Сравнение определения политик на основе классов и фиксированной частоты доступа

Содержание

Введение

Этот документ разъясняет различия между согласованной скоростью доступа (CAR), которая является функцией мониторинга трафика традиционного синтаксиса Cisco и основанным на классе применением политик, которое является более новым ограничителем трафика Cisco. Основанное на классе применение политик внедрено в модульном качестве сервиса (QoS) интерфейс командной строки (CLI) (MQC) путем настройки политики обслуживания. Основанное на классе применение политик, также известное как мониторинг трафика, было представлено в программном обеспечении Cisco IOS 12.1 (5) T.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью

осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Что такое ограничитель трафика?

Мониторинг трафика управляет максимальной скоростью трафика, передаваемой или полученной на интерфейсе. На основе результатов измерения ТВ действие может быть настроено для маркировки пакетов и отдельных пакетов во множественные классы или уровни обслуживания.

Ограничители трафика предоставляют два ключевых преимущества:

- **Управление пропускной способностью посредством ограничения скорости** - Позволяет вам управлять максимальной скоростью трафика, передаваемой или полученной на интерфейсе. Мониторинг трафика часто настраивается на интерфейсах в краю сети для ограничения трафика в или из сети. Трафик, который находится в пределах параметров скорости передачи, передается, тогда как трафик, который превышает параметры, отброшен или передан с другим приоритетом.
- **Маркировка пакетов с помощью установки IP-приоритета, группы QoS или значения параметра DSCP – Маркировка пакетов позволяет разделить сеть на уровни с разным приоритетом или классы обслуживания (CoS).**

Используйте мониторинг трафика для установки значений приоритета IP-трафика или значений точки кода дифференцированных услуг (DSCP) для пакетов, вводящих сеть. Сетевые устройства в вашей сети могут тогда использовать отрегулированные Значения приоритета IP-трафика, чтобы определить, как должен рассматриваться трафик. Например, Распределенная VIP функция Взвешенного произвольного раннего обнаружения, как описано в Обзоре Предотвращения перегрузки, использует значения приоритета IP-трафика для определения вероятности, что будет отброшен пакет.

Сравнение маршрутизации с централизованным доступом CAR и классической политики

Cisco рекомендует использовать функции Modular QoS CLI, если это возможно, для реализации качества обслуживания в сети. Используйте основанное на классе применение политик посредством команды политики в политике обслуживания для реализации ограничения скорости, не буферизуя или помещая в очередь. Избегайте использования CAR, который никакие новые характеристики или функциональность запланирован. Cisco продолжит поддерживать Car для существующих реализаций с помощью этого метода.

Эта таблица приводит функциональные различия между основанным на классе применением политик и CAR:

Функция	Ограничитель на основе классов	CAR

Активируйте метод	Включено внутри политики службы с помощью MQC	Включение только для интерфейса
Команда настройки конфигурации	**команда police в MQC**	**команда rate-limit на интерфейсе или под интерфейсе**
Классификация (в классах трафика)	Требуемый	Необязательно. Поддерживает поинтерфейсное ограничение скорости для всего IP - трафика
Действия для соответствующего и несоответствующего трафика	Три действия: приспособьте, превысьте и нарушьте	Два действия: *соответствовать и превышать. Действие "нарушать" отсутствует*
Маркерный метод измерения	Отдельные элементы token bucket для burst-normal и burst-max	Одиночный алгоритм Token bucket для обычного пакетом и разорванного макс.
Поддержка документа RFC (Request for Comments) 2697	Да, с программного обеспечения Cisco IOS версии 12.1(5)T	Нет

Примечание: Посмотрите RFC 2697 и раздел Действия нарушения этого документа для получения дополнительной информации.

Критерии сопоставления

CAR и основанное на классе применение политик поддерживают другие значения заголовка пакета, на которых можно совпасть для классификации трафика. Соответствие трафика определяет процесс определения трафика для пакетной маркировки и/или ограничения скорости.

Значение заголовка пакета	**Уровень поддержки**	
	Ограничитель на основе классов	**CAR**

Интерфейс входящих или исходящих	Да	Да
Весь IP-трафик или все IP-пакеты соответствуют стандарту или расширенному списку доступа	Да	Да
Значение приоритета IP-пакета	Да	Да
DSCP	Да	â€“
QoS group ID	Да	Да
MAC-адрес	Да	Да
Номера портов Протокола RTP IP	Да	â€“
Значение CoS уровня 2	Да	â€“
Предопределенные карты классов	Да	â€“
Экспериментальное значение MPLS	Да	â€“
Протоколы сетевого распознавания приложений (NBAR)	Да	â€“

Действия "Согласовать" и "Превысить"

Эта таблица приводит поддерживаемые действия для соответствующего и несоответствующего трафика для каждого механизма мониторинга трафика.

Действие	Уровень поддержки	
	Ограничитель на основе классов	CAR
continue	â€”	Да
отбрасывание	Да	Да
set-clp-transmit	Да	Да
set-dscp-continue	â€”	Да
set-dscp-transmit	Да	Да
set-frde-transmit	Да	â€”
set-mpls-exp-continue	â€”	Да
set-mpls-exp-transmit	Да	Да
set-prec-continue	â€”	Да
set-prec-transmit	Да	Да
set-qos-continue	â€”	Да
set-qos-transmit	Да	Да
передача	Да	Да

Поскольку вышеупомянутая таблица иллюстрирует, только CAR поддерживает продолжать действие. Это действие настраивает маршрутизатор для передачи пакета к следующей

политике учетных ставок в цепочке команд rate-limit. CAR и основанное на классе применение политик используют другие алгоритмы. Основанное на классе применение политик использует алгоритмы на основе RFC 2697 и 2698 и не нужно в операторе continue. Посмотрите следующий раздел для получения дополнительной информации.

RFC 2697 и нарушающее действие

В отличие от CAR, для ограничения на основе классов используются алгоритмы, описанные в следующих двух рекомендациях:

- RFC 2697 "одиночная скорость три цветовых маркера" - Cisco IOS Release 12.1 (5) T
- RFC 2698 "две скорости три цветовых маркера" - Cisco IOS Release 12.2 (4) T

Кроме того, важно обратить внимание, что применение политик класса использовало два алгоритма в зависимости от Cisco IOS Release. Программное обеспечение Cisco IOS версии 12.1(5)T представило новый алгоритм и поддержку ограничителя с двумя блоками с помощью действия нарушения. Механизм с двумя блоками представляет значительное функциональное различие между CAR и основанным на классе применением политик.

Алгоритм Token bucket предоставляет пользователям три действия для каждого пакета: действие согласования, действие в случае превышения и действие нарушения. Трафик, вводящий интерфейс с настроенным мониторингом трафика, размещен в одну из этих категорий. В этих трех категориях пользователи могут решить обработки пакета. Например, пакеты, которые соответствуют, могут быть настроены, чтобы быть переданными; пакеты, которые превышают, могут быть настроены, чтобы быть переданными с уменьшенным приоритетом; и пакеты, которые нарушают, могут быть настроены, чтобы быть отброшенными.

Когда опция действия нарушения задана, алгоритм token bucket использует Разделитя token bucket для приспосабливания и превысить пакета. Следующий пример использует алгоритм token bucket с двумя алгоритмами Token bucket.

```
policy-map POLICE
  class twobucket
   police 8000 1000 1000 conform-action transmit exceed-action
   set-dscp-transmit 4 violate-action drop

 interface fastethernet 0/0
  service-policy output POLICE
```

См. Обзор характеристик разделяют в Мониторинге трафика для получения дополнительной информации о настройке действия нарушения.

Дополнительные сведения

- Применение политики на основе классов
- Страница поддержки QoS
- Протоколы маршрутизируемые по IP
- Страница поддержки IP-маршрутизации
- Техническая поддержка - Cisco Systems