Контроль и маркировка QOS с помощью Catalyst 4000/4500 IOS на основе модулей управления Supervisor Engine

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Параметры QoS Профилирования (policing)
Функции контроля и маркировки, поддерживаемые модулями управления Supervisor Engine на основе Catalyst 4000/4500 IOS
Настройка и управление контролем соблюдения правил
Настройка и управление маркированием
Сравнение контроля и маркировки для Catalyst 6000 и модулей управления Supervisor Engine на основе Catalyst 4000/4500 IOS
Дополнительные сведения

Введение

Функция контроля определяет, не превышает ли уровень трафика значение для заданного профиля (контракта). При использовании функции контроля можно отбрасывать внепрофильный трафик или понижать значение трафика, устанавливая для него другое значение DSCP для обеспечения уровня обслуживания, обусловленного договором. DSCP - показатель уровня QoS для пакета. Наряду с DSCP IP-приоритет и CoS также используются для передачи QoS-уровня пакета.

Контроль трафика не следует путать с формированием трафика, хотя оба они предназначены для контроля соответствия трафика профилю (контракту). Контроль соблюдения правил не требует буферизации трафика и поэтому не влияет на задержку передачи. Вместо буферизации внепрофильных пакетов они будут отбрасываться политикой или помечаться другим уровнем QoS (метка DSCP). Формирование трафика буферизует внепрофильный трафик и сглаживает всплески трафика, но влияет на задержку передачи и ее динамику. Формирование можно применять только на исходящем интерфейсе, в то время как контроль – и на исходящем, и на входящем.

Catalyst 4000/4500 с модулем управления Supervisor Engine 3, 4 и 2+ (SE3, SE4, SE2+ далее по документу) поддерживает применение политики на входящих и исходящих направлениях. Формирование трафика также поддерживается, однако в этом документе будет описано только применение контроля и маркировка. Маркировка - процесс изменения уровня QoS пакета в соответствии с политикой.

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.

Параметры QoS Профилирования (policing)

Политики задаются с помощью определения карт политик QoS и применяя их к портам (QoS на основе портов) или VLAN (QoS на основе VLAN). Ограничитель скорости определяется параметрами скорости (rate) и размера пакетов (burst), а также действиями над профильным и непрофильным трафиком.

Поддерживаются два типа средств ограничения скорости: агрегатный и на каждый интерфейс. Каждый ограничитель можно использовать для нескольких портов или VLAN.

Общий ограничитель скорости применяет ограничения к трафику для всех используемых портов/виртуальных локальных сетей. Например, агрегатный ограничитель используется для ограничения трафика простейшего протокола передачи файлов (TFTP) до 1 Мбит/сек для VLAN 1 и 3. Такой ограничитель разрешает суммарный трафик TFTP в сетях VLAN 1 и 3 в 1 Мбит/сек. Если применяется ограничитель скорости по каждому интерфейсу, он ограничит трафик TFTP на каждой VLAN 1 и 3 до 1 Мбит/с.

Примечание: Если к пакету применяются политики для входящего и исходящего трафика, будет принято наиболее жесткое решение. Другими словами, если ограничитель входящего трафика указывает сбросить пакет, а ограничитель исходящего трафика указывает понизить приоритет пакета, то пакет сбрасывается. Таблица 1 содержит сводку действий QoS над пакетом при его обработке политиками входа и выхода.

Таблица 1: Действие QoS в зависимости от политики обработки входящего и исходящего потока

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

Аппаратное обеспечение Catalyst 4000 SE3, SE4, SE2+ QoS выполнено таким образом, что реальная маркировка пакета происходит после ограничителя исходящего потока. Это означает, что даже если политика входа перемаркирует пакет (с использованием сниженной или обычной маркировки ограничителя скорости), то политика выхода все равно увидит пакеты, маркированные исходным уровнем QoS. В политике обработки исходящего потока

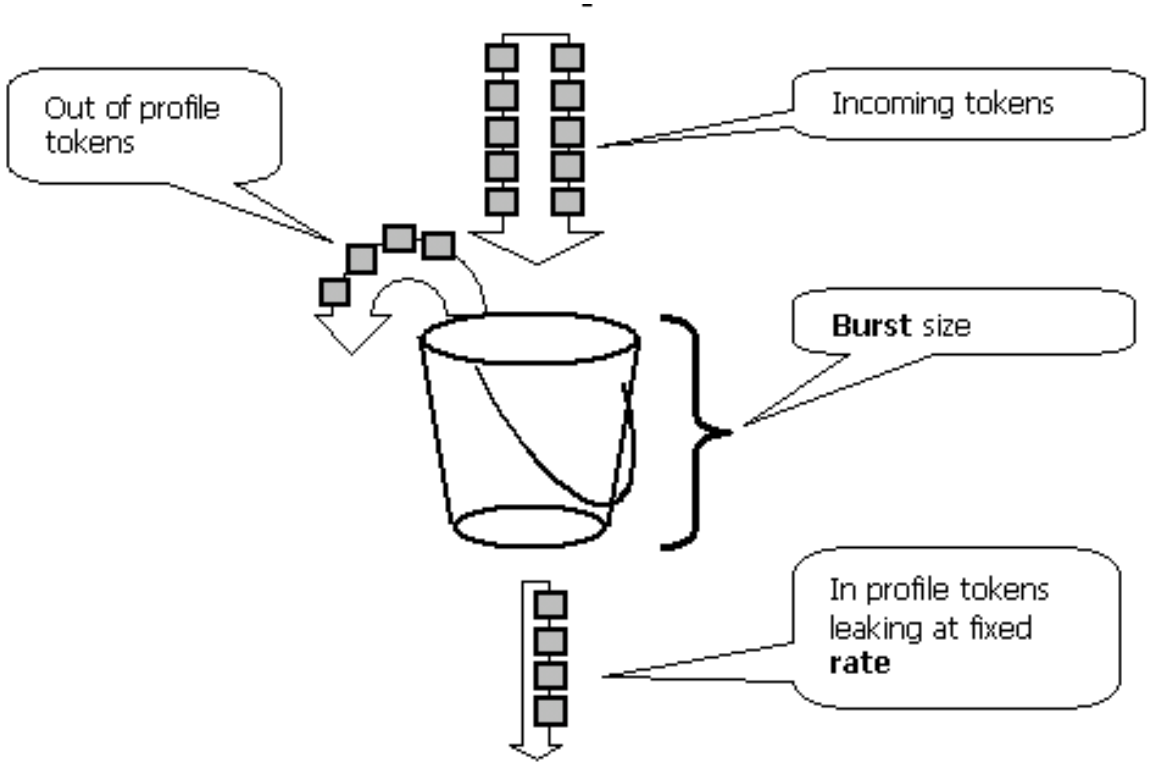
пакет будет рассматриваться как непомеченный политикой входящего потока. Это означает следующее:

- Маркировка выходного трафика переопределяет маркировку входного.
- Политика выхода не может соответствовать новым уровням QoS, которые изменяются вследствие маркировки при входе.

Другие важные последствия таковы:

- Невозможно выполнять маркировку и снижение приоритета в одном и том же классе трафика в пределах одной и той же политики.
- Агрегатные ограничители применяются для определенных направлений. То есть, если агрегатный ограничитель применяется к входящему и исходящему потоку, то получится два агрегатных ограничителя: один на входе, другой на выходе.
- Если агрегатный ограничитель применяется согласно условиям политики к VLAN и к физическому интерфейсу, то будет два агрегатных ограничителя: один для интерфейсов VLAN, другой для физических интерфейсов. В данный момент общее ограничение скорости интерфейсов VLAN и физических интерфейсов невозможно.

Контроль в Catalyst 4000 SE3, SE4, SE2+ действует по принципу "дырявого ведра", представленного на модели ниже. Маркеры, соответствующие входящим пакетам трафика помещаются в корзину (количество маркеров = размер пакета). Определенное число маркеров (установленное исходя из заданной скорости) удаляется из контейнера с регулярными интервалами. Если буфер не может принять входящий пакет, этот пакет считается непрофильным и сбрасывается или получает более низкий приоритет, в зависимости от настроенной политики.



Следует заметить, что трафик не буферизуется в контейнере, как можно подумать, взглянув на эту модель. Реальный трафик вообще не проходит через участок памяти. "Ведро" используется только для определения соответствия или несоответствия пакета профилю.

Обратите внимание, что конкретная аппаратная реализация контроля может быть разной,

но функционально она соответствует этой модели.

Следующие параметры управляют операцией упорядочения:

- Скорость определяет количество маркеров, удаляемых с каждым интервалом. Этот параметр фактически задает скорость упорядочения трафика. Весь трафик, укладывающийся в норму, считается профильным.
- Интервал определяет частоту удаления маркеров из ведра. Интервал установлен в 16 наносекунд (16 сек, умноженное на 10 в -9 степени). Изменение интервала невозможно.
- Всплеск (burst) определяет максимальное количество маркеров, которые "ведро" может удерживать в любое время.

Различия в объеме всплесков между Catalyst 6000 и Catalyst 4000 SE3, SE4, SE2+ см. в разделе "Сравнение политики и маркировки на Catalyst 6000 и модулем управления Supervisor Engine на основе Catalyst 4000/4500 IOS" в конце этого документа.

Ограничитель скорости гарантирует, что при проверке любого периода времени (от нуля до бесконечности) будет разрешено не более

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

трафика, проходящего через механизм ограничения скорости за этот период.

Аппаратное обеспечение QoS Catalyst 4000 SE3, SE4, SE2+ обладает определенной глубиной детализации контроля. В зависимости от выбранной скорости, максимальное отклонение скорости составляет 1,5%.

При настройке скорости всплесков примите во внимание тот факт, что некоторые протоколы (например, TCP) используют механизм управления потоком, реагирующий на потери пакетов. Например, TCP уменьшает окно кадрирования в два раза при каждой потере пакета. При настройке определенной скорости, фактическое использование канала ниже выбранной граничной скорости. Однако можно увеличить размер всплеска, чтобы повысить коэффициент использования. Хорошо начать с установки всплеска размером вдвое больше объема трафика, посылаемого с желаемой скоростью за период передачи-подтверждения (RTT). По той же причине не рекомендуется использовать трафик на основе соединений для сравнительной оценки функционирования ограничителя, поскольку это приведет к более низкой производительности по сравнению с разрешенной.

Примечание: Трафик без установления соединения может по-другому реагировать на контроль. Например, в сетевой файловой системе (NFS) используются блоки, которые могут состоять из нескольких пакетов протокола датаграмм пользователя (UDP). Один отброшенный пакет может повлечь за собой повторную передачу множества пакетов, даже целого блока.

Например, ниже приведен расчет всплеска для сеанса TCP при ограничительной скорости 64 Кбит/сек и заданном TCP RTT 0,05 секунды:

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

Примечание: <burst> применяется для одного сеанса TCP, поэтому нужно учесть ожидаемое количество сеансов, которые пройдут через ограничитель. Это всего лишь пример, поэтому в каждом конкретном случае необходимо оценить трафик/требования к использованию и характеристики поведения с учетом имеющихся ресурсов, чтобы выбрать соответствующие параметры политики.

Действие политики заключается в отбрасывании пакета (сброс) или изменении значения DSCP пакета (пометка). Для снижения приоритета пакета, карта контроля DSCP должна быть изменена. Установленное по умолчанию ограничительное значение DSCP используется для пометки пакета этим же DSCP, т. е. не происходит снижения приоритета.

Примечание: Если внепрофильный пакет предназначается DSCP в очередь исходящих пакетов, которая отличается от первоначальной DSCP, пакеты могут отсылаться без сохранения порядка. По этой причине, если важен порядок отправки пакетов, рекомендуется понижать приоритет внепрофильных пакетов до значения DSCP, сопоставленного с той очередью исходящих пакетов, в которой находятся профильные пакеты.

Функции контроля и маркировки, поддерживаемые модулями управления Supervisor Engine на основе Catalyst 4000/4500 IOS

На Catalyst 4000 SE3, SE4, SE2+ поддерживается как входящий трафик (входящий интерфейс), так и исходящий трафик (исходящий интерфейс). Коммутатор поддерживает 1024 входных и 1024 выходных ограничителей. По умолчанию, при отсутствии контроля, система использует два входных и два выходных ограничителя.

При применении агрегатного ограничителя к VLAN и физическому интерфейсу, используется дополнительно аппаратный ограничитель. В данный момент общее ограничение скорости интерфейсов VLAN и физических интерфейсов невозможно. Возможно, это будет исправлено в следующих выпусках программного обеспечения.

Все версии ПО включают поддержку контроля. Модель Catalyst 4000 поддерживает до 8 утверждений соответствия для каждого класса и до 8 классов для каждой карты контроля. Допустимы следующие утверждения соответствия:

- match access-group
- match ip dscp
- match ip precedence
- match any

Примечание: Для пакетов V4, отличных от протокола IP, утверждение соответствия match ip dscp является единственным способом классификации, при условии, что пакеты прибывают на транковые порты с доверием CoS. Ключевое слово “ip” в команде match ip dscp не должно ввести вас в заблуждение, так как происходит согласование внутреннего DSCP. Это применимо ко всем пакетам, не только к IP. Когда порт настроен доверять CoS, значение CoS извлекается из кадра L2 (802.1Q или маркированного ISL) и преобразуется во внутренний DSCP с помощью QoS-отображения CoS на DSCP. **Внутреннее значение DSCP можно сопоставить с контролем с помощью команды match ip dscp.**

Допустимы следующие действия контроля:

- политика
- set ip dscp
- set ip precedence
- trust dscp
- trust cos

Маркировка позволяет изменять уровень QoS пакета на основании классификации или политик. Классификация разбивает трафик на различные классы для обработки QoS на основе определенных критериев. Чтобы сопоставить приоритет IP или DSCP, необходимо установить режим доверия для соответствующего входящего интерфейса. Коммутатор поддерживает доверие CoS, доверие DSCP и ненадежные интерфейсы. Доверие указывает поле, откуда будет получен уровень QoS пакета.

При доверии CoS, уровень QoS будет наследован из заголовка L2 ISL или инкапсулированного пакета 802.1Q. При доверии DSCP, коммутатор получает уровень QoS из поля пакета DSCP. Доверенные CoS используются только на магистральных интерфейсах, а доверенный DSCP – только для пакетов IP V4.

Когда интерфейс не является доверенным (это состояние по умолчанию при включении QoS), внутренний DSCP будет производным от настраиваемых параметров по умолчанию CoS или DSCP для соответствующего интерфейса. Если CoS или DSCP по умолчанию не настроен, значение по умолчанию равно 0. После определения для пакета исходного уровня QoS этот уровень отображается на внутреннюю точку DSCP. Внутреннюю DSCP можно сохранить или заменить применением политик либо маркированием.

После прохождения пакетом обработки QoS поля уровня QoS (в поле IP DSCP для IP и в заголовке ISL/802.1Q, при его наличии) будут обновлены из внутренней точки DSCP.

Предусмотрены специальные соответствия, используемые для преобразования доверительных метрик QoS пакета во внутреннее DSCP и обратно. Используются следующие соответствия:

- DSCP к контролируемому DSCP – используется для заимствования контролируемого DSCP при уменьшении приоритета пакета.
- DSCP к CoS: используется для получения уровня CoS из внутреннего DSCP для обновления заголовка исходящего пакета ISL/802.1Q.
- CoS в DSCP: используется для получения внутреннего DSCP из входящего CoS (заголовок ISL/802.1Q header), если интерфейс находится в доверенном режиме CoS.

Помните, что когда интерфейс находится в режиме доверия CoS, исходящий CoS всегда будет таким же, как и входящий CoS. Это относится к реализации QoS в Catalyst 4000 SE3, SE4, SE2+.

Настройка и управление контролем соблюдения правил

Настройка политики в IOS включает следующие шаги:

1. Определение ограничения скорости.
2. Определение критериев отбора трафика для ограничения.
3. Определение служебной политики, используя класс и применяя к нему ограничитель.
4. Применение политики обслуживания по отношению к порту или сети VLAN.

Рассмотрим следующий пример. Существует подключенный к порту 5/14 генератор трафика, который посылает трафик UDP со скоростью 17 Мбит/сек на порт назначения 111. Необходимо ограничить этот поток трафика до 1 Мбит/сек и отбросить лишний трафик.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
```

```
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Обратите внимание, что если порт находится в режиме QoS на основе VLAN, но к соответствующей VLAN не применено никакой политики обслуживания, то коммутатор будет использовать политику обслуживания (если имеется), применимую к физическому порту. Это дает дополнительную гибкость в объединении QoS на основе портов и на основе VLAN.

Поддерживаются два типа средств ограничения скорости: именованная совокупность и на каждый интерфейс. Именованный общий ограничитель скорости ограничивает скорость общего трафика со всех интерфейсов, к которым его применяют. В приведенном выше примере использовался именованный ограничитель скорости. Ограничитель скорости для каждого интерфейса, в отличие от именованного ограничителя, будет ограничивать трафик отдельно на каждом интерфейсе, на котором он применен. Поведение интерфейсного диспетчера политик определяется в конфигурации карты политик. Рассмотрим следующий пример с общим ограничителем скорости по каждому интерфейсу:

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

Следующая команда используется для мониторинга операций ограничения:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
```

```
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Счетчик возле схемы класса определяет количество пакетов, соответствующих классу.

Помните о следующих условиях, связанных с внедрением:

- Счетчик пакета по классу не является счетчиком по интерфейсу. То есть, он подсчитывает только пакеты, совпадающие по классу во всех интерфейсах, в которых данный класс применяется в политике обслуживания.
- Ограничители не поддерживают счетчики пакетов. Поддерживаются только счетчики байтов.
- Специальная команда для проверки скорости входящего и исходящего трафика для каждого ограничителя скорости отсутствует.
- Счетчики обновляются периодически. Если быстро повторить вышеуказанную команду несколько раз подряд, счетчики какое-то время могут отображаться без изменений.

Настройка и управление маркированием

Настройка маркировки включает следующие шаги:

1. Определение таких критериев классификации трафика, как списки доступа, DSCP, IP-приоритет и т.д.
2. Определение классов трафика для классификации по указанным ранее критериям.
3. Создайте схему политик, назначая действия маркировки и/или регулировки определенным классам.
4. Настройка режима доверия на соответствующих интерфейсах.
5. Применить карту политик к интерфейсу.

Рассмотрим следующий пример. Необходимо входящий трафик с IP-приоритетом, равным 3, для хоста 192.168.196.3 UDP-порта 777, перевести на IP-приоритет, равный 6. Весь прочий трафик с IP-приоритетом, равным 3, ограничивается по скорости до 1 Мбит/с, а у лишнего трафика IP-приоритет понижается до 2.

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
```

```
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Команда sh policy interface используется для мониторинга маркировки. Примеры выходных данных и последствий заносятся в приведенную выше конфигурацию политики.

Сравнение контроля и маркировки для Catalyst 6000 и модулей управления Supervisor Engine на основе Catalyst 4000/4500 IOS

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

Дополнительные сведения

- Основные сведения и настройка QoS
- Техническая поддержка - Cisco Systems