Общие сведения о применении политик QoS и маркировке трафика на Catalyst 3550

Содержание

Введение

Функция контроля определяет, находится ли уровень трафика в пределах указанного профиля или контракта, и позволяет отбрасывать внепрофильный трафик или понижать его статус, устанавливая для него другое значение DSCP. Это позволяет обеспечить уровня обслуживания, обусловленный контрактом.

DSCP – мера уровня QoS для пакета. Наряду с DSCP для отображения QoS-уровня пакета также используются IP-приоритет и CoS.

Контроль трафика не следует путать с формированием трафика, хотя оба они предназначены для контроля соответствия трафика профилю или контракту.

Контроль соблюдения правил не требует буферизации трафика, и поэтому не влияет на задержку передачи. Внепрофильные пакеты не буферизуются – они отбрасываются функцией контроля или помечаются 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 3550 поддерживает контроль как входящего, так и исходящего трафика. Формирование трафика не поддерживается.

Маркировка изменяет уровень QoS пакета в соответствии с политикой.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Данный документ не ограничен отдельными версиями программного и аппаратного обеспечения.

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию. При работе с реально функционирующей сетью необходимо полностью осознавать возможные последствия выполнения команд до их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Версии аппаратного и программного обеспечения

Контроль и маркирование в Catalyst 3550 поддерживаются во всех версиях программного обеспечения. Здесь приводится последняя редакция руководства по конфигурации. В нем описаны все поддерживаемые функциональные возможности.

- Настройка QoS

Параметры политик и маркирования QoS

Чтобы настроить контроль, следует определить карты политик QoS и применить их к портам. Иначе это называют «QoS на основе портов».

Примечание: QoS на основе VLAN в данный момент не поддерживается Catalyst 3550.

Ограничитель определяется параметрами скорости (rate) и размера пакетов (burst), а также действиями над внепрофильным трафиком.

Поддерживаются два типа ограничителей:

- общий
- индивидуальный

Общий ограничитель применяет ограничения к трафику на всех используемых объектах. Индивидуальный ограничитель действует в отношении трафика отдельно на каждом объекте, где он применяется.

Примечание: На Catalyst 3550 общий ограничитель может применяться только к различным классам одной и той же политики. Общий ограничитель для нескольких интерфейсов или политик не поддерживается.

Например, применим общий ограничитель в целях ограничения до 1 Мбит/с трафика класса customer1 и класса customer2 в одной той же карте политик. Такой ограничитель разрешает трафик 1 Мбит/с одновременно классам customer1 и customer2. Если применить индивидуальный ограничитель, он лимитирует до 1 Мбит/с отдельно трафик класса customer1 и трафик класса customer2, то есть каждый экземпляр ограничителя будет действовать отдельно от остальных.

В данной таблице собраны действия QoS над пакетом при его обработке политиками входа и выхода.

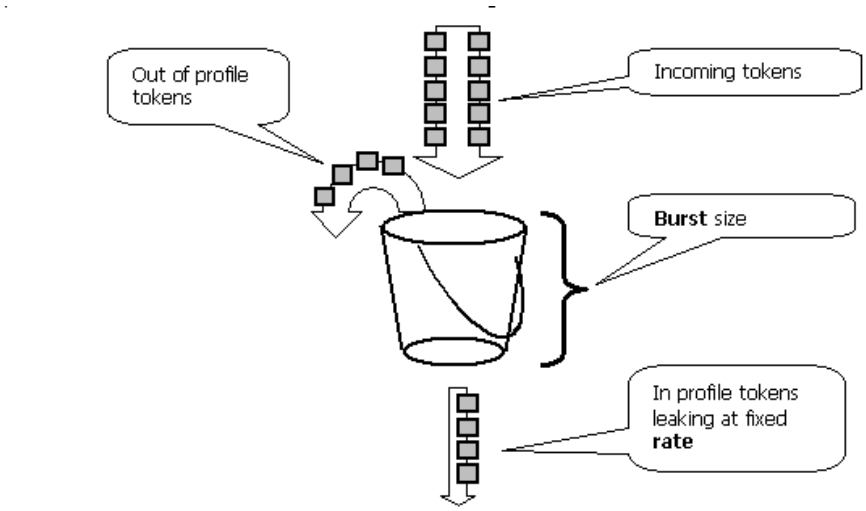
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Примечание: Невозможно выполнять маркировку и снижение приоритета в одном и том же классе трафика одной и той же политики. В этом случае сначала весь трафик этого класса будет маркирован. Контроль и снижение приоритета производятся в отношении уже маркированного трафика.

Контроль QoS в Catalyst 3550 действует по принципу дырявого ведра:

Маркеры в количестве, пропорциональном размерам пакетов входящего трафика, кладутся в маркированную область памяти token bucket; число маркеров равно размеру 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.

Этот принцип показан в следующем примере.



Примечание: Трафик не буферизуется в контейнере, как может показаться из этого примера. Реальный трафик вообще не проходит через контейнер; контейнер используется только для определения соответствия или несоответствия пакета профилю.

Примечание: Аппаратная реализация контроля может быть разной, но функционально она соответствует этой модели.

Следующие параметры управляют операцией контроля:

- **Скорость** – определяет число маркеров, удаляемых в каждом интервале. Этот параметр фактически задает ограничительную скорость трафика. Весь трафик, укладывающийся в норму, считается профильным. Поддерживаемые скорости находятся в диапазоне от 8 кбит/с до 2 Гбит/с и возрастают с шагом 8 кбит/с.
- **Интервал** – определяет частоту удаления маркеров из контейнера. Интервал является фиксированным, 0,125 миллисекунд (или 8000 раз в секунду). Менять интервал нельзя.
- **Пакет** – определяет максимальное число маркеров, которые контейнер («ведро») может удерживать в каждый момент времени. Поддерживаемые пакеты находятся в диапазоне от 8000 байт до 2 000 000 байт и возрастают с шагом 64 байта.

Примечание: Хотя с помощью командной строки можно вывести большой диапазон значений, параметр rate-bps не может превышать настроенную скорость порта, burst-byte – 2 000 000 байт. При вводе большего значения коммутатор отказывается от карты политик, когда она применяется к интерфейсу.

Для поддержания заданной скорости трафика пакет должен быть не меньше числа удаляемых с каждым интервалом маркеров.

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Вычислим, например, минимальное значение пакета для поддержания скорости 1 Мбит/с. Задана скорость в 1000 кбит/с, так что минимальный необходимый пакет будет суммой следующего выражения:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

Минимальный поддерживаемый размер пакета – 8000 байт – это больше, чем вычисленный минимальный пакет.

Примечание: Ввиду неоднородности политики аппаратного обеспечения значения точной скорости передачи данных и размера пакета округляются до ближайшего поддерживаемого значения.

При настройке размера пакета учитывайте, что некоторые протоколы используют механизмы, которые реагируют на потери пакетов. Например, TCP уменьшает окно в два раза при каждой потере пакета. Это вызывает пилообразный эффект в трафике TCP, когда TCP пытается ускориться до скорости линии и ограничитель начинает его регулировать. Если рассчитать среднюю скорость пилообразного трафика, то она будет намного ниже, чем ограниченная скорость. Однако можно увеличить размер пакета, чтобы повысить использование трафика. Хорошо начать с установки пакета размером вдвое больше объема трафика, посылаемого с желаемой скоростью за период приема-передачи (TCP RTT). Если RTT неизвестно, можно удвоить значение параметров пакета.

По той же причине не рекомендуется использовать трафик на основе соединений для сравнительной оценки функционирования ограничителя. Как правило, в этом случае производительность получается ниже той, которую обеспечивает ограничитель.

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

В данном примере приводится расчет пакета для сеанса TCP при ограничительной скорости 64 кбит/ и заданном TCP RTT 0,05 секунды:

```
= 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

В данном примере <burst> относится к одному сеансу TCP. Умножьте это число на ожидаемое количество сеансов, которые пройдут через ограничитель.

Примечание: 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 контроля.

Действие контроля заключается в отбрасывании пакета (сброс) или изменении значения DSCP пакета (снижение приоритета). Для пометки снижения приоритета пакета ограничительное сопоставление DSCP должно быть изменено. Установленное по умолчанию ограничительное значение DSCP используется для пометки пакета этим же DSCP. Таким образом, понижения не происходит.

Если непрофильные пакеты понижаются до значения DSCP, сопоставленного с другой очередью исходящих пакетов, а не до значения DSCP, сопоставленного с исходной очередью, некоторые пакеты могут отправляться без сохранения порядка. По этой причине, если важен порядок отправки пакетов, рекомендуется понижать непрофильные пакеты до значения DSCP, сопоставленного с той очередью исходящих пакетов, в которой находятся профильные пакеты.

Функциональные возможности контроля и маркировки, поддерживаемые Catalyst 3550

В данной таблице приведена совокупность функциональных возможностей контроля и маркировки, поддерживаемых Catalyst 3550, разбитых по направлению:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

На карту класса поддерживается одна инструкция сопоставления. Ниже приведены действительные инструкции сопоставления для входного контроля:

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

Примечание: В Catalyst 3550 команда **match interface** не поддерживается и в карте класса разрешается только одна команда сопоставления. Таким образом, затруднительно классифицировать весь трафик, который входит через интерфейс, и проконтролировать весь трафик с помощью одного ограничителя. См. раздел данного документа Как классифицировать весь трафик интерфейса с помощью одного ограничителя.

Ниже приведены действительные инструкции сопоставления для выходного контроля:

- match ip dscp

Ниже приведены действительные действия контроля для входной политики:

- police
- set ip dscp (marking)
- set ip precedence (marking)
- trust dscp
- trust ip-precedence
- trust cos

В данной таблице приведена матрица поддерживаемых политик входного QoS:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Этот параметр касается также сопоставления приоритета IP.
2. Этот параметр касается также доверия CoS, приоритета IP и DSCP.
3. Этот параметр касается также установки приоритета IP.

Ниже приведены действительные действия контроля для выходной политики:

- police

В данной таблице приведена матрица поддерживаемых политик выходного QoS:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

Маркировка позволяет изменять уровень QoS пакета на основании классификации или контроля. Классификация разбивает трафик на различные классы для обработки QoS на основе определенных критериев.

Обработка QoS основана на внутреннем DSCP; это показатель уровня QoS пакета. Внутренний DSCP образуется согласно настройке доверия. Система поддерживает доверие CoS, приоритет IP, DSCP и ненадежные интерфейсы. Доверие указывает поле, откуда будет получен внутренний DSCP для каждого пакета, следующим образом:

- Если CoS надежен, уровень QoS будет наследован из заголовка L2 ISL или инкапсулированного пакета 802.1Q.
- Если надежен DSCP или приоритет IP, система получает уровень QoS, соответственно, из поля пакета DSCP или приоритета IP.

Доверенные CoS используются только на магистральных интерфейсах, а доверенный DSCP (или приоритет IP) – только для пакетов IP.

Когда интерфейс не является доверенным, внутренний DSCP извлекается из настраиваемого CoS по умолчанию для соответствующего интерфейса. Это состояние по умолчанию при включенном QoS. Если CoS по умолчанию не настроен, значение по умолчанию – 0.

Как только внутренний DSCP определен, его можно сохранить или заменить контролем и маркированием.

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

- **DSCP-to-Policed DSCP** – используется для получения ограничительного DSCP при маркировании пакета для снижения приоритета.
- **DSCP-to-CoS** – используется для получения уровня CoS из внутреннего DSCP для обновления исходящего заголовка пакета ISL/802.1Q.
- **CoS-to-DSCP** – используется для получения внутреннего DSCP из входящего CoS (заголовок ISL/802.1Q header), если интерфейс находится в доверенном режиме CoS.

Существуют важные условия, связанные с внедрением:

- Входную служебную политику нельзя применять к интерфейсу, если он настроен доверять любой метрике QoS, например CoS/DSCP или приоритету IP. Чтобы сопоставить приоритеты DSCP/IP и ограничить входной трафик, следует настроить степень доверия для отдельного класса в рамках политики, а не на интерфейсе. Чтобы проводить маркирование на основе приоритетов DSCP/IP, доверие настраивать не следует.
- С точки зрения аппаратного обеспечения и QoS IP-трафиком считается только трафик IPv4 без параметров IP и инкапсуляции Ethernet II Advanced Research Projects Agency (ARPA). Весь остальной трафик считается не IP-трафиком, включая IP с параметрами, такой как инкапсулированный SubNetwork Access Protocol (SNAP) трафик IP и IPv6.
- Для не IP-пакетов match access group – это единственный метод сопоставления, поскольку нельзя сравнивать DSCP с не IP-трафиком. Для этой цели используется ACL MAC; пакеты могут сопоставляться по MAC-адресу источника, MAC-адресу назначения и EtherType. Невозможно сопоставлять IP-трафик с помощью MAC ACL, поскольку коммутатор различает трафик IP и не IP.

Настройка и мониторинг контроля

Следующие действия необходимо выполнить для настройки контроля в Cisco IOS:

1. Определить ограничитель (для общих ограничителей)
2. Определить критерии отбора трафика для контроля
3. Определить карту классов для отбора трафика с использованием определенных критериев
4. Определить служебную политику, используя класс и применяя к нему ограничитель
5. Применить служебную политику к порту

Поддерживаются два типа ограничителей:

- именованный общий
- индивидуальный

Именованный общий ограничитель контролирует общий трафик со всех классов в пределах одной политики, к которой он применяется. Общий ограничитель для нескольких интерфейсов не поддерживается.

Примечание: Общий ограничитель нельзя применять более чем к одной политике. В этом случае появится сообщение об ошибке:

```
QoS: Cannot allocate policer for policy map
```

Рассмотрим следующий пример:

Существует привязанный к порту GigabitEthernet0/3 генератор трафика, который посылает трафик UDP со скоростью примерно 17 Мбит/с на порт назначения 111. Существует также трафик TCP из порта 20. Необходимо ограничить эти два потока трафика до 1 Мбит/с и отбросить лишний трафик. В данном примере показывается, как это сделать.

```
!--- Глобальные QoS.

mls qos

!--- Задает ограничитель QoS, устанавливает для размера пакета
!--- значение 16000, чтобы повысить производительность TCP.

mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop

!--- Определяет ACL по выбранному трафику.

access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any

!--- Определяет классы трафика, которые будут контролироваться.

class-map match-all cl_udp111
 match access-group 123
class-map match-all cl_tcp20
 match access-group 145

!--- Определяет политику QoS и прикрепляет
!--- ограничитель к классам трафика.

policy-map po_test
 class cl_udp111
   police aggregate pol_1mbps
 class cl_tcp20
   police aggregate pol_1mbps

!--- Применяет политику QoS к интерфейсу.

interface GigabitEthernet0/3
switchport
switchport access vlan 2
service-policy input po_test
!
```

В первом примере использовался именованный общий ограничитель. Индивидуальный ограничитель, в отличие от именованного, ограничивает трафик отдельно в каждом классе, для которого он применяется. Индивидуальный ограничитель определяется в конфигурации карты политик. В данном примере два класса трафика ограничиваются двумя индивидуальными ограничителями; cl_udp111 ограничивается до 1 Мбит/с на пакет 8K, а cl_tcp20 – до 512 кбит/с на пакет 32K.

```
!--- Глобальные QoS.

mls qos

!--- Определяет ACL по выбранному трафику.

access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any

!--- Определяет классы трафика, которые будут контролироваться.
```

```
class-map match-all cl_udp111
 match access-group 123
class-map match-all cl_tcp20
 match access-group 145

!--- Определяет политику QoS, создает и прикрепляет
!--- ограничители к классам трафика.

policy-map po_test2
 class cl_udp111
   police 1000000 8000 exceed-action drop
 class cl_tcp20
   police 512000 32000 exceed-action drop

!--- Применяет политику QoS к интерфейсу.

interface GigabitEthernet0/3
switchport
switchport access vlan 2
service-policy input po_test2
```

Эта команда используется для мониторинга работы контроля:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
 dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
 dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a       n/a      266303     0

WRED drop counts:
 qid  thresh1    thresh2   FreeQ
  1 : 0          0         1024
  2 : 0          0         1024
  3 : 0          0         8
  4 : 0          0         1024
```

Примечание: По умолчанию статистика по каждому DSCP не собирается. Catalyst 3550 поддерживается сбор статистики по интерфейсу и по направлению для не более чем восьми различных значений DSCP. Этот параметр настраивается при задании команды **mls qos monitor**. Чтобы отслеживать статистику для 8, 16, 24 и 32 DSCP, следует выполнить следующую команду **per-interface**:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Примечание: Команда **mls qos monitor dscp 8 16 24 32** изменяет выходные данные команды **show mls qos int g0/3 statistics** следующим образом:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
 dscp: incoming   no_change  classified policed    dropped (in pkts)
   8 : 0          0          675053785  0          0
   16: 1811748    0          0          0          0         ? per DSCP statistics
   24: 1227820404 15241073   0          0          0
   32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
 dscp: incoming   no_change  classified policed    dropped (in pkts)
   8 : 675425886     n/a       n/a      0          0
   16: 0             n/a       n/a      0          0         ? per DSCP statistics
   24: 15239542      n/a       n/a      0          0
   32: 539289117     n/a       n/a      536486430  0
Others: 1983055       n/a       n/a      1649446    0

WRED drop counts:
 qid  thresh1    thresh2   FreeQ
  1 : 0          0         1024
  2 : 0          0         1024
```

```
  3 : 0          0          6
  4 : 0          0          1024
```

Это описание полей в примере:

- **Incoming** – показывает, сколько пакетов прибывает с каждого направления
- **NO_change** – показывает, сколько пакетов было оценено как надежные (такие, в которых уровень QoS не изменен)
- **Classified** – показывает, скольким пакетам после классификации был назначен данный внутренний DSCP
- **Policed** – показывает, у скольких пакетов контроль понизил приоритет; DSCP показывается перед маркировкой снижения приоритета
- **Dropped** – показывает, сколько пакетов было отброшено контролем

Помните о следующих условиях, связанных с внедрением:

- Если при задании команды **mls qos monitor** настроены 8 значений DSCP, другие счетчики, видимые при задании команды **show mls qos int statistics**, могут выдавать неадекватные данные.
- Специальная команда для проверки скорости входящего и исходящего трафика для каждого ограничителя скорости отсутствует.
- Поскольку счетчики извлекаются с аппаратного уровня последовательно, возможно, что они будут добавляться некорректно. Например, объем ограниченных, классифицированных или отброшенных пакетов может немного отличаться от числа входящих пакетов.

Настройка и мониторинг маркирования

Для настройки маркирования выполните следующие действия:

1. Определить критерии классификации трафика
2. Определить классы трафика для классификации по указанным ранее критериям
3. Создать карту политик, которая назначает определенным классам действия по маркировке и контролю
4. Настроить соответствующие интерфейсы в режим доверия
5. Применить карту политик к интерфейсу

В данном примере необходимо маркировать входящий трафик на хост 192.168.192.168 IP-приоритетом 6 и ограничить его до скорости 1 Мбит/с; лишний трафик должен быть маркирован IP-приоритетом 2:

```
!--- Глобальные QoS.

mls qos

!--- Определяет ACL по выбранному трафику.

access-list 167 permit ip any host 192.168.192.168

!--- Определяет класс трафика.

class-map match-all cl_2host
 match access-group 167

!--- Определяет политику QoS, создает и прикрепляет
!--- ограничители к классам трафика.
```

```
policy-map po_test3
 class cl_2host

!--- Маркирует весь трафик класса IP-приоритетом 6.

   set ip precedence 6

!--- Ограничивает трафик до 1 Мбит/с и снижает приоритет согласно карте QoS.

   police 1000000 8000 exceed-action policed-dscp-transmit

!--- Изменяет карту QoS ограниченного DSCP, так что
!--- IP-приоритет трафика снижается с 6 до 2.
!--- В терминах DSCP – с 48 до 16 (DSCP=IPprec x8).

mls qos map policed-dscp  48 to 16

!--- Применяет политику QoS к интерфейсу.

interface GigabitEthernet0/3
switchport
switchport access vlan 2
service-policy input po_test3
```

Та же самая команда **show mls qos interface statistics** задается для мониторинга маркирования. Примеры выходных данных и последствий приводятся в данном документе.

Как классифицировать весь трафик интерфейса с помощью одного ограничителя

В Catalyst 3550 команда **match interface** не поддерживается, и в карте класса разрешается только одна команда сопоставления. Более того, Catalyst 3550 не разрешает сопоставление IP-трафика по ACL MAC. Так что трафик IP и не IP следует классифицировать с помощью двух отдельных карт классов. Таким образом, затруднительно классифицировать весь трафик, который входит в интерфейс, и проконтролировать весь трафик с помощью одного ограничителя. Сделать это можно с помощью конфигурации, приведенной в примере ниже. В нем трафик IP и не IP сопоставляется с помощью двух отдельных карт классов. Однако обе они используют общий ограничитель для обоих видов трафика.

```
access-list 100 permit ip any any

class-map ip
match access-group 100

!--- По это йкарте классифицируется весь IP-трафик.


mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl

!--- Здесь по карте классов классифицируется только не IP-трафик.


mls qos aggregate-policer all-traffic 8000 8000 exceed-action drop

!--- Этой командой настраивается общий ограничитель, который применяется и к IP, и к не IP-трафику.


policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic

!--- Этой командой карта политик применяется к физическому интерфейсу.
```

Дополнительные сведения

- **Настройка QoS на Catalyst 3550**
-

- **Страница поддержки QoS**
- **Страница поддержки коммутации LAN**
- **Страницы поддержки продуктов LAN**
- **Техническая поддержка и документация – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/9/92097/153.shtml

---