либо активных действий по предотвращению перегрузки или по уменьшению размера очереди с целью снижения времени задержки. Активный алгоритм управления очередями позволяет маршрутизатору предвидеть перегрузку еще до переполнения очереди.

Более подробно механизм предотвращения перегрузки и политика отбрасывания пакетов рассматривается в главе 6, “РНВ-политика: предотвращение перегрузки и политика отбрасывания пакетов”, далее в этой книге.

Сигнальный протокол QoS

Сигнальный протокол RSVP является частью разработанной организацией IETF архитектуры *intserv*, обеспечивающей предоставление сквозных услуг QoS в масштабах Internet. Протокол RSVP позволяет приложениям сообщать о требованиях к обслуживанию отдельных потоков трафика. Для определения количественных показателей качества обслуживания с целью управления доступом протокол RSVP использует служебные параметры.

Более подробно сигнальный протокол RSVP рассматривается в главе 7, “Интегрированные услуги: RSVP”, далее в этой книге.

Коммутация

Главная функция маршрутизатора заключается в быстрой и эффективной коммутации входящего трафика на соответствующие выходные интерфейсы согласно информации, хранящейся в таблице продвижения пакетов. Традиционный механизм продвижения пакетов, несмотря на его эффективность, обладает низкой масштабируемостью; кроме того,

его производительность оставляет желать лучшего в периоды нестабильного функционирования сети, что выражается в резком увеличении расходов на обслуживание кэша и снижении эффективности коммутации пакетов.

Метод продвижения пакетов, учитывающий топологию сети, обладает бесспорными преимуществами перед методом, базирующимся на кэшировании пакетов, что обусловлено совпадением таблицы продвижения пакетов с таблицей маршрутизации. Механизм продвижения пакетов, учитывающий топологию сети, называется также методом скоростной коммутации пакетов Cisco (Cisco Express Forwarding — CEF). Более подробно различные механизмы коммутации пакетов рассматриваются в приложении Б, “Механизмы коммутации пакетов”, далее в этой книге.

Маршрутизация

Традиционная маршрутизация осуществляется на основании адреса назначения пакета и предполагает выбор наименее короткого маршрута, хранящегося в таблице маршрутизации. К сожалению, подобный механизм является недостаточно гибким для некоторых сетевых сценариев. Маршрутизация на основе политики — это функция качества обслуживания, позволяющая заменить традиционный механизм маршрутизации пакетов механизмом, учитывающим всевозможные настраиваемые пользователем параметры.

Современные протоколы маршрутизации, работающие по методу выбора наименее короткого пути, позволяют учитывать такие значения метрики, как административное расстояние, вес или число переходов. Маршрутизация пакетов осуществляется на основании хранящейся в таблице маршрутизации информации без учета требований потока трафика к качеству обслуживания или доступности сетевых ресурсов на всем протяжении маршрута. QoS-маршрутизация представляет собой механизм маршрутизации пакетов, учитывающий требования потоков трафика к качеству обслуживания и осуществляющий выбор маршрута в зависимости от наличия сетевых ресурсов.

Более подробно маршрутизация на основе политики рассматривается в приложении В, “Политики маршрутизации”, далее в этой книге.

Технологии качества обслуживания канального уровня

Поддержка функций качества обслуживания реализована в некоторых технологиях уровня 2 эталонной модели OSI, включая технологии ATM, Frame Relay, Token Ring и, в последнее время, коммутируемые локальные сети (LAN) семейства Ethernet. Как технология, ориентированная на установку соединения, ATM предлагает наиболее полную поддержку функций QoS с возможностью обеспечения гарантии качества обслуживания для отдельного соединения. С учетом этого узел, запрашивающий соединение, может включить в свой запрос требования к качеству обслуживания и быть уверенным в том, что сеть будет предоставлять ему соответствующие услуги в течение всего времени существования данного соединения. Сети Frame Relay способны обеспечить соединение с минимальным значением CIR, поддерживаемым даже в периоды перегрузки сети. Технология Token Ring и более поздний стандарт IEEE (Institute of Electrical and Electronic Engineers) 802.1p также обладают механизмами дифференцированного обслуживания.

Если функции качества обслуживания необходимо обеспечить в пределах подсети или облака WAN, то перечисленные выше технологии канального уровня (в особенности ATM) способны полностью оправдать возложенное на них доверие. Однако ни ATM, ни какая-либо другая технология уровня 2 эталонной модели OSI не могут быть всеобъемлющим решением для более крупных сетей, таких, как Internet.

Многопротокольная коммутация меток

Рабочая группа по созданию и внедрению технологии многопротокольной коммутации меток (Multiprotocol Label Switching (MPLS) Working Group)⁹ занимается стандартизацией базовой технологии, предполагающей применение механизма продвижения пакетов на основе замены меток (метод коммутации меток) и использующейся совместно с маршрутизацией сетевого уровня. Целью рабочей группы является разработка механизмов совместного использования технологии многопротокольной коммутации меток с различными технологиями канального уровня, включая Packet-over-Sonet, Frame Relay, ATM и Ethernet со скоростью передачи данных 10, 100 и 1000 Мбит/с. Стандарт MPLS базируется на механизме коммутации тэгов (tag switching), разработанном компанией Cisco Systems.

В числе других преимуществ технология MPLS позволяет достичь большей гибкости в предоставлении услуг QoS и управлении трафиком. Для идентификации потока трафика с определенными требованиями к качеству обслуживания используются метки, которые, кроме всего прочего, позволяют проводить выбор оптимизированного пути передачи пакета. Технология MPLS, виртуальные частные сети (VPNs) на основе технологии MPLS и управление трафиком в сетях MPLS нашли свое применение преимущественно в сетях поставщиков услуг. Более подробно многопротокольная коммутация меток и качество обслуживания в сетях MPLS рассматриваются в главе 9, “Качество обслуживания в сетях MPLS”, а управление трафиком в сетях MPLS — в главе 10, “Управление трафиком в сетях MPLS”, далее в этой книге.

Сквозное качество обслуживания

Технологии QoS уровня 2 эталонной модели OSI способны стать полноценным решением лишь в сетях ограниченного размера и не могут быть применены для обеспечения сквозного качества обслуживания в Internet и других крупных сетях IP в силу того, что эти сети состоят из множества сегментов, построенных на базе различных технологий канального уровня. В общем виде сквозное взаимодействие в сети начинается с уровня 3 эталонной модели OSI и, следовательно, только протокол сетевого уровня (каковым является протокол IP в Internet) может обеспечить предоставление сквозных услуг QoS.

В Internet применяются различные технологии канального уровня и различные линии связи. С целью реализации сквозного качества обслуживания протокол IP, обеспечивая сквозное взаимодействие узлов, должен установить соответствие между функциями QoS сетевого уровня и механизмами QoS канального уровня (особенно в коммутируемых сетях).

Магистралей некоторых поставщиков услуг построены на базе таких технологий коммутируемых сетей, как ATM или Frame Relay. В этом случае для обеспечения сквозного ка-

⁹ IETF MPLS Working Group, www.ietf.org/html.charters/mpls-charter.html

чества обслуживания сетевым инженерам придется организовать взаимодействие механизмов QoS канального уровня сетей ATM или Frame Relay и протокола IP. Это позволит проводить корректную обработку запросов к обслуживанию QoS сетевого уровня облаком ATM или Frame Relay.

Коммутируемые локальные сети являются неотъемлемой частью сетей поставщиков услуг Internet (Internet Service Provider — ISP), предоставляющих услуги по размещению Web-сайтов и обеспечивающих функционирование корпоративных интрасетей. Дифференцирование трафика в коммутируемых сетях предусматривается протоколами IEEE 802.1p и IEEE 802.1Q. Следовательно, для обеспечения в сети сквозного качества обслуживания достаточно реализовать взаимодействие этих протоколов с протоколом IP. Более подробно взаимодействие механизмов IP QoS с механизмами QoS канального уровня рассматривается в главе 8, “Качество обслуживания на уровне 2: межсетевой обмен с IP QoS”, далее в этой книге.

Технология MPLS помогает обеспечить качество обслуживания в сетях IP и предоставляет расширенные возможности по управлению трафиком, которые способствуют организации основанных на технологии MPLS виртуальных частных сетей (VPNs). С целью обеспечения в IP-сети сквозного качества обслуживания следует реализовать взаимодействие механизмов QoS сетевого уровня с механизмами QoS MPLS-сетей и виртуальных частных MPLS-сетей. Более подробно эта тема рассматривается в главе 9, “Качество обслуживания в сетях MPLS”, далее в этой книге.

Цели

Эта книга призвана стать ценным источником информации для сетевых администраторов, архитекторов и инженеров, желающих изучить и внедрить в своих сетях услуги IP QoS. Функции качества обслуживания являются крайне необходимыми в современных масштабируемых IP-сетях, обеспечивая предоставление гарантированных и дифференцированных услуг Internet путем передачи контроля за ресурсами сети и их использованием сетевому оператору.

Целью этой книги является рассмотрение архитектуры механизмов IP QoS и ассоциированных с ними функций, которые позволяют реализовать сквозное качество обслуживания в корпоративных интрасетях, сетях поставщиков услуг и, в общем случае, в глобальной сети Internet. Главный акцент при рассмотрении архитектуры механизмов IP QoS делается на архитектуре дифференцированных услуг (diffserv). Кроме этого, в данной книге уделяется внимание механизмам QoS, предусмотренным технологиями ATM, Frame Relay, IEEE 802.1p, IEEE 802.1Q, MPLS и MPLS VPN, а также взаимодействию этих механизмов с механизмами IP QoS с целью обеспечения сквозного качества обслуживания. Еще одной не менее важной темой, затронутой в этой книге, является тема управления трафиком в сетях MPLS.

В книге представлено наиболее полное описание IP QoS и всех связанных с качеством обслуживания технологий. Рассмотрение каждой технологии заканчивается практическим примером, наглядно иллюстрирующим ее применение. Читатели данной книги получают исчерпывающую информацию по следующим вопросам.

- Фундаментальные основы качества обслуживания в сетях IP и необходимость внедрения механизмов QoS.
- Архитектура дифференцированных услуг (diffserv) и разрешающие функции QoS.

- Архитектура интегрированных услуг (Intserv) и разрешающие функции QoS.
- Механизмы QoS, предусмотренные технологиями ATM, Frame Relay и IEEE 802.1p/802.1Q, — взаимодействие с механизмами IP QoS.
- Технологии MPLS и MPLS VPN — взаимодействие с механизмами IP QoS.
- Управление трафиком в сетях MPLS.
- Политики маршрутизации, общие функции IP QoS и другая информация, касающаяся качества обслуживания.

Механизмы QoS могут быть реализованы в любой IP-сети. Следовательно, материал, представленный в данной книге, относится ко всем сетям IP — корпоративным интрасетям, сетям поставщиков услуг и, наконец, Internet.

Аудитория

Эта книга предназначена для профессионалов в сфере межсетевого взаимодействия, в чью компетенцию входит разработка и поддержка функций обслуживания трафика для корпоративных интрасетей и сетей поставщиков услуг. Если вы являетесь сетевым инженером, архитектором, планировщиком, проектировщиком или оператором, обладающим лишь начальными знаниями технологий QoS, данная книга поможет вам восполнить этот пробел и позволит развить практические навыки в планировании и внедрении в сети различных уровней качества обслуживания.

Помимо этого, в книге содержится материал, полезный для консультантов, системных инженеров и инженеров по сбыту, разрабатывающих IP-сети на заказ. Другими словами, данная книга рассчитана на широкую аудиторию, поскольку планирование некоторых функций качества обслуживания является неотъемлемой частью процесса проектирования практически любой IP-сети.

Широта охвата и ограничения изложенного в книге материала

Несмотря на попытку представить полное и исчерпывающее описание механизмов качества обслуживания в сетях IP и функций QoS, специфических для оборудования компании Cisco, некоторые вопросы в этой книге не рассматривались. Так, не приводится информация об архитектуре различных платформ Cisco, которая может иметь отношение к механизмам QoS. Кроме того, несмотря на попытку унифицированного подхода к изложению материала, авторам не удалось избежать описания некоторых особенностей, характерных только для определенных устройств компании Cisco, что связано, в первую очередь, с несогласованностью в реализации функций QoS на различных платформах.

Одной из целей, которые ставились при написании этой книги, было сохранение целостности и актуальности представленного в книге материала. Тем не менее следует отметить, что качество обслуживания в целом и механизмы QoS оборудования Cisco в частности ждет много нововведений, каждое из которых способно со временем повлиять на изложенный в книге материал.

Практические примеры, приведенные в книге, предназначены для обсуждения некоторых вопросов, связанных с внедрением и конфигурацией функций качества обслуживания

ния в IP-сети. Естественно, данная книга ни в коем случае не претендует стать заменой документации компании Cisco. Документация Cisco по сей день является наилучшим источником информации, касающейся предназначенных для настройки механизмов QoS конфигурационных команд.

Следует отметить, что приведенные в книге практические примеры базируются на огромном числе различных версий операционной системы IOS. В большинстве случаев, если не оговорено противное, практические примеры базируются на версии операционной системы IOS 12.0(6)S или более поздней версии 12.0S. Практические примеры, в которых рассматривается технология MPLS, базируются на операционной системе IOS версии 12.0(8)ST или более поздней версии 12.0ST.

Организация книги

Книга состоит из четырех частей. В части I, “Качество обслуживания в сетях IP”, рассматривается архитектура качества обслуживания в сетях IP и разрешающие функции QoS. Часть II, “Качество обслуживания канального уровня и сети MPLS — межсетевой обмен с IP QoS”, посвящена механизмам QoS, предусмотренным технологиями ATM, Frame Relay, Ethernet, MPLS и MPLS VPN, а также взаимодействию этих механизмов с функциями IP QoS. В части III, “Управление трафиком”, рассматривается управление трафиком в сетях MPLS. И, наконец, в части IV, “Приложения”, приводится описание модульного интерфейса командной строки QoS и различных функций качества обслуживания; кроме того, здесь можно найти полезный справочный материал.

В большинстве глав имеются практические примеры, которые могут помочь разобраться в наиболее сложных проблемах внедрения функций качества обслуживания, а также списки часто задаваемых вопросов.

Часть I

В части I данной книги рассматривается архитектура качества обслуживания в сетях IP и разрешающие функции QoS. В главе 2 приводится описание двух архитектур IP QoS: архитектуры дифференцированных услуг (diffserv) и архитектуры интегрированных услуг (intserv). Как упоминалось ранее, главный акцент при изложении материала делается на рассмотрении архитектуры дифференцированных услуг.

В главах 3, 4, 5 и 6 рассматриваются различные разрешающие функции архитектуры diffserv. К примеру, в главе 3 обсуждается функция QoS, ответственная за формирование трафика на границе сети, что существенно облегчает задачу внедрения функций дифференцированного обслуживания. В главах 4 и 5 приводится описание механизмов обслуживания очередей, позволяющих гарантировать минимальную полосу пропускания для каждого потока трафика. В главе 6 рассматривается технология активного управления очередью, которая характеризуется превентивным отбрасыванием пакетов, сигнализирующих о перегрузке сети. И, наконец, в главе 7 речь идет о сигнальном протоколе RSVP и двух типах интегрированных в него функций QoS.

Часть II

В этой части книги, включающей в себя главы 8 и 9, рассматриваются механизмы QoS, предусмотренные технологиями ATM, Frame Relay, IEEE 802.1p, IEEE 802.1Q, MPLS

и MPLS VPN, а также способ взаимодействия этих механизмов с механизмами IP QoS с целью обеспечения сквозного качества обслуживания.

Часть III

Часть III включает в себя единственную главу 10, в которой рассматривается необходимость проведения управления трафиком и обсуждается управление трафиком в сетях MPLS.

Часть IV

В данной части книги содержится весьма полезная информация, имеющая непосредственное отношение к теме качества обслуживания в сетях IP.

Приложение А, “Модульный интерфейс командной строки Cisco QoS”, знакомит читателя с новым пользовательским интерфейсом, позволяющим проводить гибкую модульную конфигурацию служб QoS.

В приложении Б, “Механизмы коммутации пакетов”, обсуждаются различные механизмы коммутации пакетов, реализованные на платформах Cisco. Путем сравнительного анализа механизмов коммутации пакетов демонстрируются преимущества метода скоростной коммутации пакетов Cisco (CEF), являющегося необходимым условием для реализации некоторых функций QoS.

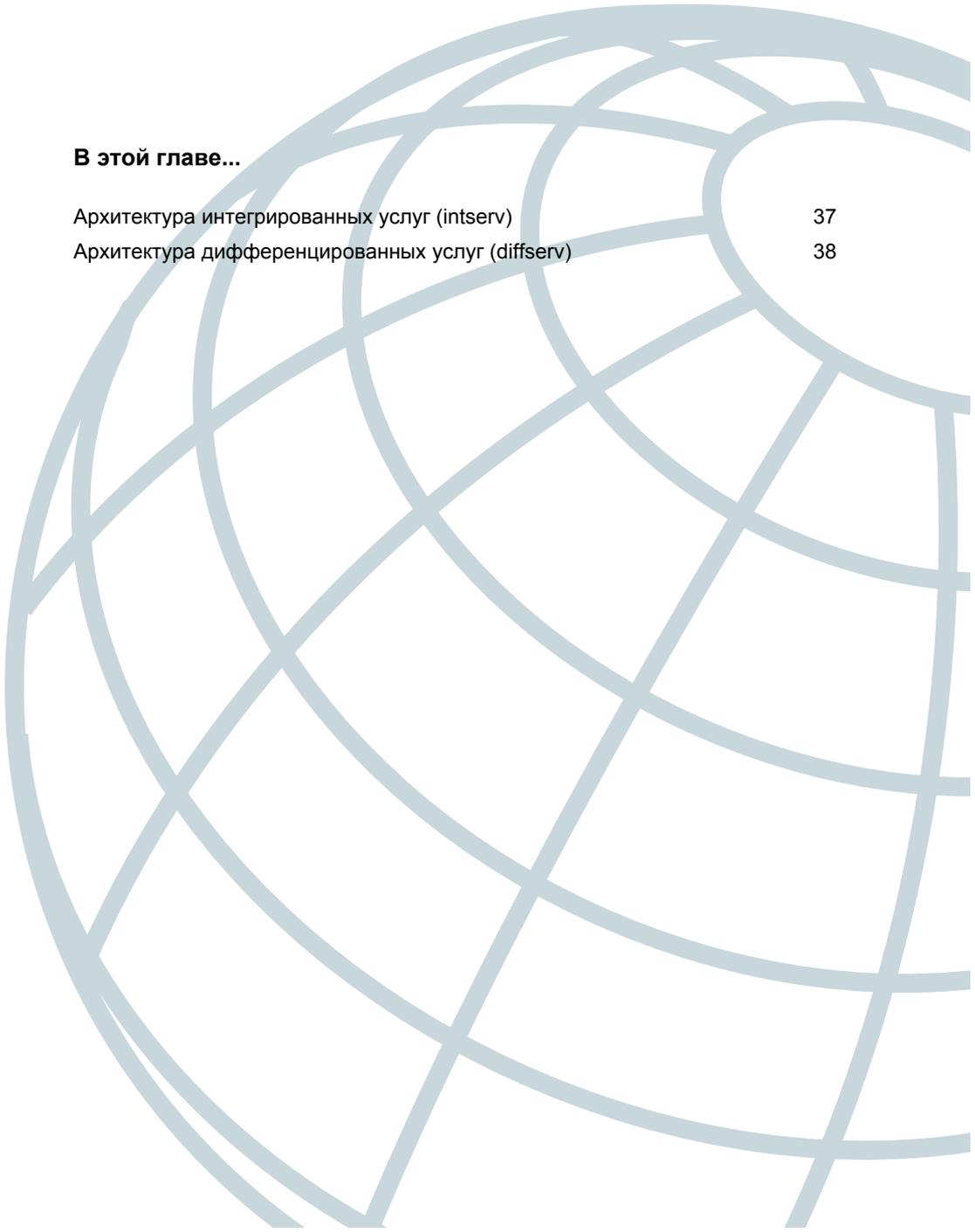
В приложении В, “Политики маршрутизации”, речь идет о маршрутизации QoS, маршрутизации на основе политики, а также распространении политик QoS с помощью протокола пограничного шлюза (QoS Policy Propagation using Border Gateway Protocol — QPPV).

В приложении Г, “Транспортный протокол реального времени (RTP)”, обсуждается транспортный протокол, использующийся для пакетной передачи голосового трафика и трафика видеоизображений в масштабе реального времени.

В приложении Д, “Общие функции линейной эффективности протокола IP”, представлен материал о некоторых функциях протокола IP, позволяющих увеличить доступную полосу пропускания.

В приложении Е, “Фрагментация и чередование пакетов на канальном уровне”, обсуждаются функциональные возможности многоканального протокола двухточечной связи (Multilink Point-to-Point protocol), касающиеся фрагментации и чередования пакетов.

В приложении Ж, “Значения поля IP-приоритета и поля DSCP”, приводятся затабулированные значения поля IP-приоритета и поля кода DSCP, а также иллюстрируется соотношение между данными характеристиками трафика.



В этой главе...

Архитектура интегрированных услуг (intserv)

37

Архитектура дифференцированных услуг (diffserv)

38

Архитектура дифференцированных услуг

Цель качества обслуживания в сетях IP (IP Quality of Service — IP QoS) — предоставление гарантированных и дифференцированных услуг в масштабах Internet или любой другой IP-сети. Дифференциация услуг обуславливает наличие нескольких уровней качества обслуживания, каждому из которых соответствует собственная архитектурная модель обеспечения функций QoS.

Главный акцент при изложении материала данной главы делается на рассмотрении архитектуры дифференцированных услуг (Differentiated Services — diffserv), использующейся для обеспечения функций QoS в масштабах Internet. Кроме этого, здесь обсуждается и другой подход к предоставлению функций QoS — архитектура интегрированных услуг (Integrated Services — intserv). Более подробно архитектура интегрированных услуг рассматривается в главе 7, “Интегрированные услуги: RSVP”, далее в этой книге. В данной главе будет описана также операционная модель QoS сетевого узла.

Архитектура интегрированных услуг (intserv)

В 1994 году проблемная группа проектирования Internet (Internet Engineering Task Force — IETF) сформировала рабочую группу по созданию интегрированных услуг (intserv Working Group), главной задачей которой являлось расширение базовой модели услуг Internet с целью обеспечения улучшенной поддержки разнообразных приложений, ориентированных на передачу голосового трафика и трафика видеоизображений. Созданная рабочая группа должна была четко определить новую усовершенствованную модель услуг Internet, разработать средства, позволяющие приложениям выражать сквозные требования к ресурсам, и создать механизмы, которые бы обеспечили надлежащую интерпретацию этих требований маршрутизаторами и различными технологиями, использующимися в подсетях. Основная идея при этом заключалась в отдельной обработке потоков трафика, запросивших определенный уровень качества обслуживания.

С этой целью были разработаны две услуги — гарантированного обслуживания¹ и регулируемой нагрузки². *Гарантированное обслуживание (guaranteed service)* предполагает

¹ Specification of Guaranteed Quality of Service/Shenker S., Partridge C., Guerin R.— RFC 2212.

предоставление детерминированных гарантий задержки, в то время как *служба регулируемой нагрузки (controlled load service)* использует механизм, похожий на механизм негарантированной доставки трафика в слегка загруженной сети. Более подробно каждая из этих услуг рассматривается в главе 7, “Интегрированные услуги: RSVP”, далее в этой книге.

В качестве сигнального протокола, использующегося для передачи требований сквозного обслуживания, был предложен протокол резервирования ресурсов (Resource Reservation Protocol — RSVP)³.

Следует отметить, что модель *intserv* требует обеспечения гарантированного качества обслуживания для каждого отдельного потока трафика в масштабах Internet. Учитывая тот факт, что на сегодня в каждый момент времени в Internet существуют тысячи потоков трафика, объем информации, который должны поддерживать маршрутизаторы, может быть предельно большим. К сожалению, это означает наличие практически неизбежных проблем, связанных с масштабированием сети, поскольку объем информации, который следует поддерживать маршрутизаторам, увеличивается пропорционально росту числа потоков трафика.

В 1998 году организация IETF сформировала рабочую группу по созданию дифференцированных услуг (*diffserv Working Group*). Архитектурную модель *diffserv* можно сравнить с мостом, соединяющим требования гарантированного качества обслуживания модели *intserv* с механизмом негарантированной доставки трафика, используемым сегодня в Internet. Модель *diffserv* обеспечивает дифференцирование трафика путем его разбивки на классы с различным приоритетом.

Архитектура дифференцированных услуг (*diffserv*)

В соответствии с моделью *diffserv*⁴ обеспечение качества обслуживания в сети IP предполагает наличие небольшого числа четко определенных “строительных” блоков, на основе которых можно создать множество различных услуг. Главной задачей подхода *diffserv* является определение стандартизированного байта дифференцированной услуги (DS) — байта типа обслуживания (Type of Service — ToS) из заголовка пакета Internet Protocol (IP) Version 4 и байта класса трафика (Traffic Class) пакета IP Version 6 — и его соответствующая маркировка, от которой зависит принятие специфического решения о продвижении пакета данных на каждом переходе (*per-hop behavior* — PHB), т.е. в каждом промежуточном узле.

Архитектура дифференцированных услуг обеспечивает базовую основу⁵, которая может быть использована поставщиками услуг для предоставления своим клиентам большого диапазона различных предложений в зависимости от предъявляемых требований к качеству обслуживания. Клиент может выбрать требуемый уровень услуг путем установки соответствующего значения поля кода дифференцированной услуги (*Differentiated Services Code Point* — DSCP) для каждого отдельного пакета. Код дифференцированной ус-

² *Specification of the Controlled-Load Network Element Service/Wroclawski J.— RFC 2211.*

³ *The Use of RSVP with IETF Integrated Services/Wroclawski J.— RFC 2210.*

⁴ *IETF Differentiated Services Working Group.*

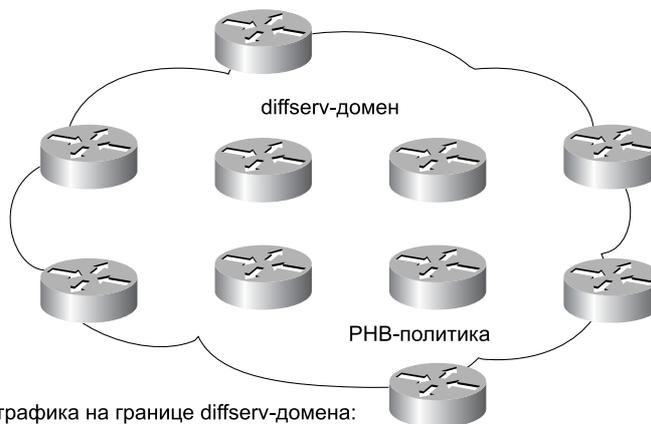
⁵ *A Framework for Differentiated Services/Bernet Y. et al., Internet Draft*

луги определяет цепочку решений о продвижении пакета в каждом промежуточном узле сети поставщика услуг (PHB-политика). Как правило, поставщик услуг обсуждает вместе с заказчиком профиль, согласно которому каждому уровню обслуживания будет соответствовать определенная интенсивность передачи трафика. Если же объем передаваемого трафика превысит установленную квоту для данного уровня обслуживания, то предоставление оговоренных услуг для “сверхплановых” пакетов не гарантируется.

Следует отметить, что архитектура дифференцированных услуг определяет всего лишь базовые механизмы, на основе которых осуществляется обслуживание пакетов. Используя эти механизмы в качестве строительных блоков, вы можете разработать целое множество различных услуг. Напомним, что в данном случае услуга определяет весьма значительные характеристики передачи пакетов, такие, как пропускная способность, задержка, дрожание, а также уровень потери пакетов в одном направлении при передаче вдоль сетевого маршрута. К тому же вы можете охарактеризовать услугу в терминах относительного приоритета при доступе к ресурсам сети. После определения услуги разрабатываются соответствующие ей решения о продвижении пакета (PHB-политика) для каждого узла сети, поддерживающего данную услугу. PHB-политике присваивается определенный код DSCP. PHB-политика — это наблюдаемая извне политика поведения сетевого узла в отношении пакетов с определенным значением поля кода дифференцированной услуги (DSCP). Все пакеты потока трафика со специфическим требованием к обслуживанию несут в себе одно и то же значение поля DSCP.

Все узлы внутри diffserv-домена определяют PHB-политику, которая должна быть применена к пакету на основе хранящегося в нем значения поля кода дифференцированной услуги. Кроме того, пограничные узлы diffserv-домена выполняют очень важную функцию формирования поступающего в diffserv-домен трафика. Формирование трафика включает в себя выполнение таких функций, как классификация пакетов и ограничение трафика, и обычно выносятся на входной интерфейс поступающих в diffserv-домен пакетов. Формирование играет решающую роль в управлении поступающим в diffserv-домен трафиком, поскольку в этом случае для каждого пакета сеть может определить соответствующую ему PHB-политику.

На рис. 2.1 схематически представлена архитектура дифференцированных услуг. Описание двух основных функциональных блоков этой архитектуры приведено в табл. 2.1.



Формирование трафика на границе diffserv-домена:

установка значения поля DSCP;
ограничение трафика.

Рис. 2.1. Архитектура дифференцированных услуг

Таблица 2.1. Функциональные блоки архитектуры дифференцированных услуг

Функциональный блок	Расположение	Разрешающая функция	Действие
Формирователи трафика	Входной интерфейс пограничного маршрутизатора diffserv-домена	Классификация пакетов, выравнивание и ограничение трафика (более подробно см. в главе 3)	Ограничение входящего трафика и установка значения поля DSCP на основе профиля трафика
Устройства, реализующие PHB-политику	Все маршрутизаторы diffserv-домена	Распределение ресурсов (более подробно см. в главе 4 и главе 5) и политика отбрасывания пакетов (более подробно см. в главе 6)	PHB-политика обработки пакетов определяется на основе характеристик качества обслуживания, соответствующих заданному значению поля DSCP

Помимо описанных выше функциональных блоков, политика распределения ресурсов играет важную роль в определении стратегии управления доступом, коэффициента бронирования ресурсов и т.д.

Примечание

Для четкого разделения и обеспечения модульной конфигурации различных разрешающих функций QoS компания Cisco разработала модульный интерфейс командной строки (Command-Line Interface — CLI) QoS (более подробно модульный интерфейс командной строки QoS рассматривается в приложении А, “Модульный интерфейс командной строки Cisco QoS”, далее в этой книге).

На рис. 2.2 изображена обобщенная операционная модель QoS.



Рис. 2.2. Обобщенная операционная модель QoS

Код дифференцированной услуги (DSCP)

В настоящее время рабочая группа IETF по созданию и внедрению дифференцированных услуг предпринимает попытки стандартизации поля DSCP, которая позволила бы использовать 6 бит из байта ToS заголовка IP-пакета для установки кода дифференцированной услуги. При этом 2 младших бита из байта ToS не используются (currently unused — CU). Фактически код дифференцированной услуги представляет собой расширение 3-битового поля IP-приоритета. Так же, как и IP-приоритет, код дифференцированной услуги позволяет определять способ обработки отмеченных соответствующим образом пакетов данных. На рис. 2.3 представлена структура байта ToS6. После стандартизации поля кода дифференцированной услуги байт ToS будет переименован в байт DS. На рис. 2.4 представлена структура байта DS.

P2	P1	P0	T3	T2	T1	T0	CU
----	----	----	----	----	----	----	----

IP-приоритет: 3 бит (P2-P0)
 Тип обслуживания (ToS): 4 бит (T3-T0)
 Не используется (CU): 1 бит

Рис. 2.3. Структура байта ToS в соответствии с документом RFC 1349

DS5	DS4	DS3	DS2	DS1	DS0	CU	CU
-----	-----	-----	-----	-----	-----	----	----

Код дифференцированной услуги (DSCP): 6 бит (DS5-DS0)
 Не используется (CU): 2 бит

Рис. 2.4. Структура байта DS

На сегодняшний день рабочая группа IETF по созданию и внедрению дифференцированных услуг определяет коды DSCP следующим образом⁷.

- **Стандартный код DCSP.** Определен как 000 000.

⁶ Type of Service in the Internet Protocol Suite/Almquist P. — RFC 1349.

⁷ Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers/Nichols K. et al. — RFC 2474.

- **Селектор класса.** Эти коды DSCP обладают обратной совместимостью с кодами IP-приоритета и представлены в табл. 2.2.

Таблица 2.2. Селекторы класса

Селектор класса	DSCP
Приоритет 1	001 000
Приоритет 2	010 000
Приоритет 3	011 000
Приоритет 4	100 000
Приоритет 5	101 000
Приоритет 6	110 000
Приоритет 7	111 000

- **PHB-политика немедленной передачи (Expedited Forwarding — EF).** Этот код DSCP соответствует наиболее высококлассному уровню обслуживания, предоставляемому за дополнительную стоимость. Рекомендуемое значение — 101 110.
- **PHB-политика гарантированной передачи (Assured Forwarding — AF).** Эти коды DSCP определяют четыре уровня обслуживания, каждый из которых, в свою очередь, может быть охарактеризован тремя уровнями приоритета отбрасывания пакетов данных. Как результат PHB-политике гарантированной передачи соответствуют 12 кодов DSCP, представленных в табл. 2.3.

Таблица 2.3. PHB-политика гарантированной передачи

Приоритет отбрасывания пакета	Класс 1	Класс 2	Класс 3	Класс 4
Низкий	001010	010010	011010	100010
Средний	001100	010100	011100	100100
Высокий	001110	010110	011110	100110

Формирователи трафика, расположенные на границе сети

Формирователи трафика — это различные функции качества обслуживания, которые должны быть реализованы в пограничных устройствах сети. Граничные функции классифицируют или маркируют трафик путем установки соответствующего значения поля DSCP, а также проводят мониторинг входящего в сеть трафика с целью проверки его соответствия установленному профилю.

Код дифференцированной услуги представляет собой поле, на основании значения которого определяется способ обработки пакета в diffserv-домене. В качестве обрабатывающей трафик функции может выступать функция классификации пакетов, функция маркировки DSCP-поля, или же функция дозирования трафика, наделенная либо полномочиями выравнивания трафика, либо полномочиями отбрасывания пакетов. Все названные выше функции рассматриваются в следующих разделах данной главы; тем не менее если вам необходимо получить более подробную информацию, обратитесь к главе 3, “Формирование трафика на границе сети: классификация пакетов, маркировка пакетов и управление интенсивностью трафика”.

Классификатор пакетов

Классификатор пакетов выбирает пакет из потока трафика на основании анализа части содержимого заголовка пакета. Наиболее распространенный способ классификации пакетов заключается в анализе поля DSCP, однако теоретически вы можете классифицировать пакет на основании значения других полей его заголовка. Функция классификации пакета определяет соответствующий этому пакету класс трафика.

Маркер

Эта функция предназначена для записи/перезаписи поля DSCP в зависимости от класса трафика, к которому относится данный пакет.

Дозирование трафика

Функция дозирования проверяет трафик на соответствие заданному профилю на основании дескриптора трафика, такого, как корзина маркеров. Результаты проверки передаются функции маркировки трафика, а также либо функции выравнивания трафика, либо функции отбрасывания пакетов для принятия соответствующего решения в отношении “плановых” и “внеплановых” пакетов.

Функция выравнивания трафика

Функция *выравнивания трафика (traffic shaping)* осуществляет задержку пакетов путем их буферизации с целью удовлетворения параметров заданного профиля.

Функция отбрасывания пакетов

Функция отбрасывания пакетов осуществляет отбрасывание всех пакетов, не удовлетворяющих параметрам заданного профиля трафика. Это действие часто называют также *ограничением трафика (traffic policing)*.

PHB-политика

Сетевые узлы с поддержкой дифференцированного обслуживания используют поле DSCP в заголовке IP-пакета для определения соответствующей этому пакету PHB-политики.

PHB-политика может быть определена в терминах приоритета в предоставлении ресурсов по отношению к другим PHB-политикам или же с помощью таких измеряемых характеристик трафика, как задержка пакетов, уровень потери пакетов или дрожание трафика. В некоторой степени PHB-политику можно рассматривать как своеобразный “черный ящик”, поскольку она определяет некоторое наблюдаемое извне поведение сетевого узла в отношении поступающих пакетов, не навязывая при этом конкретную реализацию.

В качестве стандартной PHB-политики в diffserv-сети можно рассматривать негарантированную доставку трафика. В соответствии с архитектурой дифференцированного обслуживания каждой PHB-политике рекомендуется назначить определенный код DSCP, однако поставщик услуг волен выбрать отличные от рекомендованных значения поля DSCP для своей собственной сети. Рекомендованное значение поля DSCP для политики негарантированной доставки пакетов равняется 000000.

PHB-политика, соответствующая определенному классу трафика, зависит от целого ряда факторов.

- **Интенсивность входного потока или нагрузки для заданного класса трафика.** Этот параметр контролируется пограничным формирователем трафика.
- **Распределение ресурсов для заданного класса трафика.** Этот параметр контролируется функциями распределения ресурсов, реализованными в узлах diffserv-домена. Более подробно распределение ресурсов в узлах diffserv-сети рассматривается в главе 4, “PHB-политика: распределение ресурсов (часть 1)”, и главе 5, “PHB-политика: распределение ресурсов (часть 2)”, далее в этой книге.
- **Уровень потери трафика.** Этот параметр зависит от политики отбрасывания пакетов, проводимой в узлах diffserv-домена. Более подробно данная функция рассматривается в главе 6, “PHB-политика: предотвращение перегрузки и политика отбрасывания пакетов”.

Существуют две стандартные PHB-политики — PHB-политика немедленной передачи (EF PHB) и PHB-политика гарантированной доставки (AF PHB). Их рассмотрению посвящены два следующих раздела этой главы.

PHB-политика немедленной передачи пакетов (EF PHB)

PHB-политика немедленной передачи пакетов (Expedited Forwarding PHB — EF PHB) используется для обеспечения сквозного обслуживания пакетов в узлах diffserv-домена, характерными чертами которого являются низкий уровень потери пакетов, малая задержка, незначительное дрожание трафика, а также гарантированная полоса пропускания⁸. Политика EF PHB применяется для обслуживания трафика таких приложений, как передача голоса по сетям IP (Voice over IP — VoIP), приложений видеоконференций, а также для обеспечения таких услуг, как передача информации по виртуальным арендуемым каналам, поскольку эта услуга представляет собой двухточечное соединение конечных узлов diffserv-домена. Подобный тип обслуживания достаточно часто называют также *услугами высокого класса (premium service)*.

Главными факторами, ведущими к большой задержке пакетов и дрожанию трафика, являются задержки, связанные с возникновением больших накопленных очередей. Подобные очереди характерны для перегруженных участков сети. Причиной перегрузки сети является преобладание интенсивности входного потока трафика над интенсивностью его выходного потока. Один из способов избежать задержки пакетов, связанной с возникновением больших очередей, — ограничение максимальной интенсивности входного потока трафика минимальной интенсивностью его выходного потока. PHB-политика немедленной передачи пакетов предусматривает установку значения интенсивности выходного потока трафика, в то время как интенсивность входного потока контролируется формирователями трафика, реализованными в пограничных устройствах сети.

Поскольку в соответствии с политикой EF PHB входящие пакеты не должны образовывать очередь (допускается очередь очень малого размера), интенсивность исходящего потока трафика должна быть равной интенсивности входящего потока или превышать ее. Следует отметить, что интенсивность исходящего потока трафика (полоса пропускания) не должна зависеть от других потоков трафика. Как правило, интенсивность входящего и

⁸ Expedited Forwarding (EF) PHB/Jacobson V., Nichols K., Poduri K. — RFC 2598.

исходящего потока трафика измеряется с интервалами, равными времени, которое требуется для передачи MTU-пакета (пакета максимального размера, который может быть передан через интерфейс маршрутизатора) по данной линии связи.

Маршрутизатор может выделить ресурсы, достаточные для обеспечения определенной интенсивности исходящего трафика для заданного интерфейса, путем использования различных функциональных реализаций политики EF PHB. Когда речь идет о передаче трафика через перегруженный сегмент сети (а это предполагает наличие больших накопленных очередей), данная функциональная возможность может быть реализована за счет применения различных механизмов обслуживания очередей, таких, как взвешенный механизм равномерного обслуживания очередей на основе класса трафика (Class-Based Weighted Fair Queuing — CBWFQ), взвешенный механизм кругового обслуживания (Weighted Round Robin — WRR) и механизм кругового обслуживания с дефицитом (Deficit Round Robin — DRR). В этом случае EF-трафику назначается вес, который соответствует полосе пропускания, намного превышающей интенсивность входящего EF-трафика. В дальнейшем вы можете модифицировать эти механизмы, добавив приоритетную очередь, предназначенную специально для обслуживания EF-трафика. Более подробно механизмы обслуживания очередей рассматриваются в главе 5, “PHB-политика: распределение ресурсов (часть 2)”, далее в этой книге.

Если обработка EF-трафика реализуется за счет организации приоритетной очереди, следует убедиться в том, что оставшиеся очереди трафика не испытывают недостатка в поступающих пакетах в рамках определенного предела. В целях предотвращения этой проблемы можно определить максимальную интенсивность трафика, обрабатываемого с помощью приоритетной очереди. Если интенсивность поступающего EF-трафика превысит заданный предел, весь избыточный трафик будет отброшен. Пограничные формователи поступающего в diffserv-домен трафика должны быть сконфигурированы таким образом, чтобы интенсивность EF-трафика никогда не превышала заданного предела на любом участке сети.

Рекомендуемое значение поля DSCP для EF-трафика равняется 101110.

PHB-политика гарантированной доставки пакетов (AF PHB)

PHB-политика гарантированной доставки пакетов (Assured Forwarding PHB — AF PHB)⁹ представляет собой средство, с помощью которого поставщик услуг может обеспечить несколько различных уровней надежности доставки IP-пакетов, полученных из diffserv-домена клиента. Политика AF PHB является приемлемой для большинства TCP-приложений.

PHB-политика гарантированной доставки пакетов подразумевает наличие различных уровней обслуживания для каждого из четырех классов AF-трафика. Каждому классу AF-трафика соответствует своя собственная очередь пакетов, что позволяет проводить эффективное управление полосой пропускания. Каждый класс AF-трафика характеризуется тремя уровнями приоритета отбрасывания пакетов (низкий, средний и высокий), что позволяет реализовать механизм управления очередью по типу механизма произвольного раннего обнаружения (Random Early Detection — RED).

⁹ *Assured Forwarding (AF) PHB/Heinonen J., Finland T., Baker F. (Cisco Systems), Weiss W. (Lucent Technologies), Wroclawski J. (MIT LCS) — RFC 2597.*

Политика распределения ресурсов

В последнем разделе этой главы мы обсудим способы реализации PNB-политик в diff-serv-сети. Каким образом происходит формирование трафика на границе сети и распределение ресурсов в ее узлах для достижения определенной PNB-политики? Существует три решения: инициализация сети, сигнализация о качестве обслуживания и диспетчер политик.

Инициализация сети

Один из способов распределения ресурсов заключается в инициализации ресурсов сети с использованием эвристических методов или техники систематического моделирования. Следует отметить, что этот метод может быть применен только в сетях небольшого размера, для которых политики QoS и профили трафика остаются неизменными на протяжении достаточно долгого промежутка времени.

Сигнализация о качестве обслуживания

В соответствии с этим методом реализации PNB-политики приложения извещают сеть о требованиях к качеству обслуживания с помощью сигнального протокола RSVP. С точки зрения протокола RSVP diffserv-домен рассматривается как еще одно звено сети, требующее управление доступом. С помощью протокола RSVP можно установить соответствие между запросами к качеству обслуживания приложений и классами услуг diffserv. К примеру, гарантированному обслуживанию RSVP может быть поставлена в соответствие diffserv-услуга немедленной передачи пакетов.

Сигнализация о качестве обслуживания является чрезвычайно масштабируемым решением в крупных сетях, поскольку протокол RSVP выполняется только в пограничных узлах diffserv-домена, как показано на рис. 2.5.



Рис. 2.5. Передача сигнальной информации протокола RSVP через сеть с дифференцированным обслуживанием

Установка соответствия между резервированием ресурсов протокола RSVP и diffserv-классами проводится на границе diffserv-сети. Учитывая широкую поддержку протокола RSVP (к примеру, RSVP поддерживается операционной системой Microsoft Windows 2000), уведомленные о существующей политике пограничные приложения могут использовать его для сообщения требований к качеству обслуживания, не обращая при