

Применение качества обслуживания

Содержание

[Введение](#)

[Каким приложениям требуется QoS?](#)

[Общие сведения о характеристиках приложений](#)

[Знакомство с топологией сети](#)

[Размеры заголовков уровня канала](#)

[Создание классов на основе критериев](#)

[Создание политики для отметки каждого класса](#)

[Работа от краев к центру](#)

[Создание стратегии интерпретации трафика](#)

[Применение политики](#)

[Использование администратора политики QoS \(QPM\) для наблюдения за эффективностью политики](#)

[Общие рекомендации QoS](#)

[Дополнительные сведения](#)

Введение

Данный документ содержит некоторые указания высокого уровня для реализации QoS в сетях, предоставляющих транспорт для нескольких приложений, включая чувствительные к задержке и приложения с интенсивным использованием полосы пропускания. Данные приложения позволяют усовершенствовать бизнес-процессы, но расходуют дополнительные ресурсы сети. QoS обеспечивает безопасное, предсказуемое, измеримое и гарантированное обслуживание приложений путем управления задержками, изменением задержек (разбросом), пропускной способностью и потерей пакетов в сети.

Каким приложениям требуется QoS?

Во-первых, определите, какие приложения критически важны для бизнеса и требуют защиты. Может понадобиться проверить все приложения, которые конкурируют в борьбе за сетевые ресурсы. [Используйте в данном случае учет Netflow, сетевое распознавание приложений \(NBAR\) или диспетчер устройств QoS \(QDM\) для анализа моделей трафика в сети.](#)

NetFlow Accounting предоставляет детальные данные о сетевом трафике и может быть использована для сбора классификации трафика или приоритета операций, связанных с каждым потоком.

NBAR – это средство классификации, которое может распознавать трафик вплоть до уровня приложения. Это предоставляет по-интерфейсную, по-протокольную и двунаправленную статистику для каждого потока данных, проходящего через интерфейс. NBAR также делает

классификацию суб - портов; взгляд и определение вне портов приложения.

QDM является Веб - приложение для управления сетью, который предоставляет простой в использовании графический интерфейс пользователя для настройки и мониторинга усовершенствованного на основе IP функциональность QoS в маршрутизаторах.

Общие сведения о характеристиках приложений

Важно понимать характеристики приложений, нуждающихся в защите. Если одни приложения могут быть чувствительны ко времени ожидания и потере пакетов, то другие считаются "агрессивными", поскольку создают всплески трафика или используют большую часть пропускной способности канала. Если приложение является пульсирующим, определите, существует ли постоянный пакет или маленький пакет. Является ли размер пакета приложения большим или малым? Приложение основано на TCP или UDP?

Характеристика	Рекомендация
Приложение, которое чувствительно к задержке или к потере. (Голос и живое видео)	<i>Не используйте механизм взвешенного случайного раннего обнаружения (WRED), формирование трафика, фрагментацию (FRF-12) или ограничение скорости. Для этого вида трафика необходимо внедрить Организацию очереди с малой задержкой (LLQ) и использовать очередь с приоритетами для трафика чувствительный к задержке.</i>
Приложение, которое постоянно создает пульсирующий трафик или захват полосы пропускания. (FTP и HTTP)	Используйте WRED, применение политик, формирование трафика или взвешенную организацию очереди на основе классов (CBWFQ) для гарантии пропускной способности.
Приложение на основе TCP.	Используйте WRED, поскольку утерянные пакеты заставляют протокол TCP сбавить скорость передачи, а потом снова нарастить ее с помощью алгоритма медленного старта. Если трафик основан на UDP и не изменяет свое поведение, когда пакеты отброшены, не используйте WRED. Используйте Применение политик при необходимости к rate-limit в приложении; иначе просто позвольте

[Знакомство с топологией сети](#)

Некоторым устройствам, возможно, понадобится обновление IOS для пользования преимуществами Характеристики QoS, которые вы хотите внедрить. Схемы топологии сети, конфигураций маршрутизатора и версии программного обеспечения на каждом устройстве помогают вам оценивать количество устройств, требующее обновления IOS. См.

[Библиотеку значков Cisco](#) для значков, которые могут помочь вам создавать схемы сети.

- Оцените загрузку ЦПУ на каждом маршрутизаторе во время интервалов занятости, чтобы помочь решить, как распределить Характеристики QoS среди устройств для совместного использования загрузки.
- Классифицируйте категории трафика критически важного для бизнеса и интерфейсы, которые пересечет этот трафик. Решите, какие приоритетные группы или классы создать для реализации целей QoS в вашей сети.
- Определите максимальную задержку, которую может поддерживать большинство критически важных приложений, и настройте параметры блока данных в приложениях обработки трафика (формирование трафика или ограничение скорости) для согласования данной задержки.
- Узнайте, какие скорости поддерживаются на каждом интерфейсе: PVC или подчиненные интерфейсы, и настройте соответственно пропускную способность.
- Определите медленные соединения, чтобы помочь определять, где узкие места в сети расположены и решают, как применить Механизмы эффективности линии связи в соответствующих интерфейсах.
- Вычислите издержки Уровня 2 и Уровня 3 для каждого типа носителя, который передаст критически важный для бизнеса трафик. Это поможет вычислить правильную величину полосы пропускания, необходимую для каждого класса.
- Другая важная часть информации - хотите ли вы защитить трафик на основе приложения, Источника IP и назначения или обоих.

[Размеры заголовков уровня канала](#)

Тип носителя	Заголовок уровня канала
Ethernet	14 байтов
PPP	6 байт
Frame Relay	4 байта
ATM	5 байтов/яч

[Создание классов на основе критериев](#)

Как только вы определяете, который для приложений нужны QoS и критерии классификации для использования (на основе характеристик приложений), вы готовы создать классы на основе этой информации.

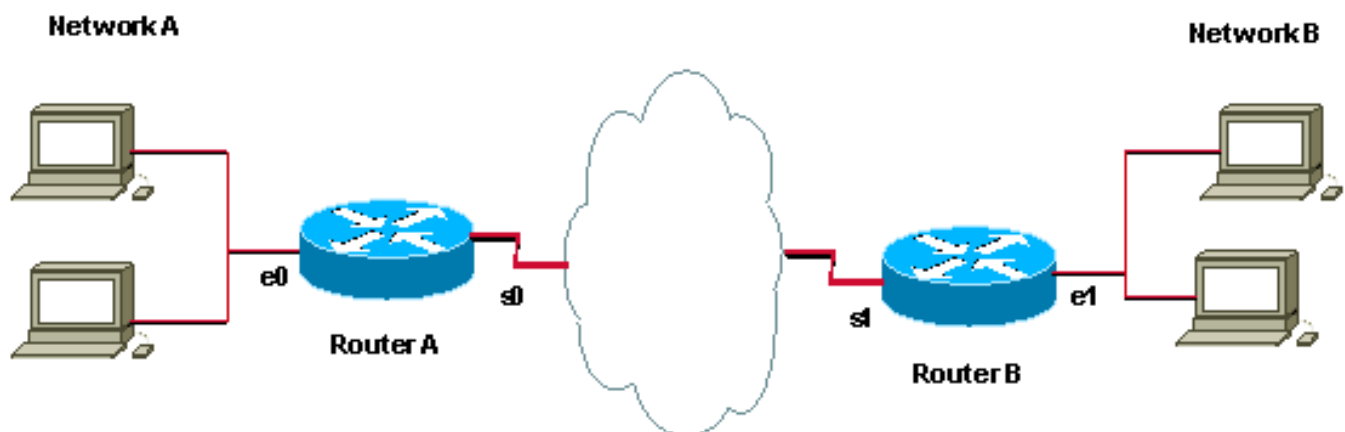
[Создание политики для отметки каждого класса](#)

Создайте политику для маркирования каждого класса трафика подходящими значениями приоритета (используйте точку дифференцированных кодов обслуживания или приоритет IP). При поступлении на входящий интерфейс маршрутизатора трафик будет помечен. Маркировки будут использоваться для обработки трафика, поскольку он оставляет маршрутизатор на исходящем интерфейсе.

Работа от краев к центру

Работайте от маршрутизатора, самого близкого к трафику к ядру. Примените свою маркировку на входной интерфейс маршрутизатора. В топологии ниже, маршрутизатор А является очевидным местом, чтобы отметить трафик и применить политику для источника данных от Сети А и предназначенный для маршрутизатора В. Трафик будет отмечен, поскольку он входит в интерфейс Ethernet0 А маршрутизатора, и политика QoS будет применена на интерфейс Serial0 А маршрутизатора, поскольку он оставляет маршрутизатор. Если та же политика должна быть применена в обоих направлениях (так, чтобы трафик, полученный от Сети В и, предназначенный для Сети А, проходит то же лечение), трафик, прибывающий из Сети В, должен быть отмечен, поскольку это входит в интерфейс Ethernet1 В маршрутизатора и рассматривало, поскольку это оставляет маршрутизатор на интерфейсе Serial1.

Как только трафик отмечен на входном интерфейсе на одном маршрутизаторе, это поддерживает те же маркировки, как это пересекает множественные переходы (пока это не отмечено). Как правило, трафик маркируется один раз. Политики QoS могут быть применены на дополнительные переходы, основанные на этих маркировках. Повторное маркирование требуется только в том случае, если трафик поступает из домена без доверия.



Создание стратегии интерпретации трафика

После маркировки трафика можно использовать метки для построения политики и для классификации трафика в остальных сегментах сети. Рекомендуется не усложнять политику, используя не более четырех классов.

По возможности выполните и протестируйте реализацию QoS в лабораторной среде. Получив удовлетворительные результаты, разверните его в действующей сети.

Применение политики

Примените политику в соответствующем направлении. Определите, нужно ли политику применять в одном направлении или обоих. Всегда метка и трафик обработки максимально близко к источнику, как описано в [Создании Политики](#) к разделу [Марка Ича Класса](#) этого документа.

Рекомендуется применять одну политику в обоих направлениях, чтобы выполнять фильтрацию трафика, получаемого и отправляемого на обе стороны узла. Это означает, что необходимо применить ту же политику ограничения исходящего трафика к последовательным интерфейсам маршрутизаторов А и Б.

Использование администратора политики QoS (QPM) для наблюдения за эффективностью политики

Используйте [QPM](#) в качестве полной системы для централизованного управления политиками и автоматизированный, надежное внедрение сетевых политик.

Общие рекомендации QoS

Ниже представлен список категорий QoS и некоторые наиболее часто используемые функции QoS, связанные с каждой категорией.

Категория	Связанные функции QoS
Служебная модель QoS	Гарантированная (Diffserv) QoS по возможности или сигнальная (RSVP) при необходимости.
Классификация/Маркировать	DiffServ Code Point или идентификатор группы qos.
Управление перегрузкой	LLQ или CBWFQ.
Предотвращение перегрузок	WRED совместимости с Diffserv.
Эффективность канала	MLPPP, LFI, FRF.11, FRF.12, CRTP
Сигнализация	RSVP, QPPB
Формирование трафика и применение политик	Класс базирующийся ограничитель и Generic Traffic Shaping (GTS) или формирование трафика Frame Relay (FRTS).
Конфигурация/Мониторинг	QPM, модульный интерфейс командной строки QoS (CLI), QDM

Дополнительные сведения

- [Страница поддержки QoS](#)

- [Протоколы маршрутизируемые по IP](#)
- [Страница поддержки IP-маршрутизации](#)
- [Страница поддержки IS-IS](#)
- [Техническая поддержка - Cisco Systems](#)