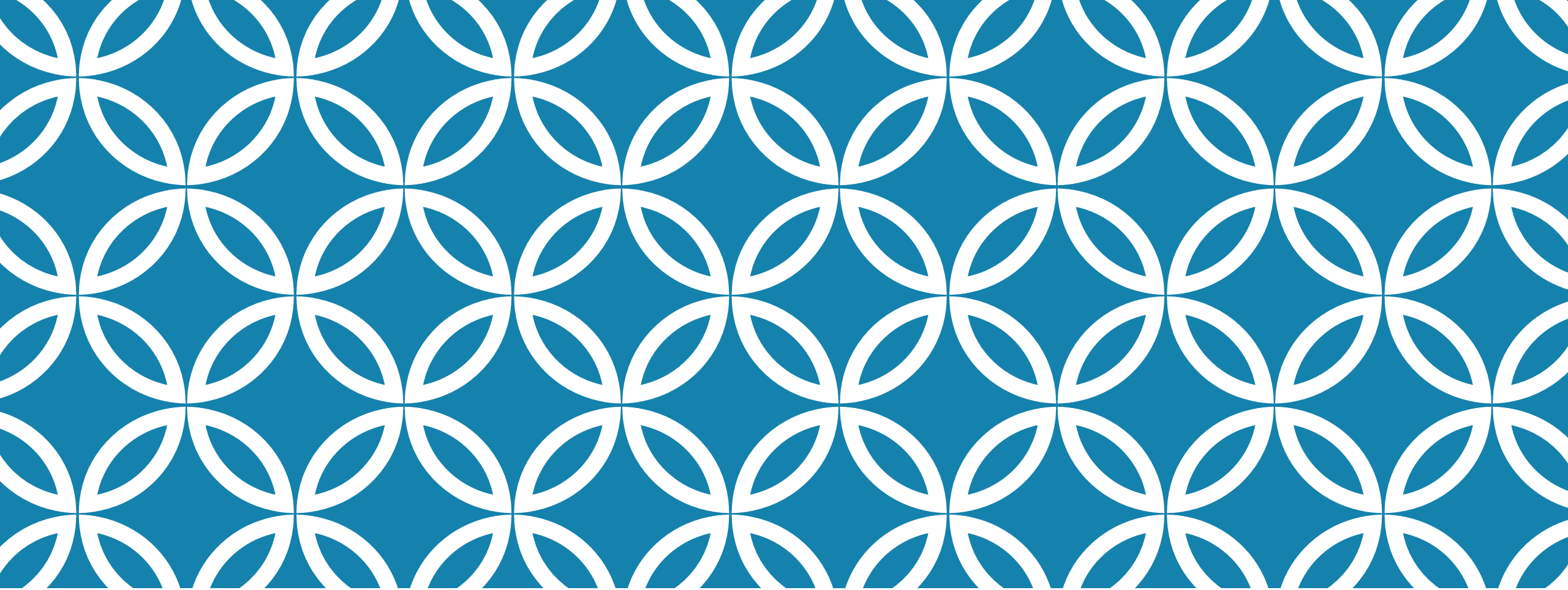


МОДУЛЬ 9. ПРИНЦИПЫ QOS

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

9.1 КАЧЕСТВО ПЕРЕДАЧИ ДАННЫХ ПО СЕТИ

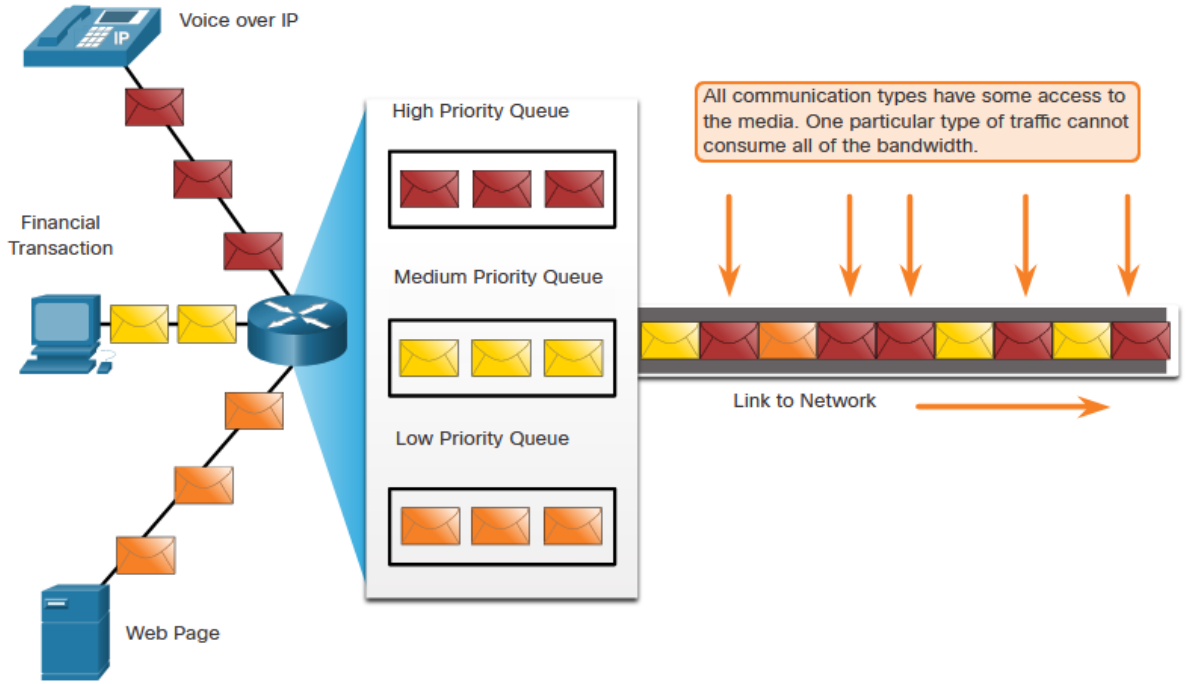
9.1.1 ПРИОРИТИЗАЦИЯ ТРАФИКА

Когда объем трафика превышает возможности доставки по сети, устройства помещают пакеты в очередь в памяти и удерживают их до тех пор, пока не будут доступны ресурсы передачи.

Постановка пакетов в очередь приводит к задержке, поскольку новые пакеты не могут передаваться до тех пор, пока не будут обработаны предыдущие.

Если число пакетов для постановки в очередь продолжает расти, память устройства заполняется и пакеты отбрасываются.

Метод QoS, который может помочь в решении этой проблемы, заключается в распределении данных по нескольким очередям, как показано на этом рисунке.



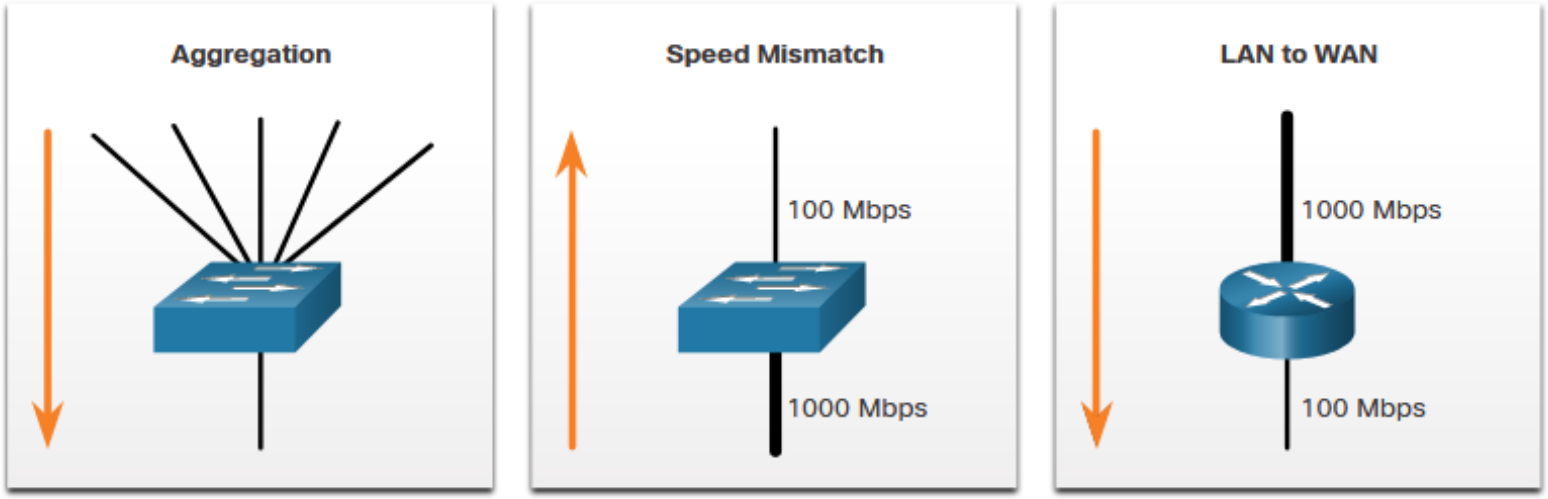
Примечание. Устройство обеспечивает доступность качества обслуживания только при возникновении перегрузки определенного типа.

9.1.2 ПОЛОСА ПРОПУСКАНИЯ, ЗАТОР, ЗАДЕРЖКА И ДЖИТТЕР

Полоса пропускания сети измеряется в количестве бит, которое можно передать за одну секунду, то есть в битах в секунду (бит/с).

Затор в сети приводит к задержке. Затор в интерфейсе возникает, когда объем трафика превышает тот объем, который может быть обработан. Точки затора в сети — та область, где необходимо использовать механизмы QoS.

Примеры типичных точек возникновения заторов: агрегация, несоответствие скорости и передача данных из локальной сети в глобальную сеть.



9.1.2 ПОЛОСА ПРОПУСКАНИЯ, ЗАТОР, ЗАДЕРЖКА И ДЖИТТЕР

Задержка - время, которое занимает передача пакета от источника до адресата.

Фиксированная задержка - определенное количество времени, которое требуется конкретному процессу, например, количество времени, требуемое для помещения бита на передающий носитель.

Переменная задержка занимает неопределенное количество времени и зависит от таких факторов, как количество текущего трафика.

Джиттер - изменение времени задержки полученных пакетов.

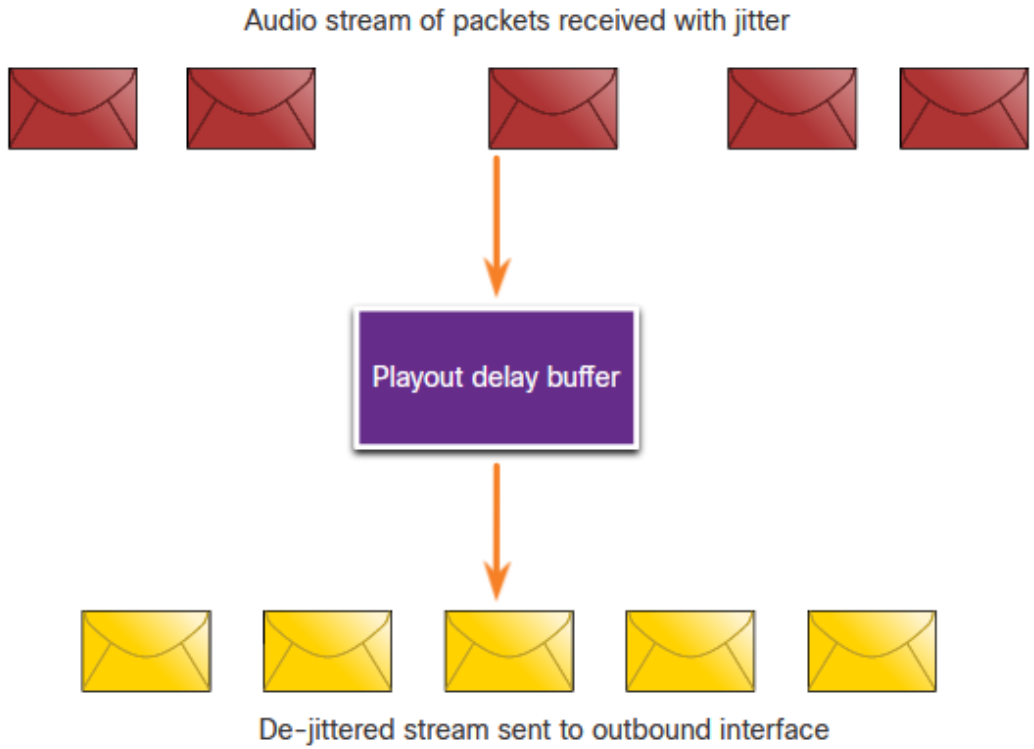
Задержка	Описание
Задержка кодирования	Фиксированное время, необходимое для сжатия данных в источнике перед передачей на первое устройство, работающее по Интернету (как правило, коммутатор).
Задержка пакетирования	Фиксированное время для инкапсуляции пакета со всеми необходимыми данными заголовка.
Задержка в очереди	Изменяемый период времени, в течение которого кадр или пакет ожидает передачи по каналу.
Задержка сериализации	Фиксированный период времени, в течение которого кадр передается в канал.
Задержка распространения	Изменяемое время, необходимое для передачи кадра между источником и получателем.
Задержка устранения джиттера	Фиксированный период времени, необходимый для буферизации потока пакетов и последующей отправки их через равные интервалы.

9.1.3 ПОТЕРЯ ПАКЕТОВ

Без механизмов QoS чувствительные ко времени пакеты, такие как видео и голос в реальном времени, отбрасываются с той же частотой, что и данные, которые не чувствительны ко времени.

Когда маршрутизатор получает цифровой аудиопоток по протоколу реального времени (RTP) для передачи голоса по IP (VoIP), он компенсирует дрожание, возникающее при использовании буфера задержки воспроизведения.

Буфер задержки воспроизведения буферизирует эти пакеты, а затем воспроизводит их в виде устойчивого потока.

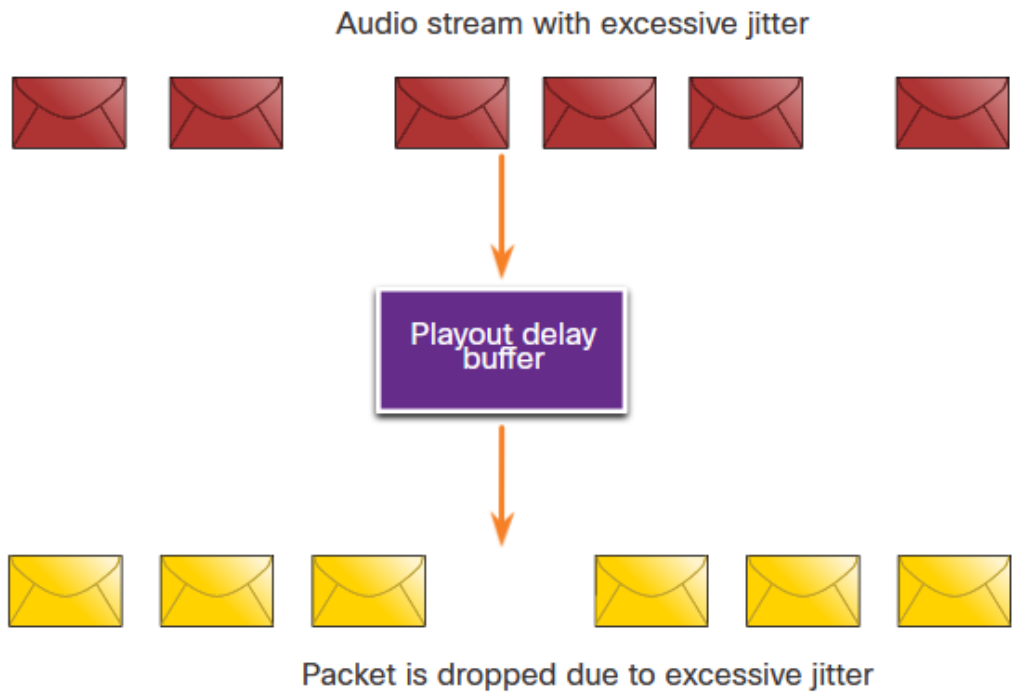


9.1.3 ПОТЕРЯ ПАКЕТОВ

Если джиттер настолько интенсивен, что приводит к выходу принимаемых пакетов из области данного буфера, пакеты вне области отбрасываются и эти потери слышны в аудиопотоке.

При небольших потерях на уровне одного пакета процессор цифровых сигналов применяет интерполяцию, восстанавливая нормальное звучание без заметных на слух дефектов.

Вместе тем, если джиттер превышает возможности DSP по компенсации потерянных пакетов, проблемы со звуком будут слышны.



9.2 ХАРАКТЕРИСТИКИ ТРАФИКА
9.2.1 ОСНОВНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ СЕТЕВОГО ТРАФИКА

В 2000-х годах в IP-трафике преобладали голос и данные.

Голосовой трафик характеризуется предсказуемой потребностью в полосе пропускания; время поступления пакетов известно.

Трафик передачи данных не является трафиком реального времени и характеризуется непредсказуемой потребностью в полосе пропускания.

Во время загрузки большого файла трафик данных может давать кратковременные всплески. Подобные всплески могут занять всю полосу пропускания канала связи.

В последнее время видеотрафик становится все более важным для бизнес-коммуникаций и бизнес-процессов.

Согласно индексу Cisco Visual Networking Index (VNI), видеотрафик составлял 70% всего трафика в 2017 году.

К 2022 году видео будет представлять 82% всего трафика.

Мобильный видеотрафик достигнет 60,9 экзабайт в месяц к 2022 году.

Требования к трафику голосовой связи, видео и данных в сети могут сильно различаться.

9.2.2 ГОЛОСОВОЙ ТРАФИК

Голосовой трафик предсказуемый, плавный и очень чувствительный к задержкам и отбросам пакетов.

Пакеты голосовых данных должны получать самый высокий приоритет над остальными типами трафика.

Продукты Cisco используют порты RTP в диапазоне от 16384 до 32767 для приоритизации трафика голосовых данных.

При передаче голоса допустимы определенные задержки, джиттер и потери без каких-либо заметных эффектов.

9.2.2 ГОЛОСОВОЙ ТРАФИК

Задержка не должна превышать 150 миллисекунд (мс).

Джиттер не должен превышать 30 мс, а потеря голосовых пакетов — 1 %.

Для трафика голосовых данных требуется пропускная способность не менее 30 Кбит/с.

Характеристики трафика голосовых данных	Требования для односторонней передачи
• Равномерность • Умеренность • Чувствительность к потерям • Чувствительность к задержкам • Приоритет UDP	• Задержка ≦ 150 мс • Дрожание ≤ 30 мс • Потеря ≤ 1% пропускной способности (30-128 Кбит/с)

9.2.3 ВИДЕОТРАФИК

Видеотрафик может быть непредсказуемым, неоднородным и неравномерным. Видео по сравнению с голосом менее устойчиво к потерям, объем пакета для такого трафика больше. Количество и размер видеопакетов, наоборот, меняются каждые 33 мс в зависимости от контента видео.
Портам UDP, например 554, которые используются для протокола потоковой передачи в режиме реального времени (RSTP), необходимо присвоить более высокий приоритет относительно другого сетевого трафика, менее чувствительного к задержкам.
Задержка не должна превышать 400 миллисекунд (мс). Джиттер не должен превышать 50 мс, а потеря видеопакетов — 1 %. Для видеотрафика требуется пропускная способность не менее 384 Кбит/с.

Характеристики видеотрафика	Требования для односторонней передачи
• Неравномерность • Ресурсоемкость • Чувствительность к потерям • Чувствительность к задержкам • Приоритет UDP	• Задержка ≤ 200–400 мс • Джиттер ≦ 30–50 мс • Потери ≤ 0,1–1 % • Полоса пропускания (от 384 Кбит/с до 20 Мбит/с и более)

9.2.4 ТРАФИК ДАННЫХ

Информационные приложения, которые не допускают потерю данных, например, электронная почта и веб-страницы, используют протокол TCP, который обеспечивает повторную отправку пакетов, потерянных при передаче.
Трафик данных может быть постоянным или пульсирующим.
Трафик управления сетью обычно является постоянным и предсказуемым.
Некоторые приложения TCP могут потреблять большую часть емкости сети. Во время загрузки большого файла, например фильма или игры, FTP использует максимально возможную полосу пропускания.

Характеристики трафика

- Равномерность/неравномерность
- Умеренность/ресурсоемкость
- Нечувствительность к потерям
- Нечувствительность к задержкам
- Передача TCP

9.2.4 ТРАФИК ДАННЫХ

По сравнению с голосом и видео трафик данных относительно нечувствителен к отбрасыванию пакетов и задержкам. Качество восприятия или QoE важно учитывать при передаче данных:
- поступают ли данные из интерактивного приложения;
- являются ли данные критически важными.

Фактор	Критически важный	Не критически важный
Интерактивный	Выполните приоритизацию для обеспечения минимальной задержки всего трафика данных и добейтесь времени отклика от 1 до 2 секунд.	Приложения могут получить преимущества при малой задержке.
Не интерактивный	Время задержки может значительно различаться при обеспечении необходимой минимальной полосы пропускания.	Получает любую оставшуюся полосу пропускания после удовлетворения потребностей всех приложений передачи голоса, видео и других данных.

9.3 АЛГОРИТМЫ ОРГАНИЗАЦИИ ОЧЕРЕДИ

9.3.1 ОБЩИЕ СВЕДЕНИЯ ОБ ОРГАНИЗАЦИИ ОЧЕРЕДЕЙ

Политика качества обслуживания, реализованная сетевым администратором, становится активной при возникновении затора в канале связи. Организация очереди является средством управления затором, которое может выполнять буферизацию, приоритизацию и, если необходимо, изменение порядка пакетов перед их передачей адресату.

Доступен ряд алгоритмов организации очередей:

1. «Первым пришел — первым ушел» (first-in, first-out, FIFO).

2. Взвешенная организация очередей (WFQ).

3. Взвешенная организация очередей на основе классов (CBWFQ).

4. Организация очередей с малой задержкой (LLQ).

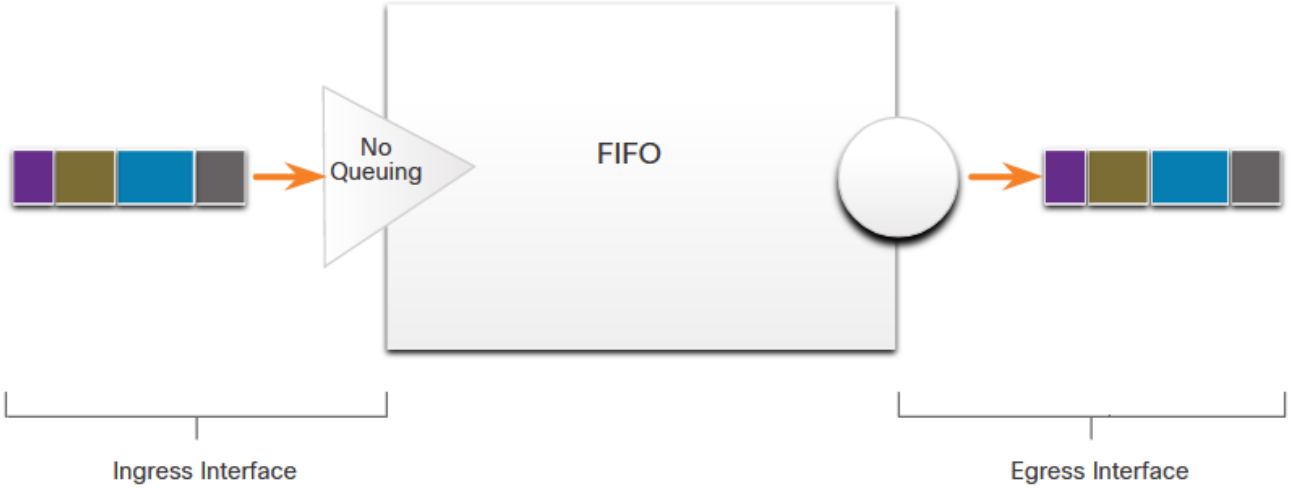
9.3.2 АЛГОРИТМ «ПЕРВЫМ ПРИШЕЛ — ПЕРВЫМ УШЕЛ» (FIFO)

Буферизирует очереди First In First Out (FIFO) и пересылает пакеты в порядке их прибытия.

В FIFO нет концепции приоритета или классов трафика и, следовательно, не принимаются решения о приоритете пакетов.

Есть только одна очередь — все пакеты обрабатываются одинаково.

Пакеты отправляются из интерфейса в порядке их поступления.



9.3.2 ВЗВЕШЕННАЯ ОРГАНИЗАЦИЯ РАВНОПРАВНЫХ ОЧЕРЕДЕЙ (WFQ)

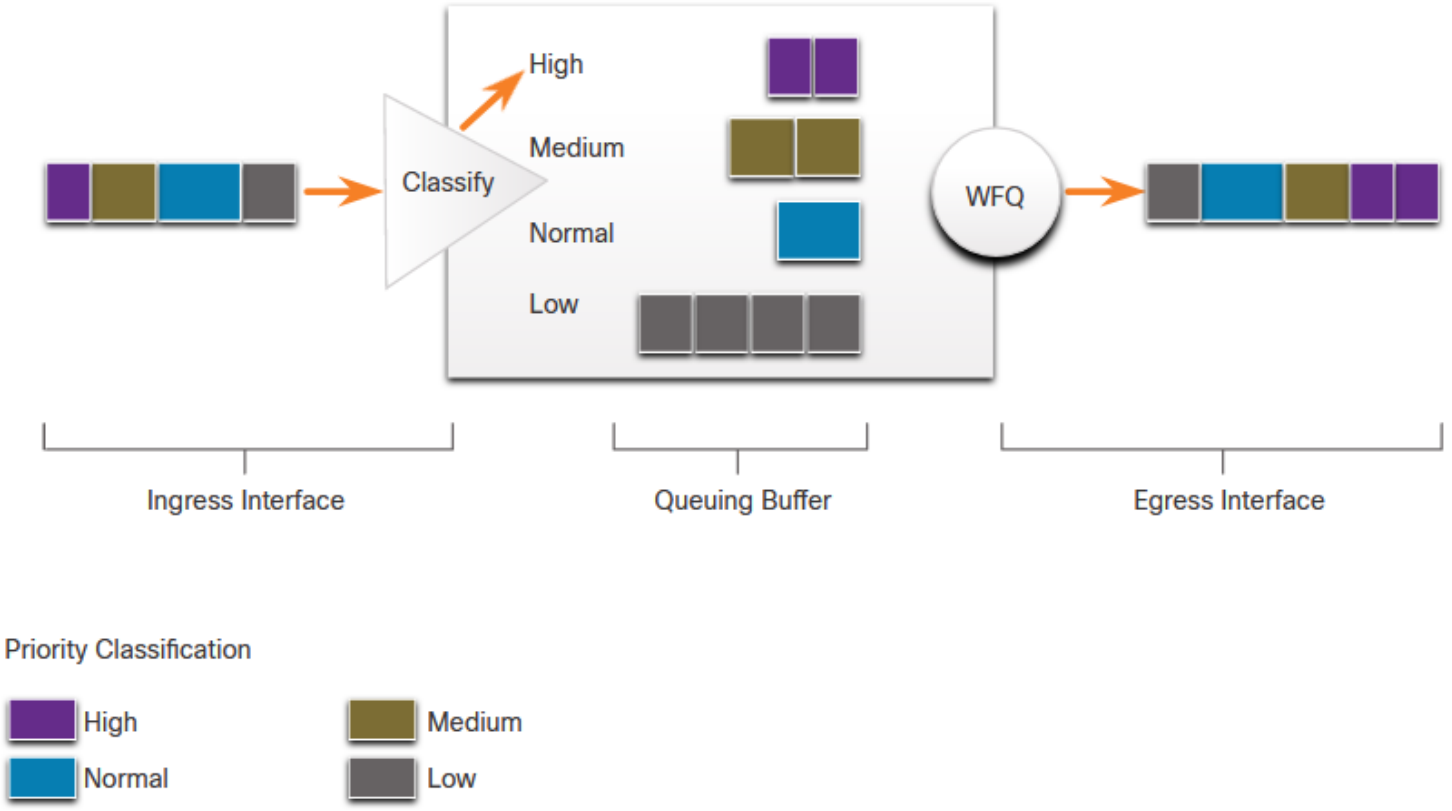
WFQ является автоматизированным методом планирования, который обеспечивает справедливое выделение полосы пропускания всему сетевому трафику.

WFQ применяет приоритет или весы к идентифицируемому трафику, классифицирует его по разговорам или потокам, а затем определяет, какая пропускная способность каждого потока разрешена по отношению к другим потокам.

WFQ классифицирует трафик, разделяя его на различные потоки с учетом адресации заголовков пакетов, включая такие характеристики, как IP-адреса источника и назначения, MAC-адреса, номера портов, протоколы и значение типа обслуживания (ToS).

WFQ не поддерживается с туннелированием и шифрованием, поскольку эти функции изменяют информацию о содержимом пакета, которая необходима WFQ для классификации.

9.3.2 ВЗВЕШЕННАЯ ОРГАНИЗАЦИЯ РАВНОПРАВНЫХ ОЧЕРЕДЕЙ (WFQ)

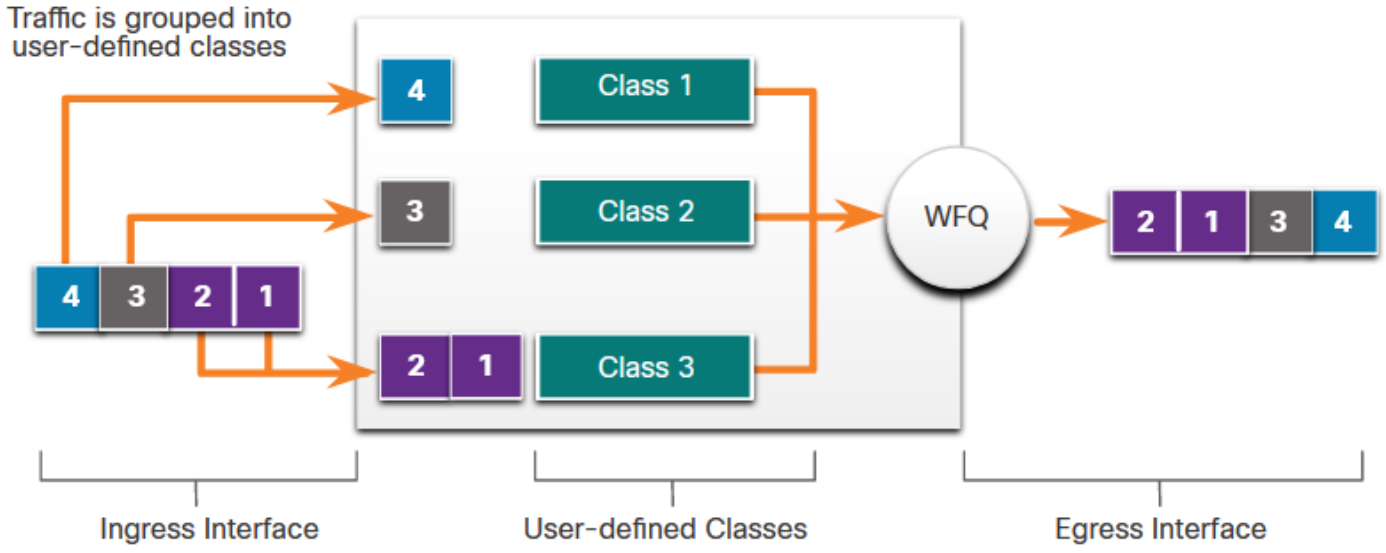


9.3.3 ВЗВЕШЕННАЯ ОРГАНИЗАЦИЯ ОЧЕРЕДЕЙ НА ОСНОВЕ КЛАССОВ (CBWFQ)

Алгоритм CBWFQ обладает более широкими возможностями, чем стандартный алгоритм WFQ, за счет поддержки определенных пользователем классов трафика.
Используя CBWFQ, вы определяете классы трафика на основе критериев соответствия, в том числе протоколов, ACL-списков и входных интерфейсов.
Совокупность пакетов, соответствующих критериям для определенного класса, образует трафик для данного класса.
Очередь FIFO зарезервирована для каждого класса, и трафик определенного класса направляется в очередь для данного класса
Чтобы характеризовать класс, ему назначаются пропускная способность, вес и максимальное ограничение пакета. Полоса пропускания, назначенная классу, является гарантированной полосой пропускания, предоставляемой классу во время затора.
Пакеты, относящиеся к классу, подпадают под ограничения пропускной способности и очереди, которые характеризуют этот класс.

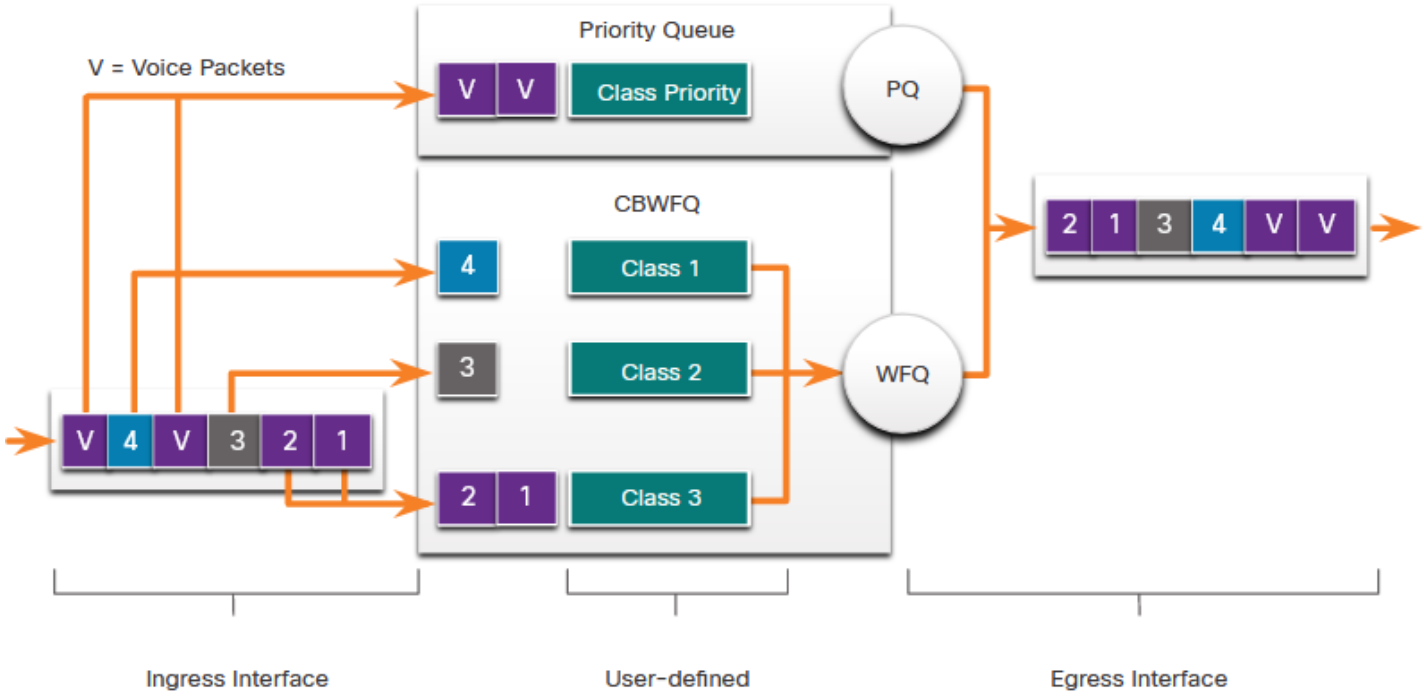
9.3.3 ВЗВЕШЕННАЯ ОРГАНИЗАЦИЯ ОЧЕРЕДЕЙ НА ОСНОВЕ КЛАССОВ (CBWFQ)

После того как очередь достигает заданного ей ограничения, добавление дополнительных пакетов в класс приводит к отбрасыванию пакетов — либо с конца, либо согласно настроенной политике класса.
Отбрасывание с конца — это когда маршрутизатор просто отклоняет любой пакет, который поступает в конец очереди, если ресурсы для хранения пакетов полностью заняты.
Таким образом механизм организации очереди реагирует по умолчанию на затор. Отбрасывание с конца приводит к одинаковой обработке всего трафика, независимо от класса обслуживания.



9.3.4 ОРГАНИЗАЦИЯ ОЧЕРЕДИ С МАЛОЙ ЗАДЕРЖКОЙ (LLQ)

Функция LLQ определяет строгий порядок формирования очередей по приоритетам (PQ) для CBWFQ.
Строгий порядок формирования очередей (PQ) позволяет отправлять чувствительные к задержке данные, например голос, перед пакетами в других очередях.
LLQ позволяет в первую очередь (до обработки пакетов в других очередях) отправлять чувствительные к задержкам данные, что обеспечивает предпочтительную обработку таких данных относительно остального трафика.
Cisco рекомендует направлять в очередь приоритетов только голосовой трафик.



9.4 МОДЕЛИ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ

9.4.1 ВЫБОР ПОДХОДЯЩЕЙ МОДЕЛИ ПОЛИТИКИ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Существует три модели реализации политики качества обслуживания. На самом деле, качество обслуживания (QoS) в сети реализуется с помощью моделей IntServ или DiffServ.

Модель **IntServ** обеспечивает максимальную гарантированную полосу пропускания, однако очень требовательна к ресурсам и, следовательно, ограничивает масштабируемость.

DiffServ — менее ресурсоемкая и более масштабируемая модель.

Иногда эти модели реализуются вместе для обеспечения необходимого уровня качества обслуживания.

9.4.1 ВЫБОР ПОДХОДЯЩЕЙ МОДЕЛИ ПОЛИТИКИ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Модель	Описание
Модель без гарантированной доставки	По сути, не является реализацией, поскольку явная настройка качества обслуживания отсутствует. Используется, когда гарантированная полоса пропускания не требуется.
Интегрированные сервисы (IntServ)	Обеспечивает очень высокое качество обслуживания для IP-пакетов с гарантированной доставкой. Определяет процесс сигнализации для приложений, которые могут уведомлять сеть о том, что им требуется особое качество обслуживания на определенный период и для этого необходимо зарезервировать пропускную способность. Однако модель IntServ может серьезно ограничивать масштабируемость сети.
Дифференцированные услуги (DiffServ)	Предоставляет высокую масштабируемость и адаптивность в реализации качества обслуживания. Сетевые устройства распознают классы трафика и предоставляют различные уровни качества обслуживания для разных классов трафика.

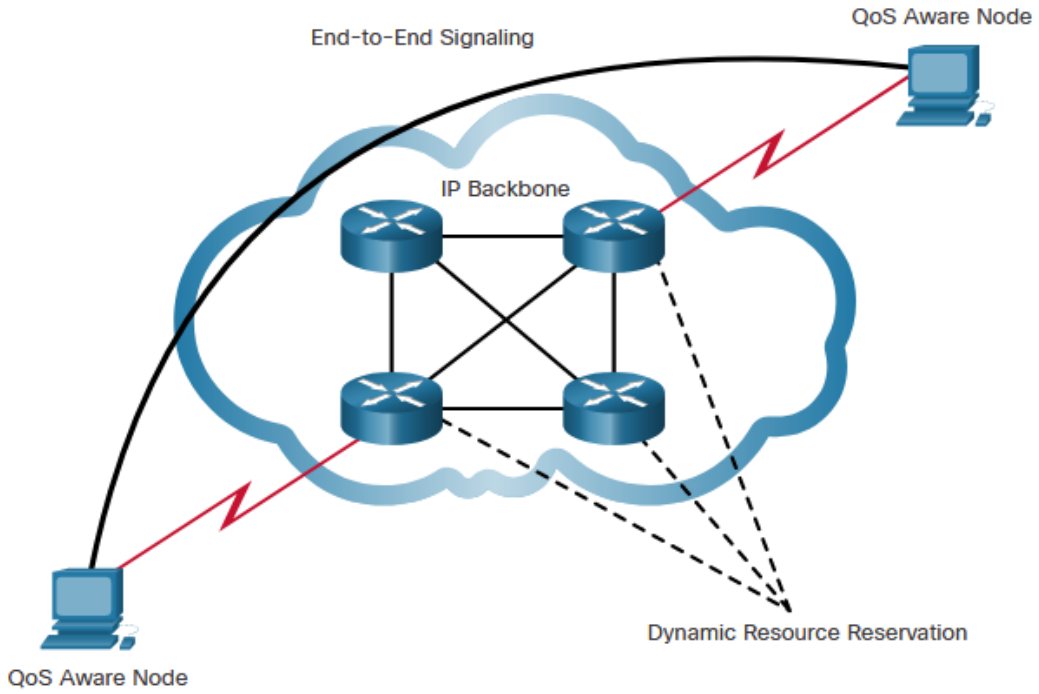
9.4.2 BEST EFFORT - МОДЕЛЬ БЕЗ ГАРАНТИРОВАННОЙ ДОСТАВКИ

Базовая модель для Интернета обеспечивает негарантированную доставку пакетов.
Модель без гарантированной доставки обращается со всеми сетевыми пакетами одинаковым образом, поэтому экстренное голосовое сообщение обрабатывается так же, как и цифровая фотография во вложении электронного сообщения.
Преимущества и недостатки модели без гарантированной доставки указаны в таблице.

Преимущества	Недостатки
Это самая масштабируемая модель.	Нет гарантии доставки.
Масштабируемость ограничена только пропускной способностью. При таком ограничении воздействие на весь трафик одинаково.	Пакеты прибывают, когда могут, и в любом порядке (если прибывают вообще).
Никакие специальные механизмы QoS не требуются.	Приоритетная обработка пакетов не предусмотрена.
Это самая простая и быстрая в развертывании модель.	Критически важные данные обрабатываются так же, как и обычные письма.

9.4.3 ИНТЕГРИРОВАННЫЕ СЕРВИСЫ

IntServ обеспечивает сквозное качество обслуживания, которое требуется приложениям реального времени.
Явно управляет сетевыми ресурсами для обеспечения качества обслуживания отдельных потоков или потоков, иногда называемых микропотоками.
В этой модели в качестве базовых компонентов используются механизмы резервирования ресурсов и контроля доступа, которые позволяют определять политику QoS и обеспечивать ее выполнение.
Использует ориентированный на подключение подход к QoS. Каждое отдельное сообщение должно явно объявлять в сети свой дескриптор трафика и запрошенные ресурсы.
Пограничный маршрутизатор осуществляет контроль допуска, чтобы убедиться, что в сети имеются достаточные ресурсы.



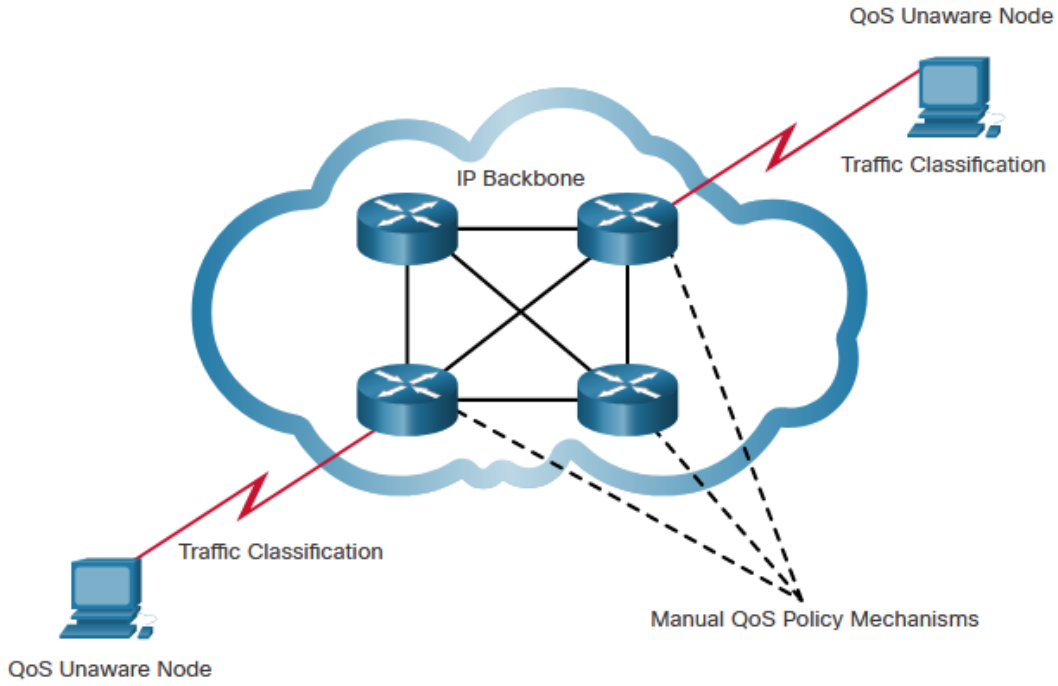
9.4.3 ИНТЕГРИРОВАННЫЕ СЕРВИСЫ

В модели IntServ приложение запрашивает конкретный тип обслуживания у сети перед отправкой данных.
Приложение сообщает сети свой профиль трафика и запрашивает конкретный тип обслуживания, который может включать требования к пропускной способности и задержкам.
Модель IntServ использует протокол RSVP для уведомления устройств на всем пути следования трафика по сети о потребностях приложения в качестве обслуживания.
Если сетевые устройства на пути следования трафика способны зарезервировать необходимую пропускную способность, исходное приложение может начать передачу. Если запрошенное резервирование на всем пути недоступно, исходное приложение не отправляет данные.

Преимущества	Недостатки
• Явное сквозное управление доступом к ресурсам. • Контроль доступа для каждого запроса. • Сигнальная передача динамических номеров портов.	• Высокая потребность в ресурсах из-за необходимости непрерывной сигнализации в архитектуре с сохранением состояния. • Подход, ориентированный на потоки, плохо реализуется в масштабных развертываниях, таких как Интернет.

9.4.4 ДИФФЕРЕНЦИРОВАННЫЕ УСЛУГИ

Модель дифференцированных сервисов (DiffServ) определяет простой и масштабируемый механизм для классификации и управления сетевым трафиком и гарантии качества обслуживания в современных IP-сетях.
Модель DiffServ не является сквозной стратегией качества обслуживания, поскольку не предоставляет сквозных гарантий.
Пересылает трафик на маршрутизатор, который классифицирует потоки на агрегаты (классы) и предоставляет соответствующую политику QoS для классов.
В модели DiffServ механизмы качества обслуживания применяются на уровне переходов, когда каждому классу трафика единообразно присваивается глобальное значение, что обеспечивает и гибкость, и масштабируемость.



9.4.4 ДИФФЕРЕНЦИРОВАННЫЕ УСЛУГИ

DiffServ делит сетевой трафик на классы, основываясь на требованиях бизнеса. После этого каждому классу можно назначить свой уровень обслуживания.
При прохождении пакетов по сети каждое сетевое устройство определяет класс пакета и обрабатывает этот пакет в соответствии с требованиями для данного класса.
Модель DiffServ предусматривает выбор из нескольких уровней обслуживания.

Преимущества	Недостатки
• Высокий уровень масштабирования. • Разнообразие уровней качества.	• Нет полной гарантии качества предоставления услуг. • Необходимость слаженной работы комплекса сложных механизмов во всей сети.

9.5 СПОСОБЫ РЕАЛИЗАЦИИ QOS
9.5.1 ПРЕДОТВРАЩЕНИЕ ПОТЕРИ ПАКЕТОВ

Потеря пакетов обычно возникает из-за заторов на интерфейсе. Большинство приложений, использующих TCP, сталкиваются с замедлением работы, поскольку при заторах в сети автоматически происходит регулировка TCP-трафика. Потерянные сегменты TCP приводят к увеличению размеров окон сеансов TCP. Некоторые приложения не используют TCP и не могут обрабатывать потерянные сегменты (уязвимые потоки).

Можно предотвратить потери пакетов для важных приложений, используя методы:

1. Увеличение пропускной способности для уменьшения или предотвращения заторов.

2. Резервирование достаточной пропускной способности и увеличение объема буфера, чтобы гарантировать обработку всплесков трафика в уязвимых потоках. WFQ, CBWFQ и LLQ могут гарантировать пропускную способность и обеспечить приоритетную переадресацию в приложения, чувствительные к отбросу.

3. Сокращение объема трафика за счет отбрасывания пакетов с низким приоритетом. Cisco IOS QoS предоставляет механизмы организации очередей, такие как взвешенное случайное раннее обнаружение (WRED), которые начинают отбрасывать пакеты с более низким приоритетом до того, как происходит перегрузка.

9.5.2 ИНСТРУМЕНТЫ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Существует три категории инструментов качества обслуживания:

Инструменты QoS	Описание
Инструменты для классификации и маркировки	• Сеансы или потоки анализируются на принадлежность определенному классу трафика. • При определении класса трафика пакеты помечены.
Инструменты для предотвращения заторов	• Классам трафика выделяются фрагменты сетевых ресурсов в соответствии с политикой качества обслуживания. • Политика качества обслуживания определяет порядок удаления, задержки или перемаркировки некоторого трафика для предотвращения заторов. • Основным инструментом предотвращения перегрузки является WRED, он используется для регулировки трафика данных TCP с целью оптимизации пропускной способности и предотвращения отбрасываний последнего элемента из-за переполнения очереди.
Инструменты для управления заторами	• Когда объем трафика превышает доступные сетевые ресурсы, трафик ставится в очередь ожидания доступных ресурсов. • Для управления заторами в Cisco IOS обычно используются алгоритмы CBWFQ и LLQ.

9.5.2 ИНСТРУМЕНТЫ КАЧЕСТВА ОБСЛУЖИВАНИЯ

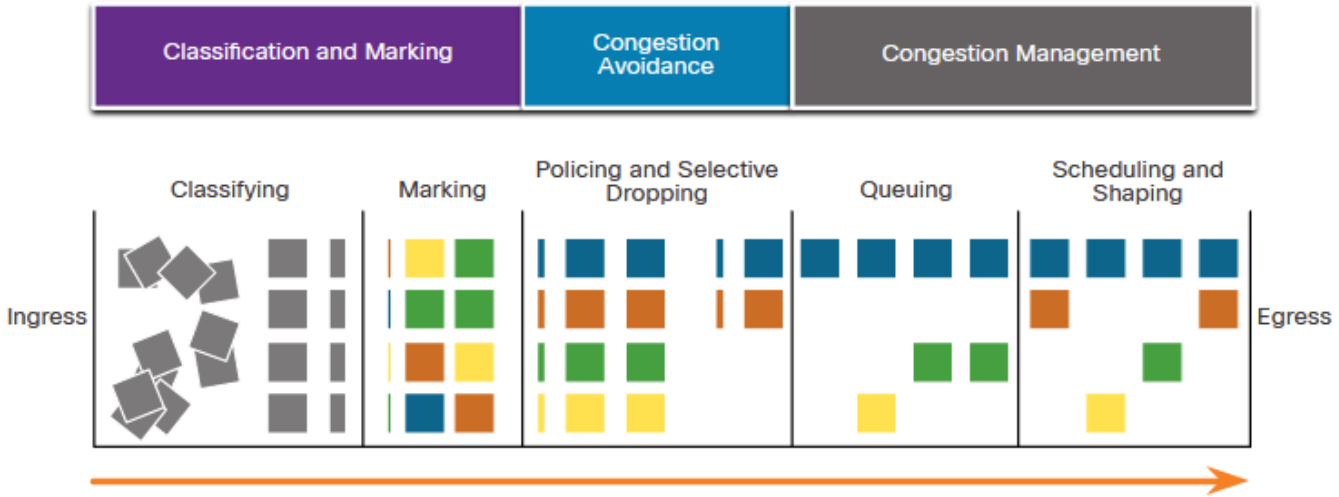
На рисунке показана последовательность использования этих трех инструментов.

Входные пакеты (серые квадраты) классифицируются, а их IP-заголовки маркируются.

Чтобы избежать заторов, пакетам назначаются ресурсы на основании заданных политик.

После этого пакеты ставятся в очередь и пересылаются из выходного интерфейса на основании заданной политики качества обслуживания, шейпинга и полисинга.

Примечание. Классификацию и маркировку можно проводить и на входе, и на выходе, а другие действия, связанные с качеством обслуживания, например, постановку в очередь и шейпинг трафика, обычно выполняют на выходе.



9.5.3 КЛАССИФИКАЦИЯ И МАРКИРОВКА

Чтобы применить политику качества обслуживания к пакету, пакет нужно классифицировать.

Классификация определяет класс трафика, к которому относятся пакеты или кадры. Применять политики можно только к маркированному трафику.

Классификация пакета зависит от реализации политики качества обслуживания.

При классификации потоков трафика на уровне 2 и 3 используются интерфейсы, списки контроля доступа и карты классов.

Трафик также можно классифицировать на уровнях с 4-го по 7-й с помощью распознавания приложений по параметрам сетевого трафика (Network Based Application Recognition, NBAR).

9.5.3 КЛАССИФИКАЦИЯ И МАРКИРОВКА

Маркировка трафика обычно зависит от используемой технологии передачи данных. Решение о маркировке трафика на уровне 2 и 3 (или на обоих уровнях) непростое и должно приниматься с учетом следующих факторов.

Маркировку уровня 2 для кадров можно выполнять для трафика, отличного от IP-трафика.

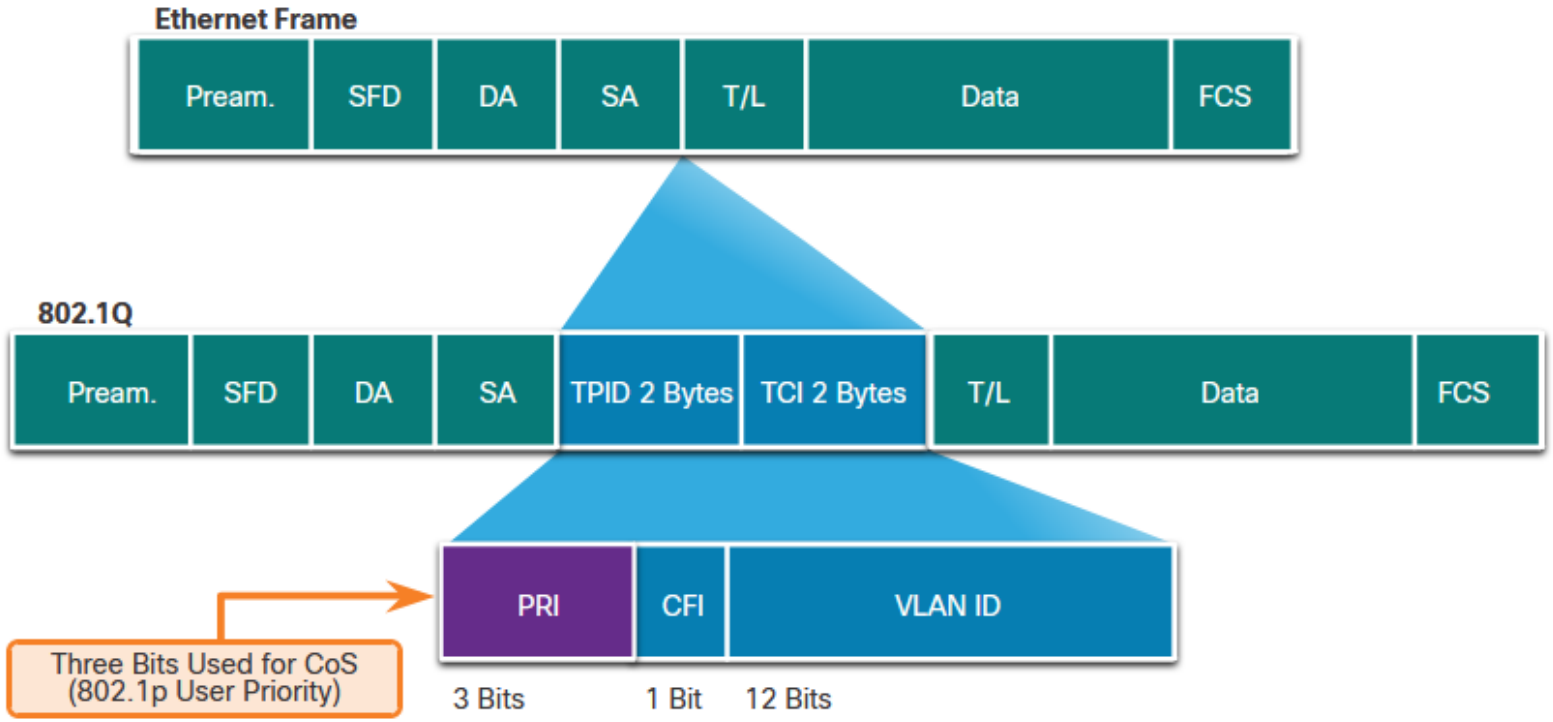
Маркировка уровня 2 для кадров является единственным возможным вариантом реализации качества обслуживания для коммутаторов, не поддерживающих IP.

Маркировка уровня 3 обеспечивает сквозную передачу данных о качества обслуживания.

Инструменты QoS	Уровень	Поле маркирования	Ширина в битах
Ethernet (802.1q, 802.1p)	2	Класс обслуживания (CoS)	3
802.11 (Wi-Fi)	2	Идентификатор трафика беспроводной сети (TID)	3
MPLS	2	Экспериментальное (EXP)	3
IPv4 и IPv6	3	Приоритет IP (IPP)	3
IPv4 и IPv6	3	Точка кода дифференцированных сервисов (DSCP)	6

9.5.4 МАРКИРОВКА НА УРОВНЕ 2

802.1Q — стандарт IEEE, который поддерживает маркировку трафика VLAN на уровне 2 в сетях Ethernet. При реализации 802.1Q в кадр Ethernet добавляются два поля после поля MAC-адреса источника, как показано на рисунке слева.



9.5.4 МАРКИРОВКА НА УРОВНЕ 2

Стандарт 802.1Q также включает схему установки приоритетов QoS, известную как IEEE 802.1p. Стандарт 802.1p использует первые три бита в поле контрольных данных тега (TCI). Это трехбитное поле называется полем приоритета (PRI) и определяет маркировку класса обслуживания (CoS).

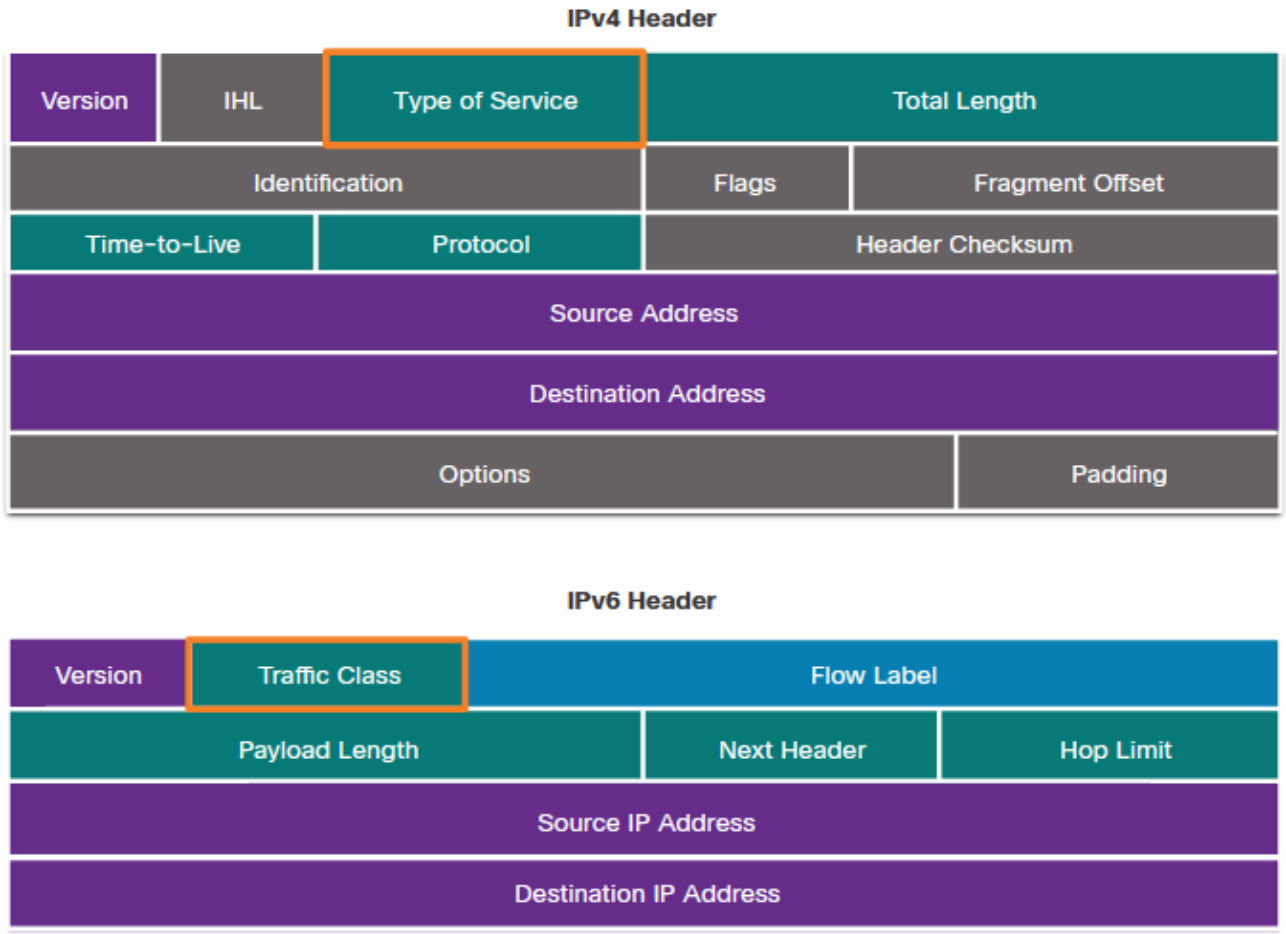
Маркировка CoS позволяет маркировать кадр Ethernet уровня 2 приоритетом одного из восьми уровней (значения 0–7), как показано на рисунке.

Значение класса обслуживания (CoS)	Двоичное значение класса обслуживания (CoS)	Описание
0	000	Данные с низким приоритетом
1	001	Данные со средним приоритетом
2	010	Данные с высоким приоритетом
3	011	Сигнализация вызовов
4	100	Видео-конференц-связь
5	101	Голосовой канал (трафик голосовых данных)
6	110	Зарезервировано
7	111	Зарезервировано

9.5.5 МАРКИРОВКА НА УРОВНЕ 3

В протоколах IPv4 и IPv6 имеется 8-битное поле в заголовке пакета, позволяющее маркировать пакеты.

Как показано на рисунке, оба протокола IPv4 и IPv6 поддерживают 8-битное поле для маркировки, поле типа обслуживания (ToS) для IPv4 и поле класса трафика для IPv6.



9.5.6 ТИП ОБСЛУЖИВАНИЯ И ПОЛЕ КЛАССА ТРАФИКА

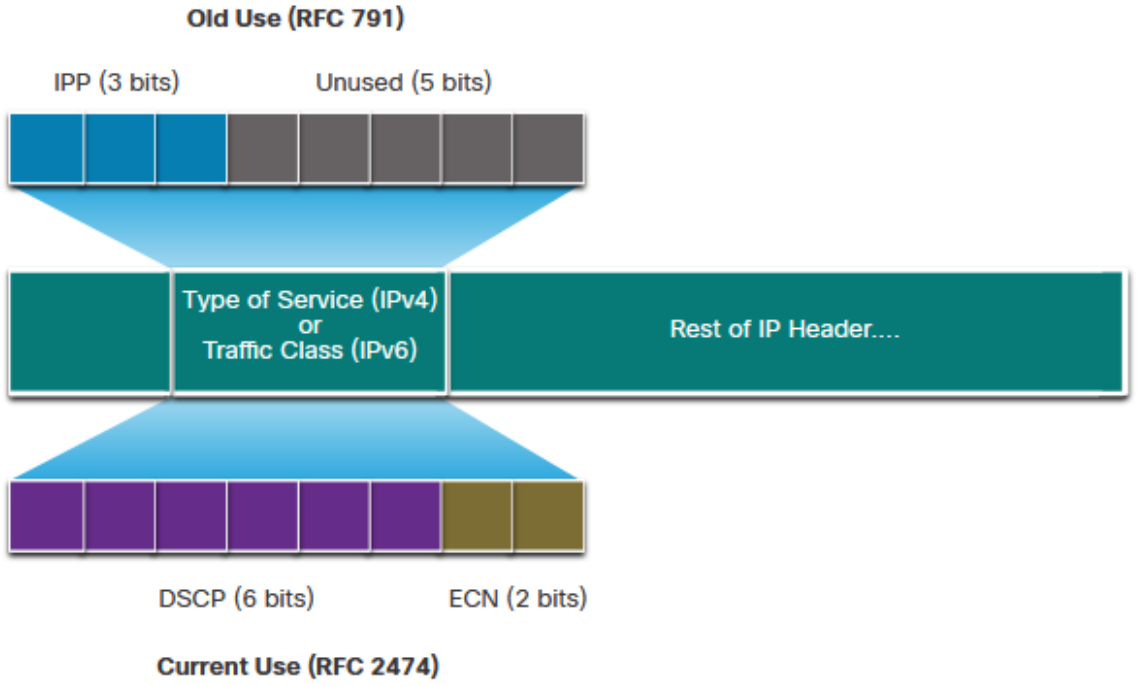
Тип службы (IPv4) и класс трафика (IPv6) несут маркировку пакетов, назначенную средствами классификации QoS.

В RFC 791 оригинальный стандарт для IP определяет поле приоритета IP (IPP), используемое для маркировки QoS.

RFC 2474 заменяет RFC 791 и переопределяет поле типа обслуживания (ToS) через переименование и расширение поля IPP.

Оно называется полем точки кода дифференцирования трафика (DSCP) и за счет этих 6 бит предлагает до 64 возможных классов обслуживания.

Остальные 2 бита расширенного уведомления о перегрузке IP (ECN) могут использоваться маршрутизаторами, поддерживающими расширение ECN, для маркировки пакетов вместо их удаления.



9.5.7 ЗНАЧЕНИЯ DSCP

64 значения DSCP организованы в три категории.

Без гарантированной доставки (BE) — это категория по умолчанию для всех IP-пакетов. Значение DSCP равно 0. Пошаговое обслуживание (PHB) является нормальной маршрутизацией. Когда на маршрутизаторе возникает затор, эти пакеты отбрасываются. Никакой схемы качества обслуживания не применяется.

Ускоренная пересылка (EF) — RFC 3246 назначает EF десятичное значение DSCP 46 (двоичный код 101110). Первые 3 бита (101) сопоставляются со значением 5 CoS уровня 2, используемого для трафика голосовых данных. На уровне 3 Cisco рекомендует использование EF только для маркировки пакетов голосовых данных.

Гарантированная пересылка (Assured Forwarding) — RFC 2597 выделяет для AF пять самых старших битов DSCP для определения очереди и приоритета отбрасывания.

9.5.7 ЗНАЧЕНИЯ DSCP

На рисунке показаны гарантированная пересылка.

Формула AFxy задается следующим образом:

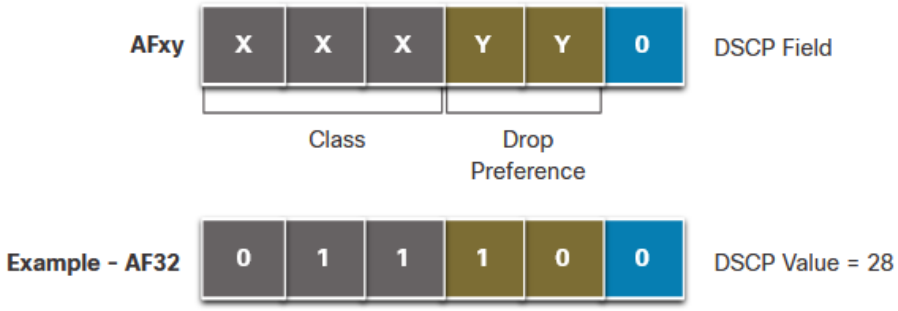
Первые три самых старших бита используются для определения класса. Класс 4 означает очередь с самым высоким приоритетом, класс 1 — с самым низким приоритетом.

4-й и 5-й (самые старшие биты) используются для определения приоритета отбрасывания.

6-й (самый старший бит) устанавливается равным нулю.

Например, AF32 принадлежит классу 3 (двоичный код 011), и для нее устанавливается средний приоритет отбрасывания (двоичный код 10). Полное значение DSCP равно 28, поскольку в него включается нулевое значение 6-го (самого старшего) бита (двоичный код 011100).

Assured Forwarding Values			
	Low Drop	**Medium Drop**	**High Drop**
Class 4	AF41 (34)	AF42 (36)	AF43 (38)
Class 3	AF31 (26)	AF32 (28)	AF33 (30)
Class 2	AF21 (18)	AF22 (20)	AF23 (22)
Class 1	AF11 (10)	AF12 (12)	AF13 (14)

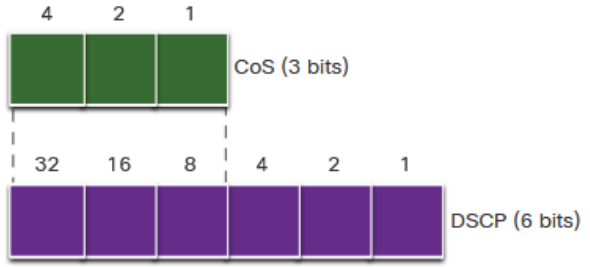


9.5.8 БИТЫ ВЫБОРА КЛАССА (CS)

Биты выбора класса (CS):

Первые 3 наиболее значимых бита поля DSCP и указывают класс.

Три бита точно соответствуют трем битам полей CoS и IPP для обеспечения совместимости со стандартами 802.1p и RFC 791.



CoS values, Class Selectors, and corresponding DSCP 6-bit value

CoS Value	CoS Binary Value	Class Selector (CS)	CS Binary	DSCP Decimal Value
0	000	CS0*/DF	000 000	0
1	001	CS1	001 000	8
2	010	CS2	010 000	16
3	011	CS3	011 000	24
4	100	CS4	100 000	32
5	101	CS5	101 000	40
6	110	CS6	110 000	48
7	111	CS7	111 000	56

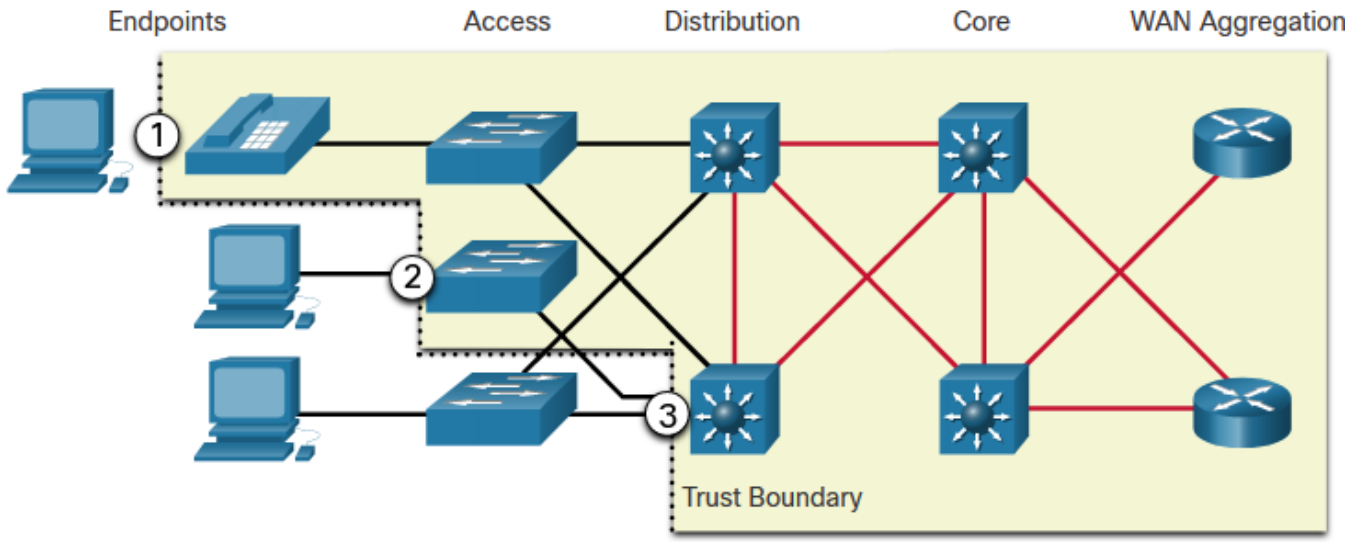
9.5.9 ГРАНИЦЫ ДОВЕРИЯ

Трафик нужно классифицировать и маркировать настолько близко к источнику, насколько это оправдано с технической и административной точки зрения. Это определяет границу доверия, как показано на рисунке.

Доверенные оконечные устройства могут и умеют маркировать трафик приложений соответствующими значениями CoS уровня 2 и значениями DSCP уровня 3.

Защищенные оконечные устройства могут работать с трафиком, маркированным на коммутаторе уровня 2.

Трафик также можно маркировать на коммутаторах и маршрутизаторах уровня 3.



9.5.10 ПРЕДОТВРАЩЕНИЕ ЗАТОРОВ

Инструменты предотвращения перегрузок отслеживают распределение сетевого трафика с целью предугадать и предотвратить возникновение заторов в узких местах общей сети до того, как возникнет серьезная проблема.

Они отслеживают распределения сетевого трафика, пытаясь предугадать и предотвратить заторы в типичных узких местах внутри сети и между сетями до того, как затор превратится в серьезную проблему.

Эти инструменты отслеживают среднюю глубину очереди. Когда заполнение очереди меньше минимального порогового значения, никакие пакеты не отбрасываются. Когда очередь заполняется до максимального порогового значения, отбрасывается небольшой процент пакетов. Если заполнение превышает максимальное пороговое значение, отбрасываются все пакеты.

Некоторые методы предотвращения заторов предлагают установку приоритетов, при которых пакеты будут отброшены.

Алгоритм WRED позволяет избегать заторов на сетевых интерфейсах за счет предоставления инструментов управления буферизацией и снижения или отбрасывания трафика TCP до того, как буфер будет переполнен.

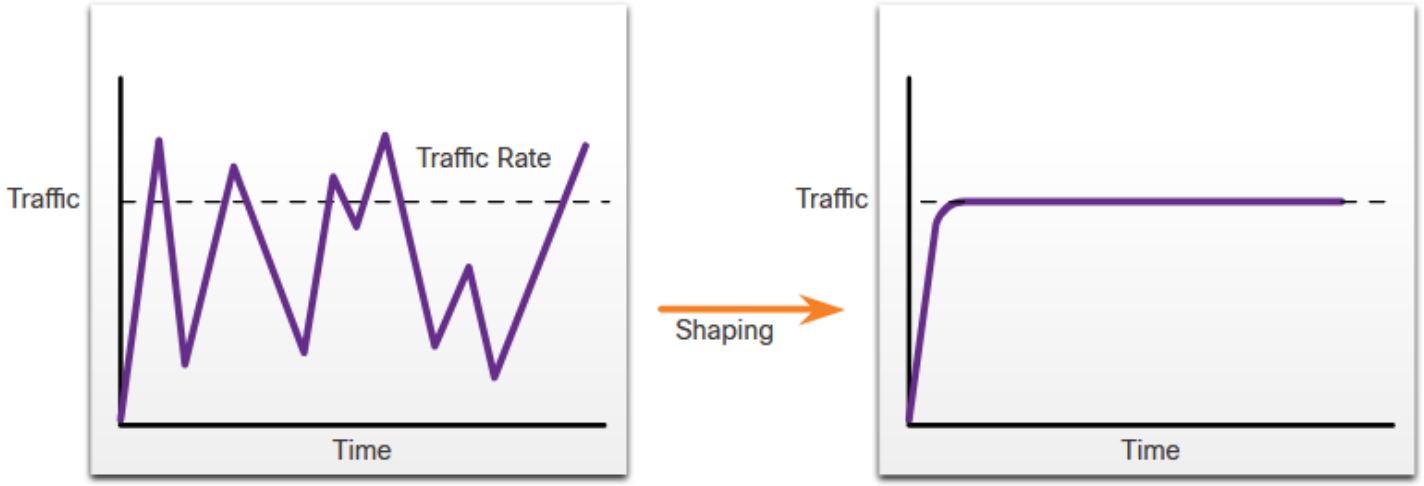
WRED помогает избежать отбрасывания последнего элемента и оптимизирует использование сетевых мощностей и производительность приложений, использующих TCP.

9.5.11 ФОРМИРОВАНИЕ И ОГРАНИЧЕНИЕ ТРАФИКА

Шейпинг трафика и **полисинг трафика** — это механизмы предотвращения заторов Cisco IOS.

Шейпинг трафика сохраняет лишние пакеты в очереди, а затем планирует последующую передачу этих пакетов через определенные промежутки времени. Формирование трафика приводит к сглаженной скорости вывода пакетов.

Шейпинг связан с управлением исходящим трафиком. Пакеты, исходящие через интерфейс, помещаются в очередь, и к ним может применяться шейпинг. Напротив, к входящему трафику на интерфейсе может применяться только ограничение.



9.5.11 ФОРМИРОВАНИЕ И ОГРАНИЧЕНИЕ ТРАФИКА

К входящему трафику на интерфейсе может применяться только ограничение (полисинг). Ограничение трафика обычно применяется операторами связи для обеспечения соблюдения показателя гарантированной скорости передачи данных (CIR). Однако оператор связи может также предусмотреть превышение показателя гарантированной скорости передачи данных, если его сеть в текущий момент не перегружена.

9.5.12 ОГРАНИЧЕНИЕ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Политики QoS должны учитывать полный путь от источника к месту назначения.

Некоторые рекомендации, которые помогают обеспечить наилучший опыт для конечных пользователей, включают следующее:

1. Включите очередь на каждом устройстве в пути между источником и назначением.

2. Сетевой трафик классифицируется и маркируется максимально близко к исходному устройству.

3. Шейпинг и полисинг транспортных потоков как можно ближе к их источникам.